BROOKINGS

United States House Committee on Appropriations – Subcommittee on State, Foreign Operations, and Related Programs

United States Efforts to Counter Russian Disinformation and Malign Influence

July 10, 2019

Dr. Alina Polyakova
Director, Global Democracy and Emerging Technology
Fellow, Center on the United States and Europe
Foreign Policy Program
Brookings Institution

Dear Chairwoman Lowey, Ranking Member Rogers, Distinguished Members of the Subcommittee:

It is an honor and privilege to address you today on this important issue. Thank you for inviting me to testify.

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.[1] Russian disinformation campaigns aim to amplify existing social divisions and further polarize democratic societies. As such, they don't stop when the ballot box closes. Elections may provide an ideal high-impact opportunity for a disinformation actor, but the barrage of disinformation against Western democracies, including the United States, continues between election cycles.

The spread of disinformation to undermine public confidence is one critical tool in the Kremlin's broader tool-kit of malign influence, which also includes cyber-hacking, illicit finance, support for radical movements and parties, and the use of economic warfare, primarily through energy exports. Disinformation, as a tool of Russia's political warfare, is not new. During the Cold War, the Soviet Union's main intelligence agency, the KGB, routinely carried out disinformation campaigns against the United States and our allies. *Dezinfomatsiya,* as it is called in Russian, was part and parcel of Soviet active measures aimed at shaping the outcome of global events of interest to the Kremlin.

For example, in the 1980s, the KGB ran a disinformation campaign called "Operation Infektion" to plant the idea that the CIA invented the AIDS virus as part of a biological weapons program. A news story was first planted in a small Soviet controlled paper in India. It was then disseminated by Soviet outlets in the Soviet Union and globally, eventually infiltrating Western media including in the United States. The Soviet Union eventually dropped the story in the late 1980s after the Reagan Administration made

[1] Alina Polyakova and Daniel Fried, "Democratic Defense Against Disinformation," (Washington, DC, United States: Atlantic Council, February 2018), https://www.atlanticcouncil.org/images/publications/Democratic_Defense_Against_Disinformation_FINAL.pdf.

countering and exposing Soviet disinformation an explicit part of U.S. policy. Eventually, Mikhail Gorbachev, who was seeking better relations with the West at the time, reportedly apologized to President Reagan for promoting the conspiracy theory, which undermined U.S. diplomatic efforts in the global south and damaged the U.S. image globally. The entire disinformation cycle for Operation Infektion, from initial plant to global spread and eventual end, took approximately five years.

Today, what used to take years, takes minutes. The advance of digital technology and communication allows for the high-speed spread of disinformation, rapid amplification of misleading content, and massive manipulation via unsecured points of influence. This digital ecosystem creates opportunities for manipulation that have exceeded the ability of democratic nations to respond, and sometimes even to grasp the extent of the challenge.

Russia's democratic and pro-Western neighbors—especially Ukraine, Georgia, and the Baltic states—have contended with Russian disinformation attacks for years. Other targets of state-sponsored disinformation campaigns—the United States and some Western European countries—woke up late to the challenge, with the United States doing so only after the 2016 presidential election. Indeed, the Russian disinformation attack on the United States was part of a long-standing pattern of Russian political warfare honed in Eastern Europe and later deployed against the West, of which the United States was another target and victim. As a result, Western democracies have learned that the very principles and values of open societies—plurality, freedom of speech, independent media—are also vulnerabilities that can be exploited by malign actors for their advantage.

One positive consequence of Russia's brazen interference in the U.S. elections has been that it has served as a wakeup call to Western democracies in Europe and North America. Since 2016, European governments, the European Union, Canada, and the United States have moved beyond "admiring the problem" and have entered a new "trial and error" phase, testing new policy responses, technical fixes, and educational tools for strengthening resistance and building resilience against disinformation. As these efforts progress, four insights have emerged:

1. There is no silver bullet for addressing the disinformation challenge. Governmental policy, on its own, will not be enough. The private sector, specifically social media platforms, and civil society groups, including independent media, must be part of the solution. **A whole of society approach is key.**
2. Exposure and identification of specific malicious entities (i.e. Russian bots or trolls) or content is necessary but not enough to curb the spread of foreign disinformation. **As we respond, the adversary's tactics evolve**.
3. A democratic response to state-sponsored information warfare must be rooted in democratic principles of **transparency, accountability, and integrity**. These principles should guide U.S. and European policy. As we learned during the Cold War, we need not become them to beat them.
4. Malicious disinformation attacks are not limited to one country. All democracies are current or potential future targets—our response is stronger with allies. Like-minded governments should establish mechanisms for consistent sharing of information, best practices, and risk-assessment guidelines. **The trans-Atlantic alliance should be the basis of a "Counter Disinformation Coalition,"** in which the United States should play a leading role.

Unfortunately, the United States has fallen behind Europe in both conceptualizing the nature of the challenges and operationalizing concrete steps to counter and build resilience against disinformation. The U.S. Congress should fill the gap. In this statement, I draw on two reports, Democratic Defense

Against Disinformation (2018) and Democratic Defense Against Disinformation 2.0 (2019),[2] which I co-authored with Ambassador Daniel Fried, in addition to my research at Brookings[3] on emerging threats in the information space and previous Congressional testimonies,[4] to:

- Provide an overview of Russia's disinformation machine;
- Provide a progress report on European and U.S. efforts to respond to Russian disinformation since 2016;
- Recommend steps that the United States, and the U.S. Congress in particular, should take to better defend against and get ahead of disinformation threats.

I. The Russian disinformation machine

Russian disinformation against democracies is multi-vectored and multi-layered, consisting of overt state-funded propaganda, covert social media entities, and constantly evolving repertoire of fly by night websites. These elements work in concert with each other to amplify and distribute content across traditional and social media outlets.

Overt Russian state-funded disinformation and propaganda includes RT, Sputnik, and other Kremlin-linked media outlets. Estimates suggest that the Russian government spends approximately $300 million on RT annually. RT broadcasts in English, Spanish, Arabic, and German, and claims to reach 700 million people in 100 countries.[5] RT, as it proudly states, is the most-watched news network on YouTube, claiming over 8 billion views and 3.5 million subscribers.[6] YouTube statistics show 2.8 billion views, however. By comparison, Voice of America has approximately 200 million views and 428,000 subscribers. RFER/RL has 32 million views and about 60,000 subscribers.

On Facebook, RT has 5.6 million followers, VOA 11.6 million, and RFE/RL 550,000. On Twitter, RT has 2.9 million followers, VOA 1.6 million, and REF/RL 77,000.

Covert social media entities include automated ("bot") accounts, trolls, cyborgs, and impersonation pages, groups and accounts used to carry out digital disinformation campaigns across social media platforms. To date, the Department of Justice Special Counsel report[7] and the investigation's related

[2] Alina Polyakova and Daniel Fried, "Democratic Defense Against Disinformation 2.0," (Washington, DC, United States: Atlantic Council, June 2019), https://www.atlanticcouncil.org/publications/reports/democratic-defense-against-disinformation-2-0.

[3] See: Alina Polyakova, "Weapons of the weak: Russia and AI-driven asymmetric warfare," (Washington, DC, United States: Brookings Institution, November 2018), https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/; and Alina Polyakova and Spencer Boyer, "The future of political warfare: Russia, the West, and the coming age of global digital competition," (Washington, DC, United States: Brookings Institution, March 2018), https://www.brookings.edu/research/the-future-of-political-warfare-russia-the-west-and-the-coming-age-of-global-digital-competition/.

[4] "Five Years after the Revolution of Dignity: Ukraine's Progress/Russia's Malign Activities," U.S. Congress, Senate, Senate Foreign Relations Subcommittee on Europe and Regional Security Cooperation, 116th Congress, statement of Dr. Alina Polyakova, Director, Global Democracy and Emerging Technology, Fellow, Center on the United States and Europe, Foreign Policy Program, Brookings Institution, https://www.foreign.senate.gov/imo/media/doc/061819_Polyakova_Testimony.pdf and "Lessons from the Mueller Report, Part II: Bipartisan Perspectives," U.S. Congress, House of Representatives, U.S. House Committee on the Judiciary, 116th Congress, statement of Dr. Alina Polyakova, Director, Global Democracy and Emerging Technology, Fellow, Center on the United States and Europe, Foreign Policy Program, Brookings Institution, https://docs.house.gov/meetings/JU/JU00/20190620/109668/HHRG-116-JU00-Wstate-PolyakovaA-20190620.pdf.

[5] Elena Postnikova, "Agent of Influence: Should Russia's RT Register as a Foreign Agent?" (Washington, DC, United States: Atlantic Council, August 2017), https://www.atlanticcouncil.org/images/publications/RT_Foreign_Agent_web_0831.pdf.

[6] "RT," YouTube channel, https://www.youtube.com/user/RussiaToday/videos?app=desktop.

[7] Robert S. Mueller, III, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election," (U.S. Department of Justice, Washington, DC, 2019), https://www.justice.gov/storage/report.pdf.

indictments from February 2018[8] and July 2018[9] against the Internet Research Agency (IRA) and Russian military intelligence (GRU) provide the most comprehensive assessment of the inner working of Russia's covert disinformation operations. The IRA's information operations against the United States relied on impersonation accounts to infiltrate public discourse online; used non-political content and issues to build audience on Facebook, Twitter, Instagram, and elsewhere; purchased ads to prop-up content on platforms to reach more users. Over the course of the U.S. operation, the IRA purchased over 3,500 ads and spent approximately $100,000—a small investment, which signals that advertising was a relatively small part of Russian disinformation operations in the United States. In mid-2017, the most popular IRA-controlled group—"United Muslims of America"—had over 300,000 followers. By the end of the 2016 election, the IRA "had the ability to reach millions of U.S. persons through their social media accounts" on Facebook, Instagram, Twitter, YouTube, and Tumblr, according to the report.[10] Facebook later estimated that IRA-controlled accounts reached as many as 126 million people,[11] and an additional 1.4 million[12] were reached through Twitter.

The Kremlin, via Putin's ally and agent, Yevgeny Prigozhin, invested in expanding the IRA's operations. In early 2015, the IRA had a staff of 225-250 people, which grew to 800-900 by the middle of the year adding new capabilities such as video, infographics, memes, etc.[13] By 2016, the number of employees at the American department or translator project almost tripled to 80-90 people, representing approximately 10 percent of the total staff. The IRA's monthly operating budget in 2016 was $1.25 million (approximately $15 million annually).[14] Since the conclusion of the Special Counsel investigation, we still don't know the full scope of the command structure, how far into the Kremlin the decision-making process reached, and how the project continues to be funded today. In 2017, an independent Russian news outlet reported that the IRA had moved into a new, larger office building. While the IRA's operations undoubtedly continue today, and other similar "troll farms" are also very likely operating in addition to the IRA, there is scant (if any) information about these entities' activities and funding.

II. How Europe has responded[15]

Following Russian interference in the 2016 U.S. elections, Russian disinformation operations have targeted elections and events in France (MacronLeaks), the United Kingdom (disinformation around the Skripal operation), Sweden (disinformation around NATO), Spain (Catalan referendum), European Union (European Parliament elections), Netherlands (MH17 investigation), North Macedonia, Greece, Ukraine, and elsewhere. The national responses have been varied based on national context and much of the response has come at the EU level.

[8] UNITED STATES OF AMERICA v. INTERNET RESEARCH AGENCY LLC A/K/A MEDIASINTEZ LLC A/K/A GLAVSET LLC A/K/A MIXINFO LLC A/K/A AZIMUT LLC A/K/A NOVINFO LLC et al. 18 U.S.C. §§ 2, 371, 1349, 1028A (2018). https://www.justice.gov/file/1035477/download.

[9] UNITED STATES OF AMERICA v. VIKTOR BORISOVICH NETYKSHO et al. 18 U.S.C. §§ 2, 371, 1030, 1028A, 1956, and 3551 et seq. (2018). https://www.justice.gov/file/1080281/download.

[10] Robert S. Mueller, III, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election," 26.

[11] Mike Isaac and Daisuke Wakabayashi, "Russian Influence Reached 126 Million Through Facebook Alone," *The New York Times*, October 30, 2017, https://www.nytimes.com/2017/10/30/technology/facebook-google-russia.html.

[12] Christopher Carbone, "1.4 million Twitter users engaged with Russian propaganda during election," *Fox News*, February 1, 2018, https://www.foxnews.com/tech/1-4-million-twitter-users-engaged-with-russian-propaganda-during-election.

[13] Polina Rusyaeva and Andrei Zakharov, "Расследование РБК: как «фабрика троллей» поработала на выборах в США," *RBC,* October 17, 2017, https://www.rbc.ru/magazine/2017/11/59e0c17d9a79470e05a9e6c1.

[14] UNITED STATES OF AMERICA v. INTERNET RESEARCH AGENCY LLC A/K/A MEDIASINTEZ LLC A/K/A GLAVSET LLC A/K/A MIXINFO LLC A/K/A AZIMUT LLC A/K/A NOVINFO LLC et al. 18 U.S.C. §§ 2, 371, 1349, 1028A (2018). https://www.justice.gov/file/1035477/download, 7.

[15] This is a summary of EU activities, for a detailed assessment of European responses, see: Polyakova and Fried, Democratic Defense Against Disinformation 2.0.

EU response

Last December, the EU launched an Action Plan Against Disinformation based on principles of transparency and accountability.[16] It increased funding to identify and expose disinformation and established a "rapid alert system" (RAS). The RAS was supposed to have an initial operational capacity by March 2019, two months before the EU parliamentary elections. But as *The New York Times* recently reported, the system is still not operational and mired in internal debates.[17]

The EU has also pushed to work with the major social media companies although in a voluntary capacity. Google, Facebook, Twitter, and Mozilla have signed onto an EU voluntary Code of Practice, which tries to set some standards for fighting disinformation. Social media companies are also submitting regular progress reports to the EU. The progress reports indicate a mixed picture. The EU Commission has recognized efforts by social media platforms to take down fake accounts, restrict ad purchasing by purveyors of disinformation, identify and block inauthentic behavior, and take other steps to meet the (general) commitments outlined in the code. But it also noted insufficient information provided by social media companies, and urged specific next steps, including calling on platforms to take more serious actions to address transparency, particularly with respect to political ads. The commission is issuing monthly progress reports to test social media companies' response to their commitments.[18]

The EU action plan also aims to improve social resilience against disinformation by creating a European network of independent fact checkers, launching a secure online platform addressing disinformation, exploring means of reliable identification of information suppliers, and supporting long-term social media literacy. It remains unclear, however, how and if these efforts have been implemented.

National European responses

National responses have varied significantly, which has only contributed to the difficulty of implementing a comprehensive EU level strategy.

France has taken the lead in conceptualizing a common democratic approach. In March 2019, President Emmanuel Macron proposed a new "European Agency for the Protection of Democracies," which included providing each EU member state with expertise to protect election processes against cyber-attacks and manipulation.[19] France has also led the "Paris Call for Trust and Security in Cyberspace," established in November 2018.[20] In relation to security of the information space, the Call includes commitments to:

[16] "Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Action Plan against Disinformation," (Brussels, Belgium: European Commission, December 5, 2018), https://eeas.europa.eu/sites/eeas/files/action_plan_against_disinformation.pdf.

[17] Matt Apuzzo, "Europe Built a System to Fight Russian Meddling. It's Struggling." *The New York Times*, July 6, 2019, https://www.nytimes.com/2019/07/06/world/europe/europe-russian-disinformation-propaganda-elections.html.

[18] "Code of Practice against disinformation: Commission calls on signatories to intensify their efforts," *European Commission*, January 29, 2019, http://europa.eu/rapid/press-release_IP-19-746_en.htm; "Second monthly intermediate results of the EU Code of Practice against disinformation," *European Commission*, March 20, 2019, https://ec.europa.eu/digital-single-market/en/news/second-monthly-intermediate-results-eu-code-practice-against-disinformation. Latest statement at time of writing: "Code of practice against disinformation: Commission welcomes the commitment of online platforms ahead of the European elections," *European Commission,* April 23, 2019, http://europa.eu/rapid/press-release_STATEMENT-19-2174_en.htm.

[19] Emmanuel Macron, "Renewing Europe," *Project Syndicate*, March 4, 2019, http://prosyn.org/kCUclh5.

[20] "Paris Call for Trust and Security in Cyberspace," (Paris, France: Ministry of Europe and Foreign Affairs, November 12, 2018), https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

- Increase prevention against and resilience to malicious online activity;
- Protect the accessibility and integrity of the Internet;
- Cooperate in order to prevent interference in electoral processes;
- Prevent the proliferation of malicious online programs and techniques.

The Paris call includes backing from 66 States, 139 international and civil society organizations, and 347 private sector entities. The implementation process is still in its early stages, but the multi-stakeholder support is a positive sign that it could serve as a platform for a global commitment on information and cyber security. The United States is not a signatory.

Sweden created a new "Psychological Defense" agency tasked with countering disinformation and increasing societal resilience to disinformation. The Swedish Civil Contingencies Agency (MSB), akin to the U.S. Department of Homeland Security, has worked closely with local authorities to establish lines of communication, conduct trainings, and analyze potential systemic weaknesses. Ahead of the Swedish national elections last fall, the MSB mailed leaflets to households explaining the threat of information influence and outlining how to respond.[21] Swedish schools also received information and materials to help teach students how to identify disinformation.

Other European countries, including the Czech Republic, Denmark, Estonia, and the Netherlands, established some form of a cross-agency team tasked with coordinating governmental efforts to identify and respond to information operations.

III. How the United States has responded

The United States has made little progress in addressing the disinformation challenge. At a basic level, it remains unclear who in the U.S. government owns this problem. Still, there have been notable activities from the Administration and the U.S. Congress. The State Department's Global Engagement Center (GEC) has been tasked with countering state-sponsored disinformation, and it has begun to fund research and development of counter-disinformation tools while supporting civil society groups and independent media on the front lines of the threat in Europe. Over time, this funding will help boost independent media and groups on the front-lines of the information war.

U.S. Cyber Command began operations ahead of the 2018 congressional elections to deter Russian operatives from potential interference.[22] Cyber Command, together with the National Security Agency (NSA), reportedly developed information about Russian trolls and their activities, and alerted the FBI and Department of Homeland Security (DHS).[23] The operation followed the Department of Justice indictments of Russian individuals, intelligence officers, and companies involved with the Internet Research Agency

[21] "Countering information influence activities – A handbook for communicators," (Karlstad, Sweden: Swedish Civil Contingencies Agency, March 2019), https://rib.msb.se/filer/pdf/28698.pdf.

[22] Julian E. Barnes, "U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections," *The New York Times*, October 23, 2018, https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html.

[23] David Ignatius, "The U.S. military is quietly launching efforts to deter Russian meddling," *The Washington Post*, February 7, 2019, https://www.washingtonpost.com/opinions/the-us-military-is-quietly-launching-efforts-to-deter-russian-meddling/2019/02/07/4de5c5fa-2b19-11e9-b2fc-721718903bfc_story.html?utm_term=.1cbbaf8bf3ae.

and in cyber operations against the U.S. elections.[24] Cyber Command has reportedly sent messages to specific individuals active in disinformation operations, de facto outing them and their activities.

While not a new policy, the Department of the Treasury used existing authorities to impose sanctions on Russian entities tied to disinformation efforts, including those directed at the 2016 U.S. presidential election. This included the sanctions designation on December 19, 2018, of entities and individuals tied to the IRA and nine GRU (military intelligence) officers. Material accompanying the Treasury Department's sanctions designations exposed details of Russian operation, including establishment of an online English-language website, "USA Really."

Current Time, the Russian language television news program produced by VOA and RFE/RL is perhaps the U.S. government's closest response to countering RT and other Kremlin-funded outlets by providing truthful information to Russian speakers in the post-Soviet states. This effort is critical as Russian speakers have little access to Russian-language broadcasting that is not Kremlin-controlled. However, *Current Time*, cannot, at this time, compete with the production values and the reach of RT. *Current Time'*s YouTube channel has received 279 million views and has 667,000 subscribers. On VKontakte (the Russian equivalent of Facebook), *Current Time* has 254,000 subscribers. Impressive for a program that started in 2014 but still far behind RT's reach.

The 2019 National Defense Authorization Act (NDAA) added significant (albeit second-order) provisions defining the importance of countering disinformation for U.S. national security.[25] It cemented the role of the GEC by defining its counter-disinformation task within the parameters of U.S. national security, likely securing the center's longer-term funding in future iterations of the NDAA. It also defined "malign influence" as "the coordinated, integrated, and synchronized application of national diplomatic, informational, military, economic, business, corruption, educational, and other capabilities by hostile foreign powers to foster attitudes, behaviors, decisions, or outcomes within the United States."

The Senate has reintroduced the Defending American Security from Kremlin Aggression Act of 2019 (DASKA); while mostly devoted to sanctions, it also "calls for the establishment of a National Fusion Center to Respond to Hybrid Threats, a Countering Russian Influence Fund to be used in countries vulnerable to Russian malign influence, and closer coordination with allies" (sections 704, 705, and 706).[26]

IV. What the U.S. should do

U.S. Congress

- **Congress should authorize and appropriate funds to "build capacity** of civil society, media, and other nongovernmental organizations," countering Russian and other sources of foreign disinformation (from DASKA Sec 705(b)), in coordination with the EU, NATO, and other bodies.

[24] UNITED STATES OF AMERICA v. INTERNET RESEARCH AGENCY LLC A/K/A MEDIASINTEZ LLC A/K/A GLAVSET LLC A/K/A MIXINFO LLC A/K/A AZIMUT LLC A/K/A NOVINFO LLC et al. 18 U.S.C. §§ 2, 371, 1349, 1028A (2018). https://www.justice.gov/file/1035477/download; UNITED STATES OF AMERICA v. VIKTOR BORISOVICH NETYKSHO et al. 18 U.S.C. §§ 2, 371, 1030, 1028A, 1956, and 3551 et seq. (2018). https://www.justice.gov/file/1080281/download

[25] "John S. McCain National Defense Authorization Act For Fiscal Year 2019," (Washington, DC, United States: U.S. Government Publication Office, July 25, 2018), https://www.govinfo.gov/content/pkg/CRPT-115hrpt874/pdf/CRPT-115hrpt874.pdf.

[26] U.S. Congress, Senate, *Defending American Security from Kremlin Aggression Act of 2019*, S 482, 116th Congress, 1st session, introduced in Senate February 13, 2019, https://www.congress.gov/116/bills/s482/BILLS-116s482is.pdf.

Funding is already available to the State Department's Global Engagement Center; this should be increased.

- Congress should authorize and appropriate funds to **establish a "fusion cell**" or NCTC-style model for coordinating U.S. government efforts on disinformation. The Cell could be housed in DHS, State, or elsewhere. There is more than one option for structuring an interagency response.

- **Congress should authorize and appropriate funds to further develop *Current Time*** to allow Current Time to broadcast and build audiences in Central Eastern Europe and the Balkans with potential expansion further into Western Europe.
    - At the same time, the United States Agency for Global Media (USAGM) should be tasked with conducting an audit of its existing programs and services to assess which are underperforming. It may not be a good use of resources to continue to fund traditional television broadcasting. More innovative, digitally oriented content should be considered to reach audiences through social media markets.

- **Congress should develop in-house expertise** on disinformation and digital media. Congress's capacity for detailed analysis, independent from social media companies, will be critical.

- **Congress should prepare legislation—on a step-by-step basis—to support a regulatory framework for social media companies.** This layered approach should start with greater Congressional scrutiny around all online advertising—an industry that is largely unregulated.
    - The **Honest Ads Act**, introduced in the last Congress, is a solid step toward setting transparency standards around online advertising (not just narrowly defined political ads). Standards should be established evenly across the tech industry, not just for social media firms. This act, revised and strengthened along the above lines, could be a vehicle for this effort.

- Consider legislation to provide a framework for regulation to address **transparency** (especially with respect to bots), **integrity and authenticity of service** (i.e. targeting deceptive and impersonator accounts, whether individuals or false-front organizations), and **common terms of service** across the social media industry.

- Congress could also consider mandating that media outlets determined by the Department of Justice to be acting as agents of foreign governments be de-ranked in searches and on newsfeeds and be barred from buying ads. RT, for example, was required to register under the Foreign Agents Registration Act (FARA). Governmental assessments and FARA determination should be one of many variables considered in rankings for search engines. However, legislators should bear in mind that mandating de-ranking based on governmental assessments and FARA determinations could set a precedent which undemocratic regimes could abuse.

- Congress should explore establishing a **federal statute that would limit companies' collection of personal data** about individuals. Such a statute would specify that any personal data collected would be specific to the stated purpose of the technology. Such data collection limitation would make microtargeting and exploitation of individuals' personal data more difficult while also reducing the ability of malicious actors to influence. The California Consumer Privacy Act of 2018[27] could serve as precedent for a federal mandate.

U.S. Administration

- The USG should continue to **impose sanctions** on foreign official, or officially-controlled or directed, purveyors of disinformation and their sponsors, and to identify and prosecute violations of federal elections laws (prohibitions on foreign contributions).
  - On September 12, 2018, the Trump administration issued Executive Order 13848, which provides for sanctions imposed against persons found to have interfered in U.S. elections. While, in part, simply an effort by the administration to preempt stronger legislation (i.e., the "DETER" Act introduced by Senators Marco Rubio (R-FL) and Chris Van Hollen (D-MD)), it provides a useful vehicle, should the administration use it.
  - U.S. sanctions laws restrict U.S. citizens from financial dealings with or "providing material support" to foreign persons under sanctions. Enforcement of these and federal election laws could limit the ability of Russian or other foreign purveyors of disinformation to work with U.S. agents.

- USG should, as some European countries have done, set up an interagency group/center or fusion cell tasked with coordinating governmental efforts to counter disinformation at home and abroad. The group should have high level political leadership to direct and coordinate policy, establish a baseline for response, educate civil servants, work via State with U.S. embassies, and create communication channels from the local to the federal level.

- **Establish a USG rapid alert system (RAS)** to inform the public, allied governments, and social media companies of emerging disinformation campaigns that threaten national security. The European rapid alert system can help the USG judge the potential of this idea. Some of the challenges can be anticipated: given U.S. politics and traditions, issues will arise around a U.S. RAS's mandate (e.g. the definition and attribution of disinformation) and its composition, credibility, and independence.

Getting ahead of the threat

The above recommendations are low-hanging fruit on which the U.S. Congress and the Administration should act. These steps will not turn the tide of disinformation attacks. Rather, these are the minimum actions needed to start to build resistance. The Kremlin's tool-kit is out in the open and Russia has faced few consequences for its malign activities. This sends a signal to other malicious actors that they can act with impunity to destabilize democracies and distort public discourse. Other state actors with perhaps greater capabilities, such as China, and non-state actors, such as terrorist groups with a higher tolerance for risk, will adapt the disinformation toolkit to undermine democracies or are already doing so.

While the democratic West is fighting yesterday's war, our adversaries are evolving and adapting to the new playing field. First, innovation in artificial intelligence (AI) is enabling the creation of "deep fakes" and other "synthetic media" products. Using video and audio manipulation, malicious actors can manufacture the appearance of reality and make a political leader appear to make remarks that they did

[27] Dipayan Ghosh, "What You Need to Know About California's New Data Privacy Law," *Harvard Business Review*, July 11, 2018, https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law.

not. As these tools become more low cost and accessible, they will become perfect weapons for information warfare. Such technologies could drive the next great leap in AI-driven disinformation.

Second, disinformation techniques are shifting from the use of simple automated bots to more sophisticated interaction with (and manipulation of) domestic groups, extremist and otherwise, through various forms of impersonation and amplification of organic posts by domestic actors. Thus, it is already increasingly difficult to disentangle foreign-origin disinformation from domestic social media conversations. Rather than trying to break through and channel the noise, the new strategy aims to blend in with the noise—obfuscating manipulative activity and blurring the line between authentic and inauthentic content.

The United States has fallen behind in addressing the challenge of foreign disinformation. But, it is not too late to change course toward a proactive rather than reactive approach. This critical issue concerns all democracies equally. Strong U.S. leadership could tip the balance toward ensuring that the digital space continues to facilitate and support democratic values of transparency, accountability and integrity. To do otherwise is to leave this arena open to authoritarians to set the rules of the game.