National Counter-Information Operations Strategy

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY
FEBRUARY 2019

Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/D3P

Statements and views expressed in this document are solely those of the authors and do not imply endorsement by Harvard University, the Harvard Kennedy School, or the Belfer Center for Science and International Affairs.

Design & Layout by Andrew Facini

Cover photo: Deputy Secretary General Alexander Vershbow and the 28 Permanent Representatives to the North Atlantic Council visit NATO's cyber defence centre at Supreme Headquarters Allied Powers Europe (SHAPE) in Mons, Belgium on Friday, 23 January 2015. (NATO Photo)

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY
FEBRUARY 2019

National Counter-Information Operations Strategy

Contents

Defending Digital Democracy Project: About Us

We established the Defending Digital Democracy Project (D3P) in July 2017 with one goal: to help defend democratic elections from cyber attacks and information operations.

Last year, we set out to provide campaign and election professionals with practical guides to the most applicable cybersecurity best practices in advance of the 2018 midterm elections. In November 2017, we released "**The Campaign Cybersecurity Playbook**" for campaign professionals. In February 2018, we released a set of three guides designed to be used together by election administrators: "**The State and Local Election Cybersecurity Playbook**," "**The Election Cyber Incident Communications Coordination Guide**," and "**The Election Incident Communications Plan Template**." What follows is a collaborative research and policy paper on countering information operations from members of the D3P team. This paper is the launch of D3P's efforts to help understand and counter information operations. We hope this Playbook will illustrate some of the possible strategic solutions to countering information operations and making our democracy more secure.

D3P is a bipartisan team of cybersecurity, political, and policy experts from the public and private sectors. To better understand both the cybersecurity and other challenges that elections face, our team spent six months researching state and local election processes in 2017. We visited with 34 state and local election offices, observed the November 2017 elections in three states and the 2018 midterms in five different states, and interviewed leading academic experts, election equipment manufacturers, and representatives of federal government agencies. We conducted a nationwide security survey with 37 participating states and territories, which identified detailed nuances in election processes and their corresponding risk considerations. We hosted three state election cybersecurity conferences where we engaged state and local election officials in "tabletop exercise" election simulations to increase awareness of the cybersecurity threats they face and improve their ability to mitigate those threats.

Good luck,
The D3P Team

Authors and Contributors

AUTHORS

Gabe Cederberg, D3P, Harvard College

Jordan D'Amato, D3P, Harvard Kennedy School

Corinna Fehst, D3P, Harvard Kennedy School

Simon Jones, D3P, Harvard Kennedy School

Kunal Kothari, D3P, Harvard Kennedy School

Aleksandra Milcheva, D3P, Harvard Kennedy School

Irene Solaiman , D3P, Harvard Kennedy School

SENIOR ADVISORY GROUP

Eric Rosenbach, Co-Director, Belfer Center;
Director, Defending Digital Democracy Project

Robby Mook, Co-Director, D3P

Matt Rhoades, Co-Director, D3P

Heather Adkins, Director, Information Security and Privacy, Google; Belfer Center Senior Fellow

Dmitri Alperovich, Co-Founder and CTO, Crowdstrike; Belfer Center Senior Fellow

Stuart Holliday, President and CEO, Meridian International Center; former United States Ambassador for Special Political Affairs at the United Nations

Nicco Mele, Director, Shorenstein Center on Media, Politics, and Public Policy at the Harvard Kennedy School

Jan Neutze, Director of Cybersecurity Policy, Microsoft

Debora Plunkett, former Director of the National Security Agency's Information Assurance Directorate

Suzanne E. Spaulding, former Under Secretary–National Protection and Programs Directorate (NPPD) at the Department of Homeland Security

Alex Stamos, Stanford University

Siobhan Gorman, Director, Brunswick Group

ACKNOWLEDGEMENTS

Mari Dugas, Project Coordinator, D3P

Frank White, Independent Communications Consultant

BELFER CENTER WEB & DESIGN TEAM

Andrew Facini, Publications and Design Coordinator, Belfer Center

Introduction

American democracy is under attack. From the daily news to our social media feeds, nation-state competitors target the United States and its citizens, seeking to fuel division and chaos at home while undermining our interests abroad and our will to defend them. It is critical that policymakers and citizens understand these threats and how to counter them. This playbook seeks to ensure that U.S. citizens, not foreign actors, determine the future of U.S. democracy.

While nation-state competitors have employed propaganda and information operations (IO) targeting the United States for decades, in recent years their efforts have changed dramatically. The rise of the Internet and social media as mechanisms for disseminating news has made our country both more globally interconnected and simultaneously more vulnerable to foreign efforts to destabilize our democracy. There is now clear evidence that Russia used influence operations designed to undermine U.S. democracy and citizens' trust in its integrity in both the 2016 and 2018 election cycles. Adversaries are actively using information as a weapon to attack the United States, our political system, and citizens' trust in it.

The consequences for the United States are severe. Foreign actors stoke social tensions and drive partisan politics in our elections. America's competitors undermine our willingness to defend our beliefs and the rules-based international system—from Ukraine to the South China Sea. The principles upon which our nation was founded are now under ongoing attack, with no letup in sight. Across each of these dimensions, strategic competitors seek to use the free and open nature of our social and political system against us. Russian efforts to undermine our elections are the most significant near-term threat, but it is far from the only challenge we face. In the medium- to long-term, China seeks to displace the United States from the Indo-Pacific and rewrite the rules-based international system to suit its own interests. Iran and North Korea both harbor ambitions to fundamentally change their regional security environments. In each of these cases, information operations targeting the United States are a key tool that our competitors use to pursue their goals.

As a result, the United States urgently needs to understand how it can better prevent information operations and mitigate their effects on our citizens and our democracy.

This report helps address the challenge posed by IO by defining the IO threats that the United States faces and then outlining an overall approach for countering them in a manner consistent with American values. This approach reflects an integrated, whole-of-nation effort—with a focus on the federal government, but also including relevant players in the private sector and civil society. Finally, the report concludes with a set of concrete actions that each of these actors can take to better counter and mitigate IO.

This Playbook consists of three parts:

1. **Our Approach:** Outlines the intent of the playbook and key considerations.
2. **Understanding the Threat:** Explains threats across the information landscape facing the United States.
3. **Recommendations:** Offers 10 key recommendations that the public and private sector in the United States can take now to combat information operations by increasing costs and reducing benefits for competitors.

Our Approach

Information operations target society as a whole, so it is difficult for any one actor to respond to them. As such, the United States needs a coordinated approach that spans the public and private sectors rather than allowing each group to react, thereby risking a duplicative and ineffective response. Proactively determining a national counter-IO approach can help the United States leverage the complementary strengths of different sectors, organizations, and technologies.

This report offers concrete actions to counter state-sponsored information operations targeting the United States. Because the volume and scope of recent information operations impacts the United States at the national level, we focus primarily on recommendations for the federal government. However, a federal-led effort must also draw on the private sector, civil society, and international allies and partners. As such, this report outlines actions that federal departments and agencies can take both in cooperation with one another and with other entities in the private sector, civil society, and abroad.

Similarly, because information operations target U.S. democracy broadly, any response must defend our entire social, political, and economic system. While information operations targeting our elections may be the highest visibility attacks, they are just one part of a broader campaign to undermine the United States, our interests, and our way of life. The recommendations in this report offer options to counter information operations that target:

- The faith of U.S. citizens in the integrity of their political system;
- Public trust in the media;
- The use of information as a tool to keep decision-makers accountable; and
- The open society that makes the American democratic system possible.

Finally, any coordinated response must also align with the fundamental values that our adversaries seek to undermine and disrupt. Information operations deliberately exploit the free and open nature of our society. As with U.S. counterterrorism and cybersecurity efforts, counter-IO actions need to balance any measures to prevent attacks on American institutions against the basic values and principles of freedom that constitute the foundation of our security and prosperity. Our efforts to counter disinformation must reflect and bolster these values, including:

- Freedom of speech and freedom of the press;
- The rule of law in domestic and international affairs;
- The right to individual self-determination, specifically that citizens have the information and transparency to make informed decisions (e.g., on political ads);
- The right to national self-determination, specifically that the decisions in U.S. democracy should be determined by U.S. actions alone; and
- The importance of protecting and securing user data.

Understanding the Threat

What are Information Operations (IO)?

Information operations, also referred to as influence operations, are the dissemination of information, true or false, that seeks to manipulate public opinion and/or influence behavior. The motivation for conducting information operations ranges from political to social to economic, with state and non-state actors leveraging technological and psychological tools to achieve their goals. Digital technologies like social media and encrypted messaging apps have made it possible for nation-states to conduct and organize information operations on an unprecedented scale. Because the tools needed for information operations are cheap and widely accessible, adversaries that cannot challenge the United States through conventional tactics often use IO as an asymmetric means to undermine the United States and compete for global influence.

Common information operation tactics include spreading fake or misleading information online, leaking stolen information online, and using social media to amplify opposing views and stir political conflict. Attackers may also penetrate networks to obtain sensitive information with the intent to manipulate or leak it as part of a broader IO campaign

What's at Stake?

Information operation campaigns undermine America's core democratic values by hijacking the public narrative and manipulating perceptions for the benefit of foreign actors. These actions represent a direct attack on American interests. Previous campaigns have undermined trust in democratic institutions, increased suspicion of the media as a check on power and a force for the public good, exacerbated social tensions and national unrest, falsely discredited political figures and groups, and directly attacked U.S. economic interests. Campaigns sponsored by Russia, for instance, have incited rallies by extremist groups, amplified hate speech and themes of excluding minority groups, and made false claims about the safety of domestic energy production methods. Simply put, these attacks have been levied with explicit goals to promote foreign interests and inflict harm on the U.S. political system and on the institutions that serve American citizens.

The "Who" Behind Information Operations

The information operations threat landscape is multifaceted, but nation-states dominate this domain of strategic competition. Russia, China, Iran, North Korea, and other state-level actors have both the capacity and intent to influence democratic politics and public opinion, and to sow division across the American electorate.

Russia's efforts have been most noticeable and widely discussed in the public domain. The U.S. intelligence community has assessed with high confidence that Russian President Vladimir Putin ordered coordinated operations to influence the 2016 Presidential elections with the intent to undermine public faith in the democratic process.[1] Moscow has made ample investments in its capabilities in recent years and has demonstrated its willingness to use them, targeting not only the United States but also former Soviet republics. Interference with public opinion and information has been observed in a variety of channels, from state-owned media outlets to professional trolls.[2] As with cyberattacks and physical attacks, information operation threats should be viewed as assaults on the American people and the institutions that serve and protect them.

China has actively employed information operations to promote its interests and undercut those of the United States, but in a subtler manner than Russia. Under President Xi Jinping, China has made both overt and covert investments in the U.S. media landscape to shape narratives regarding the Chinese and U.S. roles in the world. Since 2012, China has increased foreign direct investment in U.S. entertainment, media, and education from nearly zero to some $9 billion while expanding English-language coverage of the state-run media organizations Xinhua and China Daily.[3] Beijing has also pursued more deceptive approaches to influencing U.S. audiences. For example, a 2015 Reuters investigation reported that China state-run media employed a series of shell companies to obscure its ownership of 33 radio stations in the United States and 13 other countries.[4] These radio stations actively sought to influence U.S. listeners' perceptions of key topics, from the South China Sea to democratic elections in Hong Kong.[5] As a strategic competitor, China has used information operations to undermine U.S. citizens' commitment to the rules-based international order and democratic norms and to weaken this country's willingness to respond.

Iran has also been found to be operating information operation campaigns. In August of 2018, U.S. cyber threat intelligence firm FireEye tipped off social media companies to over 600 fake accounts that were likely to have originated in Iran. These accounts and "inauthentic news sites" were aimed at promoting Iranian political interests in the United States. FireEye characterized the accounts as evidence that actors beyond Russia continue to engage in and experiment with online, social media-driven influence operations to shape political discourse.[6]

North Korean capabilities include the country's influence over South Korea to secure attendance at the 2018 Winter Olympics and to spread their message that they are established as a nuclear power. Officials suspect that the intent may have included attempting to drive a wedge in the U.S.-ROK alliance.[7] In 2015, the state's "Cyber Army" reportedly reached 6,000 troops with the mission to cause "physical and psychological paralysis."[8] Organizations like APT37, a state-connected North Korean cyber espionage group, focus on intelligence gathering and target media, and as of 2018, North Korean is reported to be running over 160 propaganda websites with approximately 7,000 active agents supporting these operations.[9] A reported 300 agents specialize in "online opinion-rigging activities." These numbers are expected to grow as state-run websites like Pyongyang Times are becoming more user-friendly and heavily trafficked.[10]

Recommendations

The following 10 recommendations provide concrete actions that the U.S. government can take now to address the threat posed by foreign information operations. The first half of this section summarizes the recommendations. The second half elaborates on these recommendations by providing an overview, bullet points that describe subordinate objectives, and finally a table that outlines specific actions that U.S. federal departments and agencies can pursue in concert with one another to best counter or mitigate information operations.

Summary

Create Factual Counter-Narratives	Provide citizens of designated IO-offensive countries (e.g., Russia, China) with credible and accurate information, including facts about the actions of their leaders, and highlight how propagandists attempt to manipulate narratives to mislead their own citizens.
Publicly condemn IO and identify malicious actors	Clearly signal to allies and adversaries alike that the United States will not permit foreign powers to influence its democratic processes. Condemn information operations both through public messaging and by employing technical tools to "name and shame."
Freeze assets and ban visas	Impose consequences on those who interfere in our democratic processes by freezing their assets, access to the U.S. financial system, and freedom of movement.
Interrupt channels of influence	Use the full spectrum of U.S. capabilities to undermine, interrupt, block, and appropriate the capacity of adversaries to spread malicious information.
Leverage U.S. force posture to impose costs and strengthen deterrence against future IO attacks	Increase engagement, military-to-military cooperation, and foreign military sales in key states to fight the growing influence of Russia, China, and other competitors, while clearly identifying U.S. actions as a response to IO targeting our national interests.
Create a defensive public communications strategy	Actively communicate with the American public to counter the objectives of propaganda (e.g., to undermine the willingness of U.S. citizens to respond to Russian aggression in Eastern Europe, China's militarization of the South China Sea), rather than the propaganda itself.
Create national counter-information operations strategy and center	Establish a high-level interagency fusion cell modeled after the National Counter Terrorism Center to design, plan, and coordinate operational activities. Include representatives from the defense, diplomatic, and intelligence communities.

Increase media literacy	Increase media literacy training in the education system to build resilience of at-risk populations.
Update political advertising and campaign finance laws	Modernize political advertising and campaign finance laws to cover a broader range of online activity, enhance transparency requirements, and prevent political spending by foreign nationals.
Improve public-private sector collaboration	Engage "Big Tech" and the private sector more broadly to draw on the expertise of U.S. citizens to prepare and protect the whole of society from IO attacks.

1. Create Factual Counter-Narratives

Competitors have systematically targeted the United States with false narratives about our democratic system, political candidates, government officials, and government actions. Instead of allowing the cycle of disinformation to continue, the U.S. government should respond with factual counter-narratives. This strategy should provide citizens of designated IO-offensive countries (e.g., Russia, China) with credible and accurate information about the actions of their leaders and should highlight how propagandists within the country attempt to manipulate narratives to mislead their own citizens. The strategy can draw on the experience of existing programs focused on China and Iran.

There are programs currently in place that provide useful models for this strategy. For example, "Current Time" is a 24/7 Russian-language TV network operated by the Atlantic Council, Radio Free Europe / Radio Liberty, and Voice of America (VOA) that provides accurate and independent local, regional, and international news in more than 10 strategically significant countries.[11] Although the platform connects Russian speakers around the world using digital platforms, social networks, and satellite and cable TV, "Current Time" does not target Russians inside Russia. Reaching Russian citizens is challenging because the Russian government has the ability to jam transmissions, arrest and kill journalists, control the travel of journalists, and close news bureaus.[12]

- **Develop and implement a strategy for creating credible and accurate international reporting**. This effort would likely build on the "Current Time" model by expanding its reach to include other critical languages and countries. This strategy could benefit by tracking how foreign audiences are targeted with disinformation to calibrate its reporting so that those audiences are most receptive. Ensuring that reporting incorporates open source analysis from other countries, such as the UK's BBC Monitoring service, can also help ensure its objectivity.

- **Design and execute a plan to deliver the factual counter-narrative content to key foreign audiences**. This may also be done in concert with partners and could include the decision to avoid targeting certain audiences if the potential ramifications are determined to outweigh the benefits.

2. Publicly condemn IO and identify malicious actors

In messaging the nation's stance on election interference, a clear, consistent, and direct message is essential. Without a commonly understood framework for what constitutes illegal information operations, perpetrators go unpunished and a disparate set of affected candidates, organizations, and agencies will struggle to respond effectively. Therefore, it is essential that the government identify foreign interference in our democratic processes, and detail means of response against information operations in domestic elections.

Send a clear, bipartisan message by Congress that the United States does not tolerate foreign interference in our democratic processes. A unified statement defining information operations and outlining a response to provocations will demonstrate to foreign actors and American citizens the bipartisan support for taking action, and help set a framework for response.

Increase investment in attribution capabilities. In order to fully leverage the value of the United States' economic power, the government must identify which entities and individuals to target for sanctions. Building out the capacity for U.S. agencies to attribute attacks without the risk of exposing valuable sources and methods will help make targeted sanctions a simpler and more easily employed tool. This may include partnering with private sector organizations.

3. Freeze assets and ban visas

Articulating and implementing targeted sanctions in response to IO is one critical component of meaningful deterrence. Specifically, U.S. actions to enact economic sanctions, freeze assets, and ban visas have been among the most effective responses to influence operations. The United States should continue to employ these tools. Legal indictments go a step further, and jointly, all four mechanisms offer ways to impose costs on malicious actors engaged in IO campaigns against the United States. Cost imposition must play a major role in preventing actors from undertaking information operations against the U.S., in what has to date been largely an asymmetric vector of attack. Congress and the Executive Branch, namely the president and the Department of Justice, are the primary actors in this sphere and have actively engaged this set of cost imposition methods to counter IO. Congress' efforts to enact cost- imposing legislation will most likely depend on how active or inactive a response it seeks to foreign actors' misinformation attempts during the 2018 midterm elections.

Carry out clear, swift, legal punishments for foreign information operations. The United States should lead efforts to use legal and reputational tools to indict and punish nations and entities that use cyberattacks and information operations. These punishments may include corresponding asset freezes, strict travel restrictions, and other sanctions at the disposal of the U.S. government.

Implement economic sanctions against propaganda posing as journalism. The U.S. should impose sanctions, fines, and other barriers against the practice of propaganda under the guise of journalism. State-controlled media outlets that use their national or international media platforms to advance influence campaigns must be punished.[13]

Pick up and pass the Cyber Deterrence and Response Act of 2018 (HR 5576).[14] This bill would direct the Secretary of State to publish names of identified actors who have engaged in cyber attacks, and direct them to sanction those actors appropriately. Such a bill would require the State Department to work with Congress to detail the nature of attacks and develop sanctions, creating a framework for punitive response.

4. Interrupt Channels of Influence

The federal government must think creatively about how it can tackle and disrupt IO. Preventing terrorist attacks is a useful point of comparison because a large swath of agencies and departments have had to demonstrate institutional flexibility and ingenuity in adapting to emerging threats. As with terrorism, it is more effective to prevent IO than respond to it. This means disrupting the structures and circumstances that enable and facilitate IO before disinformation campaigns are launched. The government can disrupt IO channels of influence in a number of ways:

Conduct upstream interventions. The U.S. Intelligence Community's (IC) upstream interventions of terrorist activity have played a key role in keeping the United States safe. The IC could play a similar role for countering disinformation. The IC could use cyber and other technical capabilities to take troll factories offline, publicly leak damaging information about hackers, and target firms and private sector entities that enable or facilitate IO, such as Internet cafes and dark web servers. In addition, the IC could build profiles of non-state actors and proxies who contribute to IO to better understand their motivations. This might allow the development of messaging and interventions that discourage their participation.

Embrace a whole-of-society response. The federal government can draw on private sector and not-for-profit support more broadly than it has in the past. This could be conducted in a number of ways, including offering bounties for the identification of substantial troll factories and botnets; recognition for white hat hackers and groups that expose IO vulnerabilities; and hosting hackathons and conferences with the tech sector to share ideas and strategies on combating IO.

Identity and access management. The federal government can also offer ways to verify and validate online identities. As with the Twitter "blue check," which denotes a verified account, the government's standards of identity management could be applied to other forums so that citizens can trust comments posted online. Solutions would be especially relevant to online political campaigning. While Facebook's policy of required identification for political advertisements is welcome, it is unclear whether these measures would have prevented the IO conducted during the 2016 presidential election, noting the identity and financial fraud that has been uncovered. A federal government-delivered online identity and access management system that allows firms and social media companies to validate customers and users online could help to keep U.S. citizens safer in cyberspace.

5. Leverage U.S. force posture to impose costs and strengthen deterrence against future IO attacks

Improving deterrence starts with deploying the right capabilities and shaping the perceptions of foreign leaders. Because these perceptions reflect a broad assessment of U.S. intentions and capabilities, deterrence should employ the full spectrum of foreign policy tools, not just those within the cyber domain. U.S. force posture and readiness offer a wide range of options to impose costs on strategic competitors and deter future information operation attacks. On the low end, this includes actions such as increasing military-to-military cooperation with allies and partners to fight the influence of strategic competitors like Russia and China. On the high end, this includes actions such as permanently increasing troop levels or capabilities, prepositioning equipment in strategic locations, and expanding bilateral and multilateral military training and exercises.

Clearly link U.S. actions to hostile information operations targeting our national interests: Clearly labeling U.S. force posture actions as a response to Russia's previous and ongoing attacks on our democratic system is critical to improving deterrence. Signaling that these actions are a consequence of Russia's attack on our democracy demonstrates to Russia and to other competitors that the United States will forcefully defend its interests.

Improve interoperability with allies and partners: Increasing military-to-military cooperation with allies and partners can improve deterrence, impose costs on competitors, and protect U.S. interests. This can include actions such as information and intelligence exchanges, training and exercises, and deploying U.S. capabilities or providing capabilities to allies and partners. Specific examples vis-à-vis Russia include: increasing U.S. information sharing with the Balkan states; improving the capabilities of U.S. NATO forces; deploying additional combat troops in Poland or the Baltics; providing Ukraine with additional defensive capabilities; prepositioning equipment in strategic locations within NATO's eastern-most states; and improving missile defense.

6. Create a Defensive Public Communications Strategy

In addition to combatting the flow of information operations, the U.S. government should actively communicate with the American public to counter the objectives of foreign propaganda. Competitors like Russia use information operations to disseminate false information and incite social unrest. A defensive public communications strategy would provide an asymmetric counterbalance to propaganda by focusing on ends rather than means.

Counter the objectives, rather than the propaganda itself: Given the volume and content of information operations that competitors can spew out through social and traditional media, the U.S. government cannot and should not respond to each false narrative individually. Addressing the content directly adds fuel to the narrative's fire. In a world where news stories are often read only in sound bites and headline scans, any response is likely only to spread the false story, rather than effectively combat it. Instead, the government should counter the objectives of propaganda rather than its content. For example, Russian IO often contains messages reflecting American weakness and corruption or inciting chaos and distrust in American democratic institutions. A defensive public communications strategy should focus on countering these overall objectives.

Share best practices across sectors: Run workshops with government officials and members of the private sector and civil society to share best practices and learn how to effectively identify and counter disinformation. Draw on subject matter expertise from Non-Governmental Organizations (NGOs) and the private sector (e.g., social media companies).[15]

7. Create a National Counter-Information Operations Center

Effective actions against information operations require constant interagency and multiparty collaboration. Developing a central body and strategy to combat information operations will ensure that important information reaches all relevant parties and can be addressed by all relevant agencies. This organization should also have responsibility for interacting with the U.S. private sector and with international organizations and allies.

Create an interagency fusion cell to combat IO modeled on the National Counter-Terrorism Center (NCTC): A national center for countering IO can draw on the lessons of the development and operation of the NCTC to improve communication and coordination among relevant government agencies, the private sector, and international partners and allies.[16] Combining the skills, resources, and intelligence of national agencies and government bodies already dedicated to countering IO enhances U.S. government capacity and prevents intelligence hoarding or overlap.

Increase public-private sector information sharing on IO threats: Establishing regular contact with relevant private sector companies, including social media agencies, can help provide an architecture and cadence for information sharing without overlaps.[17]

Invest in government capabilities independent of the private sector to track IO on social media: Developing or using existing tools to track and flag information operations on traditional and social media can create a common operating picture for the U.S. government and reduce dependence on private sector entities to disclose information that may not be in their interests.

8. Increase Media Literacy

Public resilience in response to information operations depends on the public's awareness of IO campaigns and ability to discern them when they are launched. The government must educate its citizens about the methods that malicious actors use to spread disinformation. Building trust in public service media and improving fact-checking efforts to hold media outlets accountable are essential in mitigating the effects of information operations. The U.S. government should engage in the following coordinated efforts to improve public resiliency toward information operations:

Strengthen public service media: The government should invest in public broadcast and investigative units to emphasize the importance of a free press. This effort should include a public information campaign to educate at-risk global populations on how to recognize the signs of disinformation. As part of this initiative, the United States should leverage the authorizations proposed in CAATSA to increase foreign assistance to European and Eurasian states and build resilience by supporting civil society initiatives, including media literacy programs.[18]

Develop Department of Education guidelines on combating disinformation: Media literacy and critical thinking are key components of a modern education. In preparation for its 2018 parliamentary elections, Sweden launched a nationwide program to teach students in elementary and high school to distinguish between real and fake news.[19] The program is headed by the Swedish Media Council, a government agency whose primary task is to help students become conscious media users. The U.S. Department of Education should be responsible for spearheading a similar nationwide effort in the United States.[20]

Create an independent network of fact-checkers: Fact-checking initiatives already exist to discredit untrustworthy sources and bolster authentic reporting. In Sweden, five of the largest media outlets created a dedicated fact-checking collaborative.[21] The initiative is, in part, supported by government funds. By capturing the breadth of the ideological spectrum, the fact-checking collaborative can reasonably tout its independence. Alternatively, the U.S. government could convene a board of journalists to operate an independent fact-checking organization.

9. Update Political Advertising and Campaign Finance Laws

The 2016 U.S. presidential elections exposed many of the legal loopholes and flaws that competitors leveraged to employ information operations using political ads, campaign finance, and other forms of influence. The United States urgently needs to modernize campaign finance and political advertising laws to cover a broader range of online activity, enhance transparency requirements, and prevent political spending by foreign nationals.

Pass the Honest Ads Act: By taking advantage of disparate requirements around identifying foreign countries' involvement in advertising buys on different platforms, nation-state competitors have exploited legal loopholes in our political advertising landscape. The framework proposed in the Honest Ads Act would bring the requirements for online advertising in line with those of traditional media platforms, as mandated by the Federal Election Campaign Act of 1971. Online platforms must have a degree of accountability to disclose buyers of online campaign ads, and prevent foreign buyers from making such purchases. Platforms should also be required to include clear, legible disclosures around the buyer and funding for ad transparency, as an online equivalent to disclosures required for television and radio ads.

The framework of this regime has already garnered some support from companies like Twitter and Facebook. However, formalizing the framework and setting guidelines around reasonable expectations for identity verification is needed to help create an enduring barrier to overt information operation campaigns, and a structure with flexibility to adapt to new channels of information distribution and advertising going forward. Further, formalization will develop an expectation of accountability and clarity around enforcement. Indeed, Facebook's recent discovery of foreign engagement in coordinated influence campaigns illustrates that identifying these networks is technically feasible, and platforms selling campaign- or issue- related ads to U.S.-based users can reasonably be expected to develop systems similar to "know your customer" regulations to protect platforms from coordinated campaigns and violation of the Honest Ads Act.[22]

Update campaign finance Laws: The recommendations above represent a baseline approach, given existing campaign finance law frameworks. They will pose a deterrent to malicious actors and a higher cost barrier, but will not protect the public from loopholes and the opportunity for disguised and "pass-through" campaign influence by well-funded state actors. Strengthening campaign finance laws to improve transparency, especially around foreign actors, will help to insulate elections from foreign influence. Legislation should strengthen beneficial ownership disclosure requirements to prevent foreign influencers from establishing shell corporations to purchase ads or conduct information operations under domestic addresses. Establishing disclosure requirements for shell corporations and for corporate or foreign contributions to Political Action Committee groups can help to prevent a common workaround for making foreign contributions.

Strengthen the Foreign Agents Registration Act (FARA): FARA has been leveraged increasingly to enforce disclosure of government ties and affiliations from lobbyists and agents, along with details around financial arrangements and the distribution of informational materials. Originally passed in 1938 to combat Nazi propaganda and information dissemination, FARA needs to be modernized to cover emerging frontiers for running information operations. The DOJ took the step of requiring Russia Times and Sputnik to register under FARA, and should further strengthen the definitions and enforcement of FARA to encompass organizations distributing information on smaller, more targeted scales online.

10. Improve Public-Private Sector Collaboration

Based on the nature of the tactics, techniques, and procedures used by hostile nations, the success of new initiatives to combat IO and disinformation will depend on better public-private partnerships. Private firms and not-for-profit organizations often find themselves targeted by disinformation and the U.S. government can do more to prepare and protect the whole of society and draw on the expertise and insight of U.S. citizens. There are a number of ways to accomplish this goal, including:

Rebuild the links between social media companies and the U.S. intelligence and law enforcement communities: The Snowden leaks severely damaged links between the U.S. government and social media companies. Since then, social media has become a key focal area for hostile nations to compete with the United States, the European Union, and other allies and partners. Both sectors could do more to collaborate in countering IO. This must be done in a transparent and open way that allows both sides to better understand emerging threat pictures and tactics, techniques, and procedures.

Promote social media company voluntary codes of conduct: Competitors often use a number of different channels and platforms simultaneously to propagate information operations. Awareness and knowledge of the activities conducted on each platform could prove instrumental in responding to IO as each platform captures different information from users.[23] Twitter, for example, captures a large amount of information on users from the point of registration onwards. This includes the IP address used to create the account, basic information about the device used, and when the account and content was created. Social media companies could establish information-sharing arrangements among themselves in the event that they suspect users of disseminating disinformation, helping to disrupt IO. This could be modeled on the efforts of banks to share information on financial crimes and fraudulent transactions.

Develop Algorithm and Security Measure Audits: The U.S. government could also introduce rules requiring social media companies to submit algorithms and security measures for auditing. This would give the government a greater understanding of how social media algorithms can be targeted and exploited by IO, enhancing its ability to react and respond to disinformation. As part of this audit, the government could red-team measures implemented by social media platforms after the 2016 presidential election, including identity requirements for political campaigns, and make recommendations to strengthen these measures.

Develop incident response and business continuity plans: As with other events, such as terrorist attacks and civil disasters, the government could offer advice and guidance to the private and not-for-profit sectors on how to react and respond to IO and disinformation. This advice could include best practices for cybersecurity measures and cyber forensics around data breaches and how to work with law enforcement agencies to investigate incidents.

Provide open source threat assessments and alerts: In line with the UK's National Cyber Security Centre, the United States could offer open source assessments and alerts on IO-related threats and incidents.[24] This might include cyber-attacks, attempts by trolls to fuel violent protests, and use of botnets to amplify disinformation. This would allow the private sector and civil society to better understand threats and prepare themselves accordingly.

Department- and Agency-Specific Tasks

To support implementation of the 10 recommendations listed previously, this section offers a summary of specific tasks that different departments and agencies in the government can carry out. Numbers below correspond to the numbered recommendations in the previous section.

Dept. of Defense	**4**	Deliver more intensive operations to disrupt IO and disinformation.
	5	Rotate high-end capabilities through the Eastern Europe and Indo-Pacific theaters—particularly air assets, including F-35s and B-2s, maritime assets, and Patriot systems. Creating "variable geometry" of U.S., allied, and partner forces disrupts military planning of competitors.
	5	Increase NATO's presence in Latvia, Lithuania, and Estonia, to seven brigades, including three Armor Brigade Combat Team equivalents, in addition to the armed forces of the Baltic nations. Starting in the Baltics aligns with the president's priority of increasing the number of NATO allies who are spending two percent of GDP on defense.[25]
	5	Increase the number of Armor Brigade Combat Teams in the U.S. Army.[26]
	5	Along with DoS, communicate to Russian counterparts that a force posture change of this size should not be seen as a credible threat to Russian sovereignty or territory.[27]
	5	Continue the European Phased Adaptive Approach to missile defense.[28]
	7	Encourage NATO to build strategic communications and counter-IO efforts into its operational planning and incident management processes.
	7	Develop a center or fund to focus on building and deploying mitigation and enforcement capabilities to visualize, identify, and monitor patterns and trends in IO campaigns and media manipulation.
	7	Align the U.S. counter-IO operations center with NATO's Intelligence Fusion Centre (NIFC).
	10	With DHS, lead the development of incident response and business continuity plans for critical infrastructure, as well as private sector firms critical to the Defense Industrial Base and the Defense Innovation Base.
	10	Work with DHS to develop open source IO threat assessments and alerts.
Dept. of State	**1**	Develop a strategy both for creating credible and accurate content and delivering the content to key foreign audiences.
	2	Send a clear message stating that the United States does not tolerate foreign interference in our democratic processes.
	2	Cooperate with Congress and the Office of Foreign Assets Control (OFAC) at the Department of the Treasury to impose sanctions and economic restrictions against entities advancing information operations.
	3	Assist Congress and the Department of the Treasury (OFAC) in enacting effective sanctions by providing complete and accurate lists of individuals and entities engaged in IO campaigns against U.S. elections in 2016 and 2018.
	5	Along with the DoD, conduct Foreign Military Sales with allies and partners. For example, consider providing secure communications, counterbattery radars, reconnaissance UAVs, and armored transport vehicles to Ukraine.[29]
	7	Leverage Global Engagement Center resources and funding to develop and operate tools that more efficiently identify and attribute IO campaigns.
	8	Implement a public information campaign globally for at-risk populations.

Dept. of Homeland Security	**4** Develop programs to convene, collaborate with, and incentivize private sector, white-hat hacker community, and tech industry innovation and involvement, in countering disinformation (e.g., "bot bounties"). **8** Train public and civil servants to recognize information operations. **10** With DoD, develop incident response and business continuity plans for critical infrastructure, as well as private sector firms critical to the Defense Industrial Base and the Defense Innovation Base. **10** Work with DoD to develop open source IO threat assessments and alerts.
Dept. of Justice Fedral Bureau of Investigation	**7** Increase FBI and police collaboration and information-sharing with law enforcement bodies, including Europol and Interpol to pursue and prosecute those conducting IO. **9** Take the lead in modernizing the structure and details of FARA as it relates to the spread of information on social media networks; develop a structure for enforcing the law and treating foreign nationals attempting to influence the public discourse through social media platforms and other media under the same framework as those disseminating content through printed media or TV and radio. **10** Rebuild links with social media companies. **10** Develop alliances and partnerships with social media platforms to audit security and oversight mechanisms, enforcement capabilities, and red-team functions to test compliance.
Central Intelligence Agency	**1** Invest and expand open source analysis capabilities, including the Open Source Enterprise, and continue to partner with allies. **4** Deliver more intensive operations to disrupt IO and disinformation. **5** Provide tailored information sharing and intelligence to allies and partners.
National Security Agency	**4** Deliver more intensive operations to disrupt IO and disinformation. **5** Provide tailored information sharing and intelligence to allies and partners.
Congress	**2** Impose sanctions and economic restrictions against entities advancing information operations. **3** Pass the Counteracting Russian Hostilities Act of 2017 to further enact sanctions against individuals who were engaged in the 2016 IO campaign against U.S. elections. These proposed sanctions would expand the range of individuals targeted by sanctions and related measures while also providing a strong threat of cost to future actors. **8** Authorize an increase in foreign assistance to European and Eurasian states to build resilience in response to information operations. **9** Pass the Honest Ads Act. This would be the first step before the more nuanced work of revising campaign finance laws to close key loopholes. Congress must also work in tandem with the DOJ to update and modernize FARA. **10** Emphasize to the private sector the importance of cooperating with U.S. government departments and agencies.
Federal Communications Commsission	**4** Develop a framework for auditing security measures.
U.S. Gov't Chief Information Officer	**4** Deliver identity and access management solutions for cross-platform and private sector identity verification and validation.
Platform Companies	**9** Strengthen the ability to identify foreign accounts routinely amplifying political and issue-related content on their platforms, as well as paid promotion of related content coming from entities with affiliations to foreign governments. Doing so will leave companies more prepared to help enforce FARA once the DOJ and an intra-agency task force begin identifying likely violations.

Endnotes

[1] Background to "Assessing Russian Activities and Intentions in Recent US Elections:" The Analytic Process and Cyber Incident Attribution. DNI, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf

[2] "Innovations in Warfare & Strategy—Russia's Improved Information Operations: From Georgia to Crimea." Strategic Studies Institute (SSI), 2017. https://ssi.armywarcollege.edu/pubs/parameters/issues/Summer_2017/8_Iasiello_RussiasImprovedInformationOperations.pdf

"Modern Political Warfare: Current Practices and Possible Responses." RAND, 2018. https://www.rand.org/pubs/research_reports/RR1772.html

[3] "The U.S.-China FDI Project." https://rhodiumgroup.gistapp.com/us_china_foreign_direct_investments

[4] "China is spending billions to make the world love it." *The Economist*, 23 May, 2017. https://www.economist.com/china/2017/03/23/china-is-spending-billions-to-make-the-world-love-it

[5] Ibid.

[6] "Suspected Iranian Influence Operation Leverages Network of Inauthentic News Sites & Social Media Targeting Audiences in U.S., UK, Latin America, Middle East." FireEye, 2018. https://www.fireeye.com/blog/threat-research/2018/08/suspected-iranian-influence-operation.html

[7] "Countering North Korea's Political Warfare." RAND, 2018. https://www.rand.org/blog/2018/02/countering-north-koreas-political-warfare.html

[8] "North Korea boosted 'cyber forces' to 6,000 troops, South says." Reuters, 2015. https://www.reuters.com/article/us-northkorea-southkorea/north-korea-boosted-cyber-forces-to-6000-troops-south-says-idUSKBN0KF1CD20150107

[9] "Lesser-known North Korean cyber-spy group goes international: report." Reuters, 2018. https://www.reuters.com/article/us-northkorea-cyber/lesser-known-north-korea-cyber-spy-group-goes-international-report-idUSKCN1G42CH

[10] "North Korea's Influence Operations, Revealed." The Diplomat, 2018. https://thediplomat.com/2018/07/north-koreas-influence-operations-revealed/

[11] "Current Time: the Independent Russian-Language News Network." BBG, Broadcasting Board of Governors, 7 Feb. 2017, www.bbg.gov/2017/02/07/current-time-independent-russian-language-news-network/.

[12] Hill, Thomas M. "Is the U.S. Serious about Countering Russia's Information War on Democracies?" Brookings, Brookings Institution, 21 Nov. 2017, www.brookings.edu/blog/order-from-chaos/2017/11/21/is-the-u-s-serious-about-countering-russias-information-war-on-democracies/.

[13] One of Congress' strongest actions in response to the 2016 Russian IO campaign was the passage of H.R. 3364 "Countering America's Adversaries Through Sanctions Act" (CAATSA), which passed with an overwhelming majority and was signed into law by President Trump on August 2, 2017. While the bill itself allows for greater action against Russian individuals and entities involved in IO campaigns, many of the provisions have yet to be acted on by the Trump administration.

[14] United States Congress, House, "Cyber Deterrence and Response Act of 2018." Congress, 18 Apr. 2018, https://www.congress.gov/bill/115th-congress/house-bill/5576

The sanctions bar funds from going to support any individuals or countries that back Russia's 2014 annexation of Crimea, and any persons who engaged in "malicious cyber-enabled activities." Specifically, Congress calls for the President to "impose the sanctions…with respect to any person…[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," with sanctions including freezing assets and visa suspension. In a section specifically labeled "Countering Russian Influence and Aggression," the bill also outlaws any federal money flowing to the Russian government and authorizes $250 million for the Countering Russian Influence Fund.

[15] "Information warfare in the Internet: Countering Pro-Kremlin Disinformation in the CEE Countries." *StopFake*, June 2017, https://www.stopfake.org/content/uploads/2017/07/Information-warfare-in-the-Internet_report_19.07-2.pdf

[16] The Atlantic Council. “Democratic Defense Against Disinformation.” 2018. https://disinfoportal.org/democratic-defense-against-disinformation-3/

RAND. “Modern Political Warfare.” 2018. https://www.rand.org/pubs/research_reports/RR1772.html

[17] The Atlantic Council. “Democratic Defense Against Disinformation.” 2018. https://disinfoportal.org/democratic-defense-against-disinformation-3/

[18] United States Congress, “Countering America’s Adversaries Through Sanctions Act.” 2017. https://www.congress.gov/bill/115th-congress/house-bill/3364/text.

[19] “Introducing Source Criticism in the Classroom.” Sharing Sweden, Swedish Institute, 13 Dec. 2017. https://www.sharingsweden.se/toolkits/introducing-source-criticism-classroom/; Roden, Lee. “Swedish Kids to Learn Computer Coding and How to Spot Fake News in Primary School.” The Local, The Local Europe AB, 13 Mar. 2017, www.thelocal.se/20170313/swedish-kids-to-learn-computer-coding-and-how-to-spot-fake-news-in-primary-school.

[20] Brattberg, Erik, and Maurer, Tim. “Russian Election Interference: Europe’s Counter to Fake News and Cyber Attacks.” Carnegie Endowment for Peace. 2018. https://www.carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435.

[21] Santalo, Janetta. “Sweden Prepares for Fake News Ahead of Election.” Mundus International, 2018, https://www.mundus-international.com/sweden-prepares-for-fake-news-ahead-election/.

[22] “Removing Bad Actors on Facebook.” Facebook Newsroom, 31 July, 2018. https://newsroom.fb.com/news/2018/07/removing-bad-actors-on-facebook/

[23] Shaffer, Kris. “Spot a Bot: Identifying Automation and Disinformation on Social Media.” Medium, 5 June 2017, https://medium.com/data-for-democracy/spot-a-bot-identifying-automation-and-disinformation-on-social-media-2966ad93a203.

[24] https://www.ncsc.gov.uk/threats; https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36311.htm#_idTextAnchor066

[25] RAND, “Deterring Russian Aggression in the Baltic States: What it Takes to Win,” Testimony presented before the House Armed Services Committee, Subcommittee on Tactical Air and Land Forces on 1 March 2017: https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT467/RAND_CT467.pdf; NATO, “Defence Expenditure of NATO Countries (2011-2018),” 10 Jul 2018: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_07/20180709_180710-pr2018-91-en.pdf.

[26] RAND, “Deterring Russian Aggression in the Baltic States: What it Takes to Win,” Testimony presented before the House Armed Services Committee, Subcommittee on Tactical Air and Land Forces on 1 March 2017: https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT467/RAND_CT467.pdf; NATO, “Defence Expenditure of NATO Countries (2011-2018),” 10 Jul 2018: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_07/20180709_180710-pr2018-91-en.pdf.

[27] RAND, “Deterring Russian Aggression in the Baltic States: What it Takes to Win,” Testimony presented before the House Armed Services Committee, Subcommittee on Tactical Air and Land Forces on 1 March 2017: https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT467/RAND_CT467.pdf; NATO, “Defence Expenditure of NATO Countries (2011-2018),” 10 Jul 2018: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_07/20180709_180710-pr2018-91-en.pdf.

[28] CFR, “Containing Russia, Again: An Adversary Attacked the United States—It’s Time to Respond,” 19 Jan, 2018: https://www.cfr.org/article/containing-russia-again-adversary-attacked-united-states-its-time-respond.

[29] CFR, “Containing Russia, Again: An Adversary Attacked the United States—It’s Time to Respond,” 19 Jan, 2018: https://www.cfr.org/article/containing-russia-again-adversary-attacked-united-states-its-time-respond.

Do you see a way to make this Playbook better?

Are there new technologies or vulnerabilities we should address?

We want your feedback.

Please share your ideas, stories, and comments on Twitter @d3p using the hashtag #IOplaybook or email us at connect@d3p.org so we can continue to improve this resource as the digital environment changes.

Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 John F. Kennedy Street
Cambridge, MA 02138

www.belfercenter.org/D3P