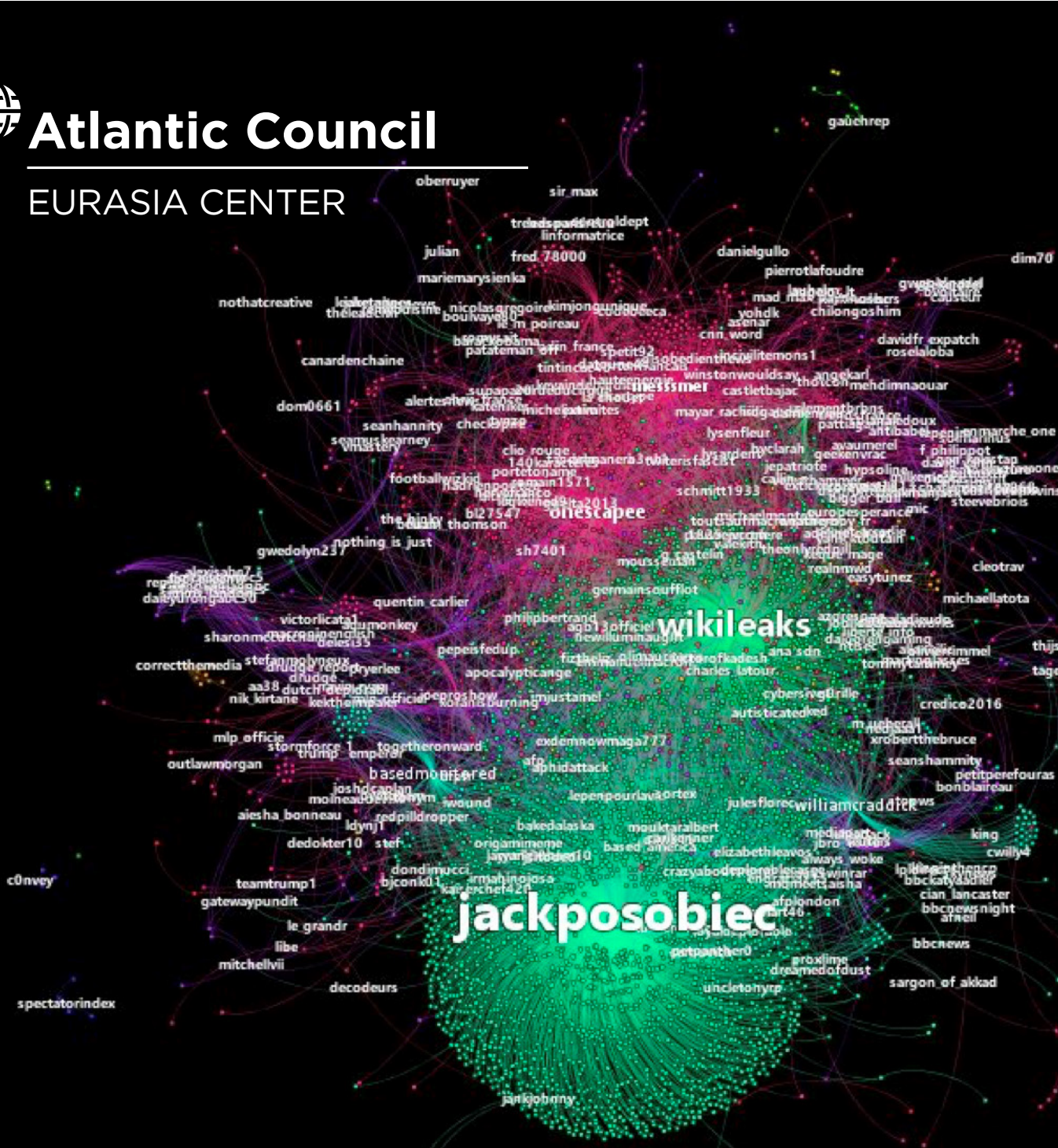
Atlantic Council

EURASIA CENTER



DEMOCRATIC DEFENSE AGAINST DISINFORMATION

Daniel Fried and Alina Polyakova

DEMOCRATIC DEFENSE AGAINST DISINFORMATION

Daniel Fried and Alina Polyakova

ISBN: 978-1-61977-530-5

Cover photo credits:

EU DISINFO LAB

This report is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The authors are solely responsible for its analysis and recommendations. The Atlantic Council and its donors do not determine, nor do they necessarily endorse or advocate for, any of this report's conclusions.

February 2018

TABLE OF CONTENTS

FOREWORD

Following Russia's interference in the 2016 US presidential campaign, "disinformation" became a topic du jour. Revelations, detailed in multiple congressional testimonies, of how the Russian government and its proxies infiltrated social-media platforms to spread false narratives and manipulate public discourse jolted the American public and policy makers to attention.

Amid important European elections in 2017, including those in France and Germany, European countries faced the same challenge of how to respond to and resist disinformation campaigns aimed against them. Since the US election, governments, multinational institutions, civil-society groups, and the private sector have launched various initiatives to expose, monitor, and get ahead of disinformation attacks. Through these efforts, the transatlantic community has gleaned three valuables lessons: The problem is broader than Russia or any single actor; a democratic response to malign influence must engage the whole of society; and we must work together to learn from each other's mistakes and successes as we craft governmental and nongovernmental strategies and solutions.

This paper is part of the broader transatlantic effort to identify democratic solutions for countering disinformation in the short term and building societal resistance to it in the long term. At this point, the transatlantic community has moved beyond acknowledging that it has a problem. Today, we need concrete solutions that can be readily implemented, tested, and refined. Rather than elaborating the details of the challenge, this paper presents a menu of options for key stakeholders: national governments, civil society, and tech companies.

In the process of writing this paper, we drew on a community of experts, practitioners, and policy makers on both sides of the Atlantic who shared their experiences, research, and ideas. Over the last year, we regularly consulted with European partners—academics, journalists, activists, government officials, and analysts—who are engaged in the debate on disinformation.

This community came together in September 2017 for StratCom DC, the first transatlantic forum on strategic communications and digital disinformation, hosted in Washington by the Atlantic Council. The event brought together more than one hundred experts from almost every European country to discuss new research and brainstorm solutions. We gathered additional feedback from Europeans at a workshop hosted by the Swedish Institute of International Affairs in Stockholm. We also benefitted from the suggestions, edits, and critiques of many colleagues, including: Franklin Kramer, Alexander Vershbow, Justin Levitt, Matt Chessen, Jakub Kalensky, Ben Nimmo, Mikael Tofvesson, and the policy teams at Facebook and Twitter. We are thankful for their time and thoughtful comments. In addition, none of this would have been possible without the operational genius and leadership of Geysha Gonzalez, associate director of the Eurasia Center at the Atlantic Council. She deserves as much credit for the realization of this paper as the authors.

We would also like to thank our funders for this endeavor: the Swedish Civil Contingencies Agency, the United Kingdom's Foreign & Commonwealth Office, the Baltic-American Freedom Foundation, and NATO.

A caveat: While writing this paper, we endeavored to update the content to reflect the constantly evolving conversation on this topic, but this issue, like the threat itself, remains a moving target. Inevitably, identifying what works—and what does not—will require trial and error, with no expectation of permanent, fixed solutions. We will need the full scope of democratic dynamism to get ahead of our adversaries.

INTRODUCTION

Caught off guard by Russian interference in its 2016 election, the United States belatedly realized something many Europeans have known for years: Russia has returned to its past practices of hostile propaganda and various forms of active measures—disinformation, political subversion, and corruption—directed against the West.

President Vladimir Putin's Russia seeks to weaken Western governments and transatlantic institutions, discredit democratic and liberal values, and create a post-truth world, with the aim of shielding Moscow's autocracy from liberal influence and easing Russia's domination of its neighbors. There is nothing new about the Kremlin's use of disinformation[1]—the intentional spread of inaccurate information to undermine public confidence—with the goal of destabilizing its opponents. But the advance of digital technology and communication allows for the high-speed spread of disinformation, via massive and unsecured points of influence. This creates opportunities for manipulation that have exceeded the ability of democratic nations to respond, and sometimes even to grasp the extent of the challenge.

Much has been written about the threat of Russian disinformation; its impact, still being evaluated, varies between countries and among audiences. While influence is difficult to quantify, disinformation can affect closely contested political campaigns and other public debates in the short run, and it can have a corrosive effect on public discourse in the longer term, especially if unchecked. In the United States, Russian disinformation around the presidential election has become a hot political issue, with congressional hearings, legislation, and changes in social-media corporate policy unfolding at a rapid pace. Russia may have developed the techniques, but malicious actors learn from one another. Disinformation tools are being deployed by other foreign entities seeking to undermine democracies. Thus, the challenge is broader than Russia, and the response should be broadly applicable.

This paper looks beyond the political context and focuses on potential methods and tools—by governments, civil society, and private businesses—for resisting disinformation operations and getting ahead of the threat by building democratic resilience. As such, it is a "menu of options," many of which still need to be tested, rather than a strategy. The policy recommendations presented are also not the only possible solutions; there is more than one way to approach the problems; institutional solutions should develop organically; and we should remain flexible and agile as we test new ideas.

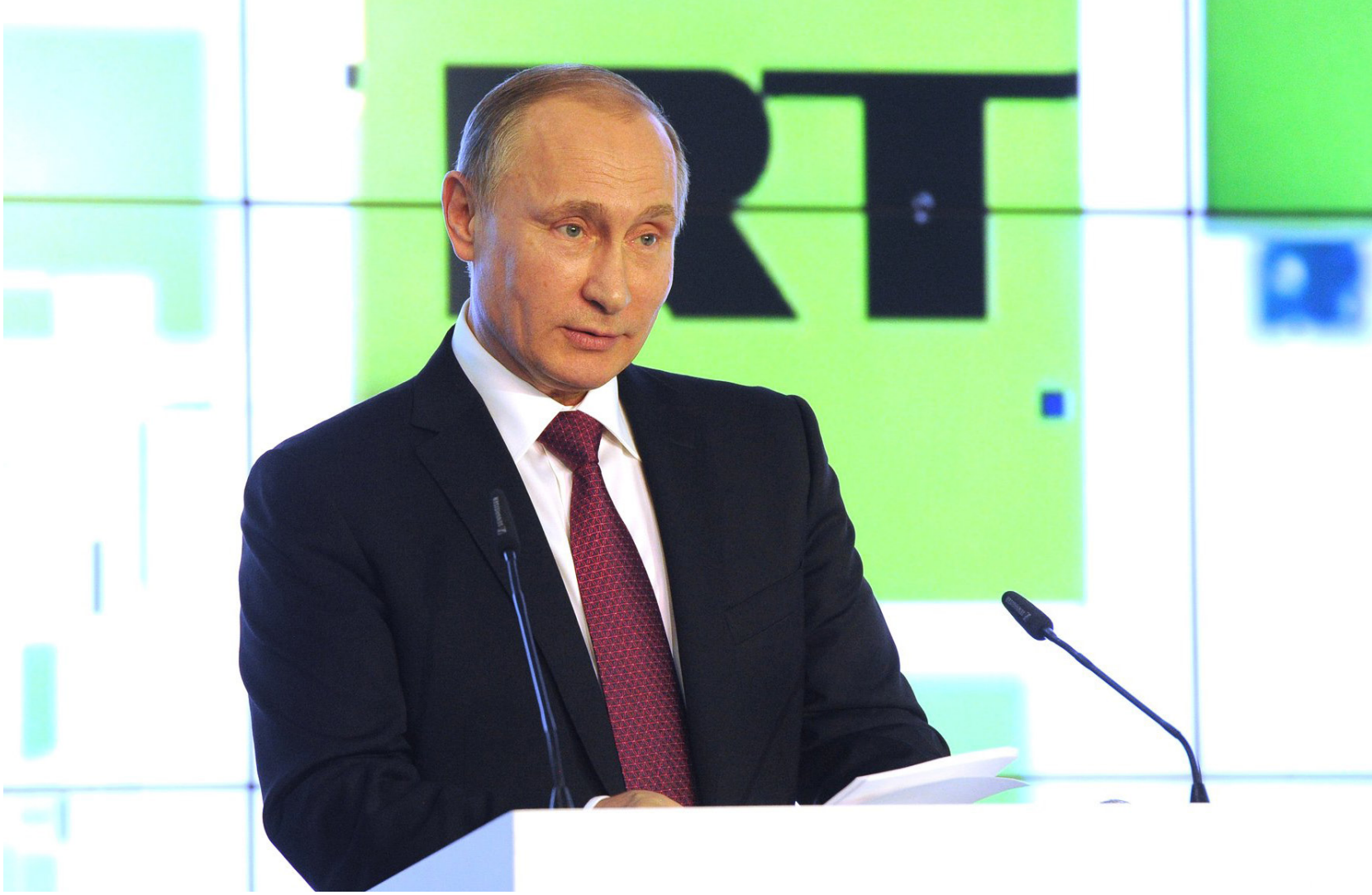
BEYOND ADMIRING THE PROBLEM

We have options. Government policy, legislation, and corresponding technical fixes can expose and limit the potential damage of foreign disinformation. So, too, can corporate commitments to norms of behavior that align with shared international security objectives. At the same time, barriers that democratic states and societies build will be imperfect. There is no one fix, or set of fixes, that can eliminate weaponization of information and the intentional spread of disinformation. Still, policy tools, changes in practices, and a commitment by governments, social-media companies, and civil society to exposing disinformation, and to building long-term social resilience to disinformation, can mitigate the problem. As technology advances and malicious actors become more sophisticated in their tactics, the window of opportunity to respond effectively is narrowing. **Now is the time for action.**

This paper outlines potential tools available to the United States and Europe. Individual countries, as well

1 *Propaganda* is a tricky term, because one person's propaganda is another person's political opinion. This paper adapts a definition from Richard Alan Nelson in his 1996 book *A Chronology and Glossary of Propaganda in the United States* (Westport, Conn. and London: Greenwood Press, 1996). Propaganda, he writes, is "a systematic form of purposeful persuasion that attempts to influence the emotions, attitudes, opinions, and actions of target audiences for ideological or political purposes through the transmission of one-sided messages (which may or may not be factual) via mass and direct media channels."

Disinformation is "false information or intentionally misleading facts communicated with the intent to deceive." Fake news is disinformation, but the term is politically loaded and not highly useful.



Russian government control of the media is essential to the Kremlin's disinformation campaign. *Photo credit: The Presidential Administration of Russia*

as the European Union (EU) and NATO, can apply these and other tools to fit their circumstances. In addition to specific suggestions, **we recommend creation of a "Counter-Disinformation Coalition," an informal group of like-minded governments and nongovernmental stakeholders,** to develop best practices for defending against disinformation—including standards for social media such as a voluntary code of conduct—and recommend responses to future challenges originating in non-democratic countries. While nongovernmental actors can and should develop coordination mechanisms and communication channels among themselves, governments must be part of the broader conversation. Public policy is a core element of an effective response.

Our responses must be consistent with our democratic values and freedoms. As we learned during the Cold War, we need not become them as we fight them. As an open system, democracy is more vulnerable in the short run to certain forms of manipulation, but it is more resilient than authoritarian systems in the longer term. As the Cold War also demonstrated, our open, democratic societies will prove an asset in countering disinformation; social resilience is going to be a better defense against influence operations in the long term.

The challenge we face is tough, but not unprecedented. We should be mindful of historic time lags in the development of social and legal norms to limit the destructive potential of new media. The introduction of the printing press; cheap, mass-circulation newspapers; and radio and television all gave tools to dictators and demagogues as well as spreading knowledge. So too with digital media. It takes time to develop legal, social, and ethical norms to limit the exploitation and manipulation of new media. We seek to shorten the time lag.

UNPACKING THE CHALLENGE

- **Overt foreign propaganda.** Countering purposeful misinformation and distortion, such as that conveyed by RT, Sputnik, and other Kremlin-linked media outlets, is relatively straightforward in concept but difficult in practice. These are not news organizations in democracies' understanding of the term, nor are they state-run but independent

media organizations like the BBC. They are arms of the Russian state no more independent than *Pravda* was during the Soviet period.

The roles of governments, civil-society organizations, private-sector tech companies, and media (traditional and digital) will differ, and the mix of actions will be different in the United States and Europe, reflecting, among other things, different legal traditions. For example, the First Amendment to the US Constitution includes protections for potentially offensive and hateful speech, whereas European countries can ban hate speech.

- **At the line: social-media infiltration.** Russian manipulation of social media utilizes unattributed political ads or officially organized bots, trolls, cyborgs (human/bot combinations), and other means of mounting and masking disinformation campaigns. Defending against it introduces complexities on a new level. The culture of social media has left that industry vulnerable to exploitation "at the line" of legality, and social-media companies have until recently denied the problem.

The Russians and other purveyors of disinformation will constantly improve their tactics; our counter-tactics therefore cannot be static.

As October 2017 Congressional hearings revealed,[2] the scope of Russian infiltration was broader, more sophisticated, and more subversive than most experts anticipated. And much activity might not have been revealed because it could not be attributed to Russia, e.g., the Internet Research Agency (IRA)—the Russian troll farm—whose role has been reported and which Congressional testimony addressed. The challenge of attribution will grow. Indeed, many savvy "entrepreneurs" have learned how to turn disinformation into a profitable business. The Russians and other purveyors of disinformation will constantly improve their tactics; our counter-tactics therefore cannot be static.

- **Below the line: cyber hacking**. Information theft, cyberattacks, and vote-manipulation attempts—"below the line" of legality—serve purposes beyond disinformation and influence operations, but they can support such operations. Leaked and hacked emails or other stolen information can be used to spin disinformation narratives to push on existing pressure points and inflame societal tensions. This was the case in the 2016 US and the 2017 French presidential elections.[3] The ease with which Russian hackers were able to use targeted phishing campaigns to acquire data useful for disinformation purposes signals that weak cybersecurity is a significant vulnerability.

OPTIONS FOR ACTION

Governments, civil society, and private companies in the United States and Europe have options and capabilities that, while individually incomplete, may collectively help reduce and manage the disinformation challenge. Democracies have space to take such steps, working within the framework of free speech and freedom of expression.

In the United States, First Amendment protections seem strongest with respect to US persons engaging in non-commercial speech. Its protections seem weaker when applied to foreign persons, especially those outside the United States. For example, current US law and regulations ban foreign persons (unless they are lawful permanent residents) from contributing to candidates or political parties; placing or financing ads in a campaign context; or engaging in other campaign-related activities, broadly understood.[4] Foreign persons may engage in issue ads (at least, that is how the law has been interpreted to date). However, American private companies are not obligated to accept paid advertisements, from either foreign or US persons.

EU/European options are broader still. The European Commission published a set of guidelines and principles to encourage social-media platforms to detect and

2 Alina Polyakova, "Social Media's Half-Measures," *American Interest,* November 5, 2017, https://www.the-american-interest.com/2017/11/05/social-medias-half-measures/.

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

4 "Who can and can't contribute," Federal Election Commission of the United States, accessed January 16, 2017, https://www.fec.gov/help-candidates-and-committees/candidate-taking-receipts/who-can-and-cannot-contribute/.

remove content that incites hate and violence. In Germany, a law enacted in October 2017 expands the government's mandate to regulate offensive speech into the online space. The Network Enforcement Act, or NetzDG, as the measure is widely known, includes an expansive provision for regulating "ambiguous" context beyond obvious hate speech. French President Emmanuel Macron has announced that he will seek legislation to curb the spread of misinformation during elections.

ROLE OF GOVERNMENTS

UNITED STATES

- **The United States should label foreign state propaganda organs for what they are.** Given First Amendment protections and traditions, the US government should not attempt to ban RT, Sputnik, and the like. But the United States (and other democracies) should properly identify the Russian networks as propaganda vehicles. The US Department of Justice (DOJ) has already taken the first step by requiring RT to register under the Foreign Agent Registration Act (FARA).[5] The department announced on November 13, 2017, that RT's US-based operating company, T&R, had filed under FARA. However, FARA enforcement has been notoriously difficult.
  - Legislation before the US Congress would grant greater powers to DOJ to investigate FARA violations, improve compliance, and enforce the act.[6] For example, Congress can grant to DOJ units such as the National Security Division civil investigative authority to compel production of records from potential and current registrants. Congress should also update the definition of "information materials" to account for the digital age. DOJ may also need to update its public guidance on FARA.[7]
  - We are skeptical about complaints that FARA registration has triggered a cycle of retaliation from the Kremlin. Putin's government has, for some years now, been using the label "foreign agents"—a term with sinister, even lethal historical connotations in a Russian context—to attack civil-society groups.

Information sharing between social-media platforms and the intelligence community is crucial for identifying emerging threats.

- **The US government should actively monitor overt foreign propaganda narratives and inform the public on their content.** In the United States, the State Department's Global Engagement Center (GEC) received a new mandate in the 2016 National Defense Authorization Act to counter state-sponsored propaganda, with its mission focused beyond US borders.[8]
  - In its expanded capacity, the GEC should act primarily as a funder of independent research, investigative journalism, and civil-society efforts to counter state-funded disinformation attempts in allied states (EU and NATO). The GEC should also act as a coordinator and convener of civil-society and academic endeavors in the United States and Europe. It should serve as the point of contact for European StratCom teams.
  - Congress should increase funding to the GEC beyond the $40 million currently appropriated to support counter-disinformation civil-society initiatives abroad.
- Information sharing between social-media platforms and the intelligence community is crucial for identifying emerging threats. **The US government should establish an office that would serve as the point of contact for private-sector companies with respect to such information.**

5 FARA dates from 1938 and was designed to apply to Nazi propaganda organs operating in the United States; it was later applied to TASS, the Soviet news agency. FARA requires public disclosure of income sources and certain expenditures, but it does not restrict the right to publish or broadcast.

6 Senate Judiciary Committee, "Disclosing Foreign Influence Act: Summary of Legislation," October 31, 2017, https://www.judiciary.senate.gov/imo/media/doc/FARA,%2010-31-17,%20Disclosing%20Foreign%20Influence%20Act%20-%20Summary.pdf.

7 Elena Postnikova, "Agent of Influence: Should Russia's RT Register as a Foreign Agent?," Atlantic Council, August 2017, http://www.atlanticcouncil.org/images/publications/RT_Foreign_Agent_web_0831.pdf. Our recommendations for revising FARA are adapted from this report, which includes additional, specific suggestions.

8 "National Defense Authorization Act for Fiscal Year 2016," United States Congress, November 25, 2015 https://www.gpo.gov/fdsys/pkg/PLAW-114publ92/pdf/PLAW-114publ92.pdf.

President Obama visits the National Cybersecurity and Communications Integration Center on January 13, 2015. Photo credit: Department of Homeland Security

This coordination office should liaison and share information with **the Office of the Director of National Intelligence (ODNI), the Department of Homeland Security (DHS), the GEC, and appropriate Congressional oversight committees.**

  - The office could be housed within DHS and modeled on the Information Sharing and Analysis Centers (ISACs) established at federal request by different industry sectors to cooperate with DHS on cybersecurity and protection of critical infrastructure.[9] The coordination office would be primarily responsible for information sharing between the private sector, Congress, and relevant government agencies. It would not necessarily be responsible for implementation or operations.

- To design, plan, and coordinate operational activities at the interagency level, the president should follow the recommendation of a January 2018 report by the Senate Foreign Relations Committee's Democratic staff and "**establish a high-level interagency fusion cell, modeled on the [US government's] National Counterterrorism Center (NCTC**)."[10]

  - This "National Counter-Disinformation Center" would include representatives from the Federal Bureau of Investigation, the Central Intelligence Agency, the aforementioned DHS information coordination office, the Department of Defense, the GEC, and other relevant agencies. As with the NCTC, it would share analysis and intelligence across the US government. The head of the center should be empowered with the mandate and the necessary budget to implement operational activities. He/she should also be appointed as a senior rank of undersecretary or higher. The head would

9 "About ISACs," National Council of ISACs, https://www.nationalisacs.org/about-isacs.

10 Bob Corker et al., "Putin's Asymmetric Assault on Democracy in Russia, and Europe: Implications for US National Security," US Senate Committee on Foreign Relations, January 10, 2018, https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf.

report to the head of ODNI as well as the president.

  - The center would likely be far smaller than the NCTC but would serve the same interagency coordinating function at the operational level.

- **The US government should upgrade and restructure its media arm for the digital age.** During the Cold War, Voice of America (VOA) and Radio Free Europe/Radio Liberty (RFE/RL) were more trusted within the USSR for their independent reporting than were the Soviet state media. Since 2014, RFE/RL, in cooperation with VOA, has operated Current Time, a Russian-language news network.[11] These media vehicles need to be buttressed with sufficient funds and updated to function in a digital environment. This may include restructuring the Broadcasting Board of Governors (BBG), which oversees the two agencies; reallocating resources within VOA toward online rather than traditional broadcast media; and an aggressive social-media push to increase these entities' digital impact.
  - Congress should allocate more resources for RFE/RL to disseminate local-language content in Central and Eastern Europe through RFE/RL's Prague offices.
  - Congress should also task the BBG with developing a strategy for VOA focused on digital and online content.

- **Legislation and regulation can be applied to political and issue ads generated by Russia and other authoritarian sources.**
  - **We recommend enacting the Honest Ads Act.** This bipartisan measure sponsored by senators John McCain, Amy Klobuchar, and Mark Warner would extend disclosure requirements for political and issue ads to social media, matching standards for other media.[12] The distinction between political/campaign ads, prohibited for foreign persons, and permitted issue ads has in practice opened the door to Russian use of social-media ads for disinformation purposes.
    - The Honest Ads Act seeks to address this problem by requiring social-media companies to make reasonable efforts to prevent foreign persons from engaging in any campaign-related communication activities, including ads. By making companies liable should they provide a platform for illegal foreign expenditures aimed at influencing US elections, the act seeks to discourage such firms from accepting Russian-origin issue ads with a political purpose.

The US government, in coordination with Europe and the G7, should impose financial sanctions on malign cyber actors that undermine democratic institutions and their supporters.

    - Expanding the definition of prohibited campaign ads to include issue ads in campaign contexts could extend the scope of this measure. While it is difficult for social-media platforms to distinguish between political ads and issue ads, social-media firms should clearly identify the sponsors and funders of all content. Such labels should appear directly in the newsfeed rather than asking the user to click through an ad to see its source.[13]
    - To be effective, the legislation should include provisions for enforcement by

11 "Current Time Network Launches Real News, for Real People, in Real Time," Broadcasting Board of Governors, last updated February 6, 2017, https://www.bbg.gov/2017/02/06/current-time-network-launches-real-news-real-people-real-time/.

12 "Warner, Klobuchar, McCain Introduce Legislation to Improve National Security and Protect Integrity of U.S. Elections by Bringing Transparency and Accountability to Online Political Ads," Office of Senator Mark R. Warner, October 19, 2017, https://www.warner.senate.gov/public/index.cfm/2017/10/klobuchar-warner-mccain-introduce-legislation-to-improve-national-security-and-protect-integrity-of-u-s-elections-by-bringing-transparency-and-accountability-to-online-political-ads.

13 In October 2017, Facebook announced that it is rethinking its ads policy to make advertising more transparent. Joel Kaplan, "Improving Enforcement and Transparency of Ads on Facebook," Facebook, October 2, 2017, https://newsroom.fb.com/news/2017/10/improving-enforcement-and-transparency/.

expanding and funding Federal Election Commission authority.

  - **We recommend expanding ad-disclosure regulations** to require that the chief donors to organizations sponsoring political or issue ads be named. An ad-sponsor group called Americans for Puppies might appear in a different light if its chief donors were identified as Putin cronies. (Attribution will remain a problem. This measure, like other recommendations, is no cure-all.)

- US and European governments should develop regulations to **prevent front companies from registering URLs nearly identical to those of known media** so as to confuse readers, e.g., a Russian-controlled site mimicking the *New York Times* with a small change in the URL (www.nytimess.com rather than www.nytimes.com). These impersonation sites should also be treated as malware by the providers.

- **The Department of State should develop, in coordination with US embassies abroad, a 24/7 warning system to track online disinformation campaigns that threaten US national-security interests.** This should include metrics to determine when direct response to disinformation is needed; embassies and the State Department should choose their battles.

The EU should require all member states to provide a seconded national expert to the East StratCom Task Force.

- **The US government, in coordination with Europe and the G7, should impose financial sanctions on malign cyber actors that undermine democratic institutions and their supporters**. Existing US legal authority to do so, via vehicles such as Executive Order 13757,[14] issued by President Obama in late 2016, and the Countering America's Adversaries Through Sanctions Act,[15] overwhelmingly passed by Congress in July 2017, could be expanded through additional executive orders.

  - Potential targets for financial sanctions include Russian bot factories and troll farms for which requisite evidence of interference exists, and persons and entities financing them, including banks, Kremlin cronies, and cut-outs or proxies often used in such Russian operations.

  - Among other things, sanctions designations would chill such entities' ability to engage in business with social-media companies. Sanctions will have to be carefully tracked and updated to account for evasion tactics, such as the use of shell companies.

EUROPE

European governments may have more options with respect to foreign propaganda organs such as RT and Sputnik.

- **Where possible, EU members and other states should apply impartiality and accuracy standards.**

  - For example, the United Kingdom's (UK's) Broadcasting Act 1990 requires impartiality and accuracy in news broadcasts. Violators can face financial penalties. Although fines are rare, the reputational damage of being found guilty of violations by UK broadcasting regulator Ofcom—as RT has been, repeatedly—might deter disinformation. Such regulation, which focuses on the content of individual broadcasts rather than the broadcaster itself, appears to be a more promising route than legislation to ban certain outlets. The aim should be to expose malpractice so that viewers can identify and (hopefully) ignore it.

  - Lithuania and Latvia have repeatedly fined Russian state-run outlets for reporting false information; the fines are small but publicized. Latvia has also promoted independent Russian-language media by hosting Meduza, an online outlet founded by independent Russian journalists in exile.

14 "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities," Federal Register, January 3, 2017, https://www.federalregister.gov/documents/2017/01/03/2016-31922/taking-additional-steps-to-address-the-national-emergency-with-respect-to-significant-malicious.

15 "HR 3364 - Countering America's Adversaries Through Sanctions Act," Congress.gov, August 2017, https://www.congress.gov/bill/115th-congress/house-bill/3364/text.

Heiko Maas, German Minister of Justice and Consumer Protection, and architect of Germany's NetzDG law. *Photo credit: A. Savin.*

- **EU member states should tread carefully when considering legislation aimed at regulating online content so as not to slip into censorship.** Germany's NetzDG law requires social-media platforms to remove hate-speech content within twenty-four hours of receiving complaints (seven days in cases of more ambiguous content) or face fines of up to 50 million euro. At the time of writing, no specific information on France's potential anti-"fake news" law was available, but Macron's vague announcement received early criticism for potentially encroaching on free expression.

- **The EU and NATO, in coordination with national governments, can play a direct role in countering Russian propaganda organs.** The EU's East StratCom Task Force, NATO's StratCom Center of Excellence, and similar bodies established by national governments (including Lithuania, Latvia, Finland, Estonia, the United Kingdom, Sweden, the Czech Republic, and Germany) have launched official counter-propaganda and counter-influence operations. The East StratCom team has become both a data hub, collecting and sharing information about disinformation, and a means of leveraging national efforts and raising awareness of the problem. NATO's StratCom Center has engaged in analytical work concerning Russia's disinformation methodology, while NATO's Public Diplomacy Division debunks misinformation mainly about NATO activities. However, all these bodies, and the EU East StratCom team in particular, remain under-resourced and under pressure, with full potential yet to be realized; it needs both autonomy to act within its charter and political support.

- **The European Commission and European Parliament should:**

  - **Continue to fund East StratCom through the EU budget** (at a minimum of 1.1 million euro per year, as stipulated in the 2018–20 budget). The EU should also expand the East StratCom mandate to include all member states.

    - The EU should require all member states to provide a seconded national expert to the East StratCom Task Force.

  - **Similarly, NATO should continue to support the StratCom Center of Excellence in Riga**. NATO should also consider establishing a second center in Europe's south, which would focus on identifying emerging threats in NATO's southern flank.

- **The European Commission's new High-Level Group (HLG) on fake news and online disinformation should, as a first order of business, assess existing governmental efforts to counter disinformation and produce a set of proven best practices.** As part of its advisory function to the commission, the HLG is tasked with assessing the "effectiveness of the voluntary measures put in place by online platforms and news media" to counter disinformation. By including tech companies as HLG members, the group has the potential to serve as a bridge between the EU and the private sector.[16]

  - The HLG's assessments should be made publicly available.

- **Public-diplomacy sections in European and US embassies should intensify efforts to counter false information online, both by exposing falsehood**

16 "Experts Appointed to the High-Level Group on Fake News and Online Disinformation," European Commission, last updated January 12, 2018, https://ec.europa.eu/digital-single-market/en/news/experts-appointed-high-level-group-fake-news-and-online-disinformation.

and by opening a "firehose of truth" through their own social-media channels and (even more effectively) by supporting independent local civic groups engaged in such innovative efforts (e.g., StopFake in Ukraine).

  - The aim should be to inoculate audiences against disinformation as well as to counter examples of it. Washington should hold the reins loosely: Domestic US government offices can provide support, but embassies and regional media hubs will need latitude and resources to act in real time.

- Restricting foreign ownership of media in general is an unattractive option, because it can be abused to weaken independent media to the advantage of government-favored (and government-favoring) domestic state media. However, the United States and Europe could consider limits on foreign media ownership, or on control by persons from countries that lack democratic standing or media freedom, as determined by Freedom House, Reporters Without Borders, or other independent assessors.

Print, television, and radio outlets and civil-society groups should educate editors and reporters on how to quickly identify suspected disinformation.

ROLE OF CIVIL SOCIETY

- **Civil society can be faster and more effective than most governments in identifying, countering, and discrediting Russian propaganda.**

  - **Tech-savvy civil-society groups** such as StopFake, the Atlantic Council's DFR Lab, the Alliance for Securing Democracy's Hamilton 68, and Baltic Elves have shown an ability to identify prominent Russian troll/bots/cyborgs and, more important, to expose significant campaigns run by them. The initial tools are not perfect, but over time they will get better.

  - **Such "bot/cyborg hunters" should expose such activities in as close to real time as possible and inform social-media companies of the technical details**. However, they will need to exercise judgment as to the timing and manner of exposure to avoid amplifying bad tweets or posts.

  - **Governments and social-media firms alike should fund such civil-society efforts,** including research, bot/cyborg hunting, and independent investigative journalism.

    - Social-media companies should give researchers and bot/cyborg hunters access to data to help them identify vulnerabilities in social-media platforms and expose Russian and other covert infiltration**.** The Defending Digital Democracy effort from the Belfer Center at Harvard University is one example of research in this space, which Facebook has sponsored.

    - **Civil society and academia should support development of open-source standards for sharing information on malicious actors and their activities.**

- Traditional media and high-impact online "influencers" are often the target of disinformation campaigns. **Print, television, and radio outlets and civil-society groups should educate editors and reporters on how to quickly identify suspected disinformation**.

ROLE OF THE PRIVATE SECTOR

Social-media companies should not and cannot be the "arbiters of truth," but they have a responsibility to prevent and get ahead of malicious manipulation of their platforms, and options available to this end.

- **Traditional media organizations should identify content originating from propaganda organs such as RT and Sputnik and treat their output as intrinsically suspect.** Journalists and researchers should explicitly label propaganda and questionable sources in their reporting (e.g., "the Russian propaganda outlet RT" rather than "the Russian news organization RT").

- Attribution of foreign, politically motivated social-media infiltration will be both a challenge and a moving target. We do *not* recommend prohibitions on placing RT- and Sputnik-created stories. **However, tech companies—Twitter, Facebook, Google, and others, and in some areas internet service providers (ISPs) such as Verizon, ATT, and non-US ISP firms—can and should take steps to limit the effects of disinformation.**

  - **Identify and label the likes of RT and Sputnik as Russian propaganda organs and their material as propaganda.** This would be a transparency measure, not a restriction on their ability to broadcast. RT's and Sputnik's registration under FARA would give social-media companies a basis to label their content.

  - **"Mute" content from automated accounts** to prevent such content from appearing on newsfeeds or influencing trending topics or trending news. Distinct from deleting such accounts, muting serves much the same function as "de-ranking," which Google recently took steps to do to RT and Sputnik.[17]

  - **Experiment with labeling automated and fake accounts** in a limited manner, and test reaction among users and those who control the bots (i.e., will operators simply delete the accounts once they are labeled and start new ones?). Facebook's initial experiment with labeling content as "disputed" was unsuccessful, as users interacted with such content *more* when it was labeled.[18] This suggests that social-media companies need to better understand the emotional and psychological appeal of disinformation and further refine experiments.

  - **Redesign Facebook, Google, and Twitter algorithms to better identify "credible" versus "weak" content** based on transparent metrics, such as third-party independent reference points for media quality (e.g., the Stanford Web Credibility Project) and site longevity (an indicator for pop-up disinformation sites). Weak content should be demoted or muted. Credible content, as determined by a clear set of metrics including user feedback, should be prioritized.[19]

  - **Be active in identifying troll and impersonation accounts and shutting them down**.

  - **Limit dissemination of known propaganda outlets such as RT/Sputnik** (but again, do not ban them). More generally, social media should introduce more transparency into how their algorithms work and why the algorithms favor some content over other.

    - Google rankings could be smarter about pushing down fabrications and propaganda content in search results. (Such steps, e.g., Google's de-ranking of RT and Sputnik, would have temporary value, as the Russians would find other ways of disseminating information.)

The norm of free speech does not require allowing commercial relations with foreign propaganda organs.

  - **Revise advertising policies to ban ads from known propaganda outlets.** The norm of free speech does not require allowing commercial relations with foreign propaganda organs. Twitter has already taken this step. Google could do the same for its AdSense program. **Alternatively, companies could accept such ads, but with prominent labels to disclose their origin and/or FARA status**.

    - **Funders of ads on social-media platforms should be identified prominently, directly in the newsfeed, rather than requiring the user to click through an ad to see the**

17 Alex Hern, "Google plans to 'de-rank' Russia Today and Sputnik to combat misinformation," *Guardian*, November 21, 2017, https://www.theguardian.com/technology/2017/nov/21/google-de-rank-russia-today-sputnik-combat-misinformation-alphabet-chief-executive-eric-schmidt.

18 Catherine Shu, "Facebook will Ditch Disputed Flags on Fake News and Display Links to Trustworthy Articles Instead," *Tech Crunch*, last updated December 20, 2017, https://techcrunch.com/2017/12/20/facebook-will-ditch-disputed-flags-on-fake-news-and-display-links-to-trustworthy-articles-instead/.

19 In January 2018, Facebook announced that it will begin testing prioritizing content that Facebook users rate as more trustworthy. As the company undertakes this effort, it should be cautious to ensure that the ranking system is not vulnerable to manipulation. Adam Mosseri, "News Feed FYI: Helping Ensure News on Facebook is From Trusted Sources," Facebook, January 19, 2018, https://newsroom.fb.com/news/2018/01/trusted-sources/.

funding source. The click-through rate for most paid content is notoriously low. Users should be able to easily identify the funders of content that appears in their newsfeeds.

» **Companies in this sector should restructure targeting tools available to foreign advertisers** to limit micro-targeting of users where it could be deployed in a political and campaign context. For example, advertisers should not be able to cross-reference social-media users' political attitudes with district-level geographic data.

– **Limit dissemination of social-media content by bots and cyborgs,** either by blocking them outright or labeling them. (This may have an impact on domestic commercial and other uses of bots and cyborgs. Nevertheless, the principle of transparency suggests a practice of labeling.)

- **Social-media companies, operating independent of governments, should supplement algorithmic review with a human editorial element in the content review process.** Artificial intelligence tools can identify extremist or violent content but are limited in their ability to flag ambiguous malicious content. Given the large amount of content posted on social-media platforms, managing scalability and ensuring user privacy will be challenging. One solution is to establish de facto editorial departments staffed with regional experts who could review randomly selected anonymized content.

Winning the new information war will require a whole-of-society approach. Top-down will not work...

- **Disinformation often appeals to human emotions and exploits human psychology.** Private-sector firms that act as content publishers and content filters (social media and others) should fund research that examines the "demand" side of disinformation—e.g., why some messages are more appealing than others, why some go viral while others do not, and how to counter such messaging with truthful content that has comparable emotional appeal.

- **In practice, many of these steps may affect domestically generated bots and cyborgs.** Freedom of expression needs to be considered and respected. Nevertheless, the principle of transparency and a general rule of "a human behind the keyboard," should give space for social-media firms and other tech companies to take the steps we have recommended and other similar ones.

TOOLS OF LONG-TERM RESILIENCE

While measures to block and constrain disinformation will help, there is no perfect shield. As digital and cyber technologies such as artificial intelligence, machine learning, and automation evolve, the speed and efficiency of influence operations will increase, and the expense will drop. The tools of information influence, initially pioneered by state actors, are already available to anyone or any group to deploy at a low cost. This "democratization" of influence operations, coupled with democratic vulnerabilities, means that societies need to invest in resilience as well as resistance. Winning the new information war will require a whole-of-society approach. Top-down will not work: Governments are likely to lack the technological sophistication of social-media companies and the operational skill of civil-society "bot/troll hunters."

Successful disinformation operations work because they exploit cognitive vulnerabilities common to human beings and use these to target specific communities. They do so quickly, at a large scale, and with increasing automation. Existing and emerging tools are enhancing the precision and persuasiveness of technologically-driven propaganda and disinformation. Beyond efforts to block, label, and squeeze sources of disinformation, governments (including the intelligence community), civil society, and industry also have opportunities, and responsibilities, to help their respective societies defend themselves from "cognitive hacking" by foreign actors. At a more traditional level, and beyond the scope of this study, democratic societies need to develop narratives that are simultaneously true and persuasive.

Governments, civil-society groups, industry, and media should raise social awareness about how disinformation works and how to identify and expose it.

- **Like-minded governments should establish mechanisms for consistent sharing of information, best practices, and risk-assessment guidelines,**

such as the proposed "Counter-Disinformation Coalition" outlined below.

- **National governments, along with the EU and NATO, should implement internal training and education courses for civil servants, election officials, and diplomats on how to identify disinformation, reduce its spread, and report it internally.**
  - Within governments, services that have familiarity with "psychological operations" should help educate other public-sector employees on these strategies.
- **Civic-education and media-literacy courses should be a driving force in the West's response to disinformation.** Possibilities will vary widely among countries, but sharing standards can help create common ground for supranational responses and make it harder for foreign actors to divide allied states and communities within nations.
  - Public education campaigns, ranging from statements by political leaders to public-service announcements, should be widely practiced.
  - Education should include a focus on digital literacy, including the ability to think critically about online and social-media content.
    - » While it is difficult to mandate national educational standards of any kind in the United States, "coalitions of the willing" can lead to wider digital solidarity. If backed by resources, these coalitions can, over time, raise the level of digital literacy and sensitivity to manipulation.
    - » Ongoing revelations about Russian disinformation could generate a national inflection point—a contemporary version of the "Sputnik moment" in 1957, which provided political energy for a generation of science and math education in the United States.
    - » There are examples to consider. Finland's strong education system, paired with its government's acknowledgement of the information war, is often credited with reducing the effect of disinformation campaigns within the Finnish population. Similar efforts have sprouted throughout Europe. Most recently, Italy included media literacy as part of its high-school curriculum to help students be critical news consumers.
- **Civil-society groups and tech firms should reach out to local communities to offer courses and workshops at schools, community colleges, and universities.**
  - Social-media firms should support media literacy programs and civic education programs. Some firms have already invested in partnerships with universities and schools of journalism.[20] But much more needs to be done at every level of the education system.

Ongoing revelations about Russian disinformation could generate a national inflection point…for a generation of science and math education in the United States.

THE COUNTER-DISINFORMATION COALITION

The scope of the challenge is broad and evolving, demanding commitment by governments, societies, and private companies on both sides of the Atlantic. No one's recommendations are likely to be complete. However, the current high level of attention might provide an opportunity to lock into place both strong policies and habits of consultation. The various initiatives already in play—the European Center of Excellence in Countering Hybrid Threats, for example—cannot carry the policy and political burdens on their own.

We recommend that the United States and the EU establish a public/private group, bringing together on a regular basis like-minded national government and nongovernmental stakeholders, including social-

20 Áine Kerr, "Improving New Literacy Through Collaboration," Facebook, March 2, 2017, https://media.fb.com/2017/03/02/improving-news-literacy-through-collaboration/.

media companies, traditional media, ISP firms, and civil society.

- **This Counter-Disinformation Coalition would develop, share, and recommend, in non-binding fashion, best practices for confronting disinformation originating from non-democratic countries, now and in the future, consistent with democratic norms. It would address issues such as:**
  - transparency;
  - procedures to identify and label bots, trolls, and cyborgs;
  - identification and labeling of overt propaganda; and
  - issues of free speech and general internet freedom in this context.
- It would also offer tools, information, civic-education programs, and other knowledge to developing countries, which are frequently the target of domestic and international disinformation campaigns.
- Tech companies and civil society groups should continue to coordinate and share best practices outside the coalition.
- **The coalition would start by developing a voluntary code of conduct outlining principles and some agreed procedures for dealing with disinformation.**
  - Recent precedent exists: In 2016, EU- and US-based social-media companies agreed on a voluntary code to combat hate speech.[21]
  - A counter-disinformation code of conduct could, for example:
    - » outline responsibilities for media and social-media companies to deal with abuse of their platforms by trolls, bots, cyborgs, and other threats from outside, non-democratic actors such as Russia;
    - » outline best practices for transparency;
    - » set standards for disclosing ads and issue ads being pushed by propaganda arms of non-democratic governments;
    - » recommend best practices for identifying and exposing bot/troll/cyborg campaigns directly or indirectly supported by non-democratic governments;
    - » generate political and financial support for official organizations and civil-society groups skilled at exposing and countering disinformation;
    - » develop risk-assessment metrics for when an official response to a disinformation campaign is warranted—not all disinformation needs to be countered;
    - » and develop best practices to increase social resilience in the face of disinformation.
  - The principles and recommendations should reflect the practical complexity of distinguishing between domestic and foreign-origin bots and trolls.
  - **The Counter-Disinformation Coalition would meet on a regular basis; issue updates, informal guidelines, and recommendations; and monitor implementation of the agreed principles in the code of conduct.**
  - **The Coalition should remain flexible and primarily serve as a platform for regular discussions by core stakeholders.** We do not recommend a highly structured top-down organization. Rather, a democratic response to foreign malign influence will and should be organic and bottom-up.
  - Social-media companies that have resisted oversight may now be more amenable to such an initiative, given revelations about their role as unwitting instruments of Russian disinformation operations. **The United States, the EU, and individual governments should collectively use their leverage to bring social-media firms to the table on a sustained basis.**

21 "Code of Conduct on Countering Illegal Hate Speech Online," European Commission, accessed January 16, 2018, http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf.

CONCLUSION

We regard the recommendations above—near-term steps to resist and restrict disinformation; investment in long-term tools of resistance; and an ongoing consultative mechanism for like-minded governments, civil society, and the private sector—as a menu for democratic countries and a platform for further work. Russia's aggressive use of disinformation has drawn immediate attention to the challenge, but Russia is merely a pioneer. The problem will grow.

We are realistic about the efficacy of our own (and others') recommendations. The challenge of disinformation is evolving and complex; no one set of actions can eliminate it. Moreover, measures to counter disinformation will raise questions of freedom of expression. We do not recommend trading off freedom for security. Rather, we have tried to identify steps that can be effective while respecting the values we seek to protect.

We believe that democratic societies may be at a short-term disadvantage in contending with propaganda and demagogues, but history demonstrates that they have longer-term advantages, especially when supported by tools of transparency, fair (and limited) regulation, and an active civil society.

ABOUT THE AUTHORS

DR. ALINA POLYAKOVA

David M. Rubenstein Fellow - Foreign Policy, Center on the United States and Europe
Brookings Institution

Dr. Alina Polyakova is the David M. Rubenstein Fellow in the Foreign Policy program's Center on the United States and Europe at the Brookings Institution and Professor of European Studies at the Paul H. Nitze School of International Studies at Johns Hopkins University. She is the editor and co-author of the Atlantic Council's report series, *The Kremlin's Trojan Horses*, which examines Russian political influence in Western Europe. Dr. Polyakova specializes in Russian foreign policy, European politics, and far-right populism. Her recent book, *The Dark Side of European Integration* (ibidem-Verlag and Columbia University Press, 2015) examines the rise of far-right political parties in Western and Eastern Europe. She has also written extensively on Russian political warfare, Ukraine, and transatlantic relations for the *New York Times, Wall Street Journal, Foreign Affairs, Foreign Policy*, and the *American Interest*.

Prior to joining Brookings, Dr. Polyakova served as director of research and senior fellow for Europe and Eurasia at the Atlantic Council. She is a term member of the Council on Foreign Relations and a Swiss National Science Foundation senior research fellow. She has also been a fellow at the Fulbright Foundation, Eurasia Foundation, Woodrow Wilson International Center for Scholars, National Science Foundation, Social Science Research Council, International Research and Exchanges Board (IREX), and a senior research fellow and lecturer at the University of Bern. Dr. Polyakova holds a doctorate from the University of California, Berkeley.

AMBASSADOR DANIEL FRIED

Distinguished Fellow, Future Europe Initiative and Eurasia Center
Atlantic Council

Ambassador Daniel Fried is a distinguished fellow with the Atlantic Council's Future Europe Initiative and Eurasia Center. Ambassador Fried has played a key role in designing and implementing US policy in Europe after the fall of the Soviet Union. Prior to joining the Atlantic Council, Ambassador Fried served as the US Department of State's coordinator for sanctions policy from 2013 to 2017. Previously, he served as special envoy for the closure of the Guantanamo detention facility and was assistant secretary of state for European and Eurasian affairs under the Bush Administration, as well as special assistant to the president and senior director for European and Eurasian affairs at the National Security Council. From November 1997 until May 2000, he served as ambassador to Poland, where he had developed much of his earlier career. Ambassador Fried has focused on designing and implementing US policy to advance freedom and security in Central and Eastern Europe, NATO enlargement, and the Russia-NATO relationship. Ambassador Fried holds a BA with magna cum laude honors from Cornell University and earned his MA at Columbia University's School of International and Public Affairs.

Atlantic Council Board of Directors

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org