United States Senate Foreign Relations Subcommittee on State Department and USAID Management, International Operations, and Bilateral International Development

Hearing on "The Global Engagement Center: Leading the United States Government's Fight Against Global Disinformation Threat"

March 5, 2020

Dr. Alina Polyakova
President and Chief Executive Officer
Center for European Policy Analysis (CEPA)

Senator Portman, Senator Booker, Distinguished Members of the Subcommittee:

It is an honor and privilege to address you today on this critical issue for United States national security. Thank you for inviting me to speak.

I am the President and CEO of the Center for European Policy Analysis (CEPA), a nonprofit, nonpartisan, independent foreign policy think-tank focused on the transatlantic alliance and the study of Europe. My views are my own and do not represent those of the organization, which takes no institutional position. In addition, I would like to disclose that CEPA is a sub-grantee for a Federal Assistance Award from the U.S. Department of State's Global Engagement Center (GEC) for a two-year project that aims to provide civil society actors with tools and capacities to combat Russian disinformation throughout Central Eastern Europe. The sub-grant agreement came into effect in February 2019.

The Russia challenge

President Vladimir Putin's Russia seeks to weaken Western governments and transatlantic institutions, discredit democratic and liberal values, and create a post-truth world. Its strategic aim is, first and foremost, to undermine U.S. credibility and leadership in the world. The United States, from Moscow's point of view, is Russia's greatest enemy – a narrative that is frequently voiced on Russian state-controlled media. Yet, Russia presents a unique challenge to the United States. It is simultaneously a country in decline and a global power with proven ability and determination to undermine U.S. interests

in multiple arenas. Russia has been particularly adept at using asymmetric tools of political warfare – information operations and cyberattacks – to project power, undermine democratic institutions, and influence public opinion. In brief, Russia's great power ambitions supersede its capacity to act as a great power – militarily, economically, and politically. It is precisely because of this mismatch between ambition and ability that **Moscow has sought out and developed low-cost but high-impact tools of political warfare to challenge the United States and our allies.**

The spread of disinformation to undermine public confidence is one critical tool in the Kremlin's broader toolkit 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. These elements work together in a concert of chaos, each amplifying the other in various degrees, depending on the target of attack.

Americans experienced Russian political warfare in the context of Russian disinformation and cyberattacks during the 2016 U.S. presidential elections. Then and now, Russian disinformation campaigns aimed to amplify existing social divisions and further polarize democracies by spreading content on divisive social issues, infiltrating social media groups, attempting to plant content to be shared by authentic users, and using automated accounts to amplify content.

But Russian disinformation campaigns do not 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 world's democracies need to organize themselves now to address the challenge – the window for doing so is narrowing.[1]

One positive consequence of Russia's brazen interference in elections has been to wake up Western democracies to the threat. 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, three insights have emerged:

1. **A whole of society approach is key.** 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.

2. **As we – democratic governments, social media platforms, and civil society – have responded since 2016, adversarial tactics have evolved along at least three threat vectors**

    - **The Russian playbook has gone global**: other state actors are deploying info-ops at an increasing rate, and Russia is testing and expanding its operations globally, most notably in Africa. The Russians may be leaders in state-sponsored disinformation, but they will not be the

[1] "Russian Disinformation Attacks on Elections: Lessons from Europe" U.S. Congress, House of Representatives, House Committee on Foreign Affairs Subcommittee on Europe, Eurasia, Energy, and the Environment, 116th Congress, Statement of Ambassador Daniel Fried, Distinguished Fellow, the Atlantic Council: https://www.congress.gov/116/meeting/house/109816/witnesses/HHRG-116-FA14-Wstate-FriedD-20190716.pdf

last. China, Iran, and other state and non-state actors have already learned from the Russian toolkit and deployed it across the world. In

- **Russian disinformation activities have adapted** to obfuscate their origins and avoid detection. De facto, it is now almost impossible to distinguish between domestic and foreign activities on social media platforms.
- **Russia is increasingly developing an ecosystem approach** to influence operations, of which disinformation campaigns are a key, but not the only, element.

3. **To get ahead of the threat rather than reacting to disparate attacks in a whack-a-mole fashion, democracies must invest in building long-term societal resilience while at the same time getting on the offensive to deter foreign disinformation operations**.

    - The response must take an ecosystem approach to match Russia's ecosystem strategy, which operates across multiple social media and traditional media platforms, has overt and covert elements, and increasingly works in lockstep with private military groups, illicit finance, and intelligence operations.

In this testimony, I draw on my recent research with my co-author Ambassador Daniel Fried,[2] in addition to my research[3] on emerging threats in the information space, and previous Congressional testimonies,[4] to:

- Provide an overview of Russia's disinformation machine, including its evolution since 2016;
- Provide a progress report on 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.

The Russian disinformation machine

Disinformation is the intentional spread of false or misleading information to influence public discourse and narratives. Russian disinformation against democracies is multi-vectored and multi-layered, consisting of overt state-funded propaganda, covert social media entities, and a 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

[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.
"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.

on RT annually,[5] and $1.3 billion on all state media.[6] RT broadcasts in English, Spanish, Arabic, and German, and claims to reach 700 million people in 100 countries.[7] RT, as it proudly states, is the most-watched news network on YouTube, claiming over 8 billion views and 3.5 million subscribers.[8] YouTube statistics show 2.8 billion views, however.[9] On Facebook, RT has 5.6 million followers[10] and 2.9 million followers on Twitter.[11]

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. The Department of Justice Special Counsel report,[12] the investigation's related indictments from February 2018[13] and July 2018[14] against the Internet Research Agency (IRA) and Russian military intelligence (GRU), and the subsequent Senate Intelligence Committee reports[15] provide the most comprehensive assessment of the inner workings 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 an audience on Facebook, Twitter, Instagram, and elsewhere; and 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.[16] Facebook later estimated that IRA-controlled accounts reached as many as 126 million people,[17] and an additional 1.4 million[18] were reached through Twitter.

Yevgeny Prigozhin, Putin's ally and agent, who has been sanctioned by the United States, is in charge of the IRA project as well as the private military group, Wagner (more on this below). Prior to the 2016 elections, the Kremlin significantly expanded the IRA. 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.[19] By 2016, the number of employees at the American department or

[5] Vladimir Milov, "Stop Funding RT: Better Ways to Spend the Budget Money." Free Russia Foundation, August 5, 2017. https://www.4freerussia.org/stop-funding-rt-better-ways-to-spend-the-budget-money/
[6] "Figure of the Week: 1.3 Billion." StopFake, October 1, 2019. https://www.stopfake.org/en/figure-of-the-week-1-3-billion/.
[7] 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.
[8] "RT – YouTube," https://www.youtube.com/user/RussiaToday/videos?app=desktop.
[9] "RT – YouTube," YouTube. Accessed March 2, 2020. https://www.youtube.com/user/RussiaToday/about.
[10] "RT - Home Facebook." Facebook. Accessed March 2, 2020. https://www.facebook.com/RTnews/.
[11] account, RTVerified. "RT (@RT_com)." Twitter. February 21, 2020. https://twitter.com/rt_com?lang=en
[12] 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.
[13] 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.
[14] 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.
[15] U.S. Congress, Senate, Committee on Intelligence. RUSSIAN ACTIVE MEASURE;S CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION ' VOLUME 2: RUSSIA'S USE OF SOCIAL MEDIA WITH ADDITIONAL VIEWS, 116th Congress, 1st session .https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf
[16] Robert S. Mueller, III, "Report on the Investigation into Russian Interference in the 2016 Presidential Election," 26.
[17] 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.
[18] 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.
[19] 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.

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).[20]

Four years later, we still don't know to what extent the IRA remains operational, the full scope of the IRA's command structure, how far into the Kremlin the decision-making process reached, how the project continues to be funded today, and if the Kremlin has established other similar entities. 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) open source information about these entities' activities and funding.

Evolution of Russia's tactics since 2016

Since 2016, the Kremlin has stepped up its interference operations across the globe. Ukraine remains a test-lab for Russian information operations and the primary target.[21] During Ukraine's 2019 parliamentary elections, Ukraine's intelligence service arrested a man who confessed to being a Russian agent sent to Ukraine to recruit locals to rent or sell their Facebook account, which would then be used to spread false content or ads.[22]

Increasingly, Russia is aggressively deploying a combination of disinformation, private military groups, and corruption to exert influence in Africa, where it has been active in Libya, Sudan, Ivory Coast, Cameroon, Mozambique, Madagascar, the Central African Republic, and the Democratic Republic of the Congo.[23]

Prigozhin's two projects – Wagner and the IRA – came together in Africa as well. In October 2019, Facebook took down several disinformation networks that affected Madagascar, the Central African Republic, Mozambique, Congo, Ivory Coast, Cameroon, Sudan, and Libya. The broad disinformation campaign was linked to the Wagner Group, whose members were involved in setting up proxy media groups and contracting disinformation campaigns to local entities to obfuscate the link to Russia.[24] In some countries, Russian mercenaries worked to establish local media organizations that would employ locals hired to post false and misleading content on social media. The Russians would also hire existing media companies for the same purpose.[25] In Madagascar, the Russian operators carried out an expansive influence operation that included publishing newspapers in the local language, hiring local students to write articles in support of the president, buying television and billboard ads, paying people to attend rallies (and paying journalists to cover the rallies), and attempting to bully opposition groups to take bribes to drop out of the race.[26] The Madagascar case is the most prominent example of how the

[20] 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.
[21] Jack Stubbs, "Facebook says it dismantles Russian intelligence operation targeting Ukraine." Reuters, February 12, 2020. https://www.reuters.com/article/us-russia-facebook/facebook-says-it-dismantles-russian-intelligence-operation-targeting-ukraine-idUSKBN2061NC
[22] Michael Schwirtz and Sheera Frenkel,"In Ukraine, Russia Tests a New Facebook Tactic in Election Tampering." The New York Times, March 29, 2019. .https://www.nytimes.com/2019/03/29/world/europe/ukraine-russia-election-tampering-propaganda.html
[23] Shelby Grossman, Daniel Bush, and Renée DiResta, "Evidence of Russia-Linked Influence Operations in Africa." Stanford Internet Observatory, October 30, 2019. https://cyber.fsi.stanford.edu/io/news/prigozhin-africa
[24] Craig Timberg, "'Putin's Chef,' Architect of Interference in 2016 U.S. Election, Is Now Meddling in African Politics, Facebook Says." The Washington Post. WP Company, October 30, 2019. https://www.washingtonpost.com/technology/2019/10/30/putins-chef-architect-us-election-interference-now-meddling-politics-across-africa-facebook-says/
[25] Alba Davey and Frenkel Sheera, "Russia Tests New Disinformation Tactics in Africa to Expand Influence." The New York Times, October 30, 2019. https://www.nytimes.com/2019/10/30/technology/russia-facebook-disinformation-africa.html
[26] Michael Schwirtz and Gaelle Borgia, "How Russia Meddles Abroad for Profit: Cash, Trolls and a Cult Leader." The New York Times, November 11, 2019.https://www.nytimes.com/2019/11/11/world/africa/russia-madagascar-election.html

Kremlin deploys a multi-faceted influence operation of which information ops are one key but not the only element. Similarly, in South America, Russian influence operations aim to amplify and exploit unrest in Venezuela, Ecuador, Peru, Bolivia, Colombia, and Chile.[27]

Tellingly, Russian mercenaries are present in many of the countries where social media companies, governments, and researchers are identifying active disinformation campaigns. Prighozhin's Wagner Group is the best known but not only such group active in Africa.[28] Wagner mercenaries have been pouring into Africa in recent months.[29] In Libya, some estimate that up to 2,000 Russian fighters have been deployed to support Khalifa Hifter in the country's civil war.[30] In Mozambique, an estimated 200 Russian mercenaries are thought to be active.[31] Russian PMCs and advisers have also been active in the Central African Republic, where approximately 250 Russian mercenaries are training recruits,[32] and allegedly in Venezuela.[33]

These recent Russian activities signal new threat developments to which the U.S. and our allies are not well-equipped to respond:

1. Russian information operations pose a global threat, no longer contained to the frontline states of Central and Eastern Europe.
2. Russian influence operations form a full spectrum ecosystem approach, in which disinformation campaigns work across digital and traditional media and in concert with other tools of political warfare.
3. Russia is engaged in information warfare by proxy – using cutouts, local groups and individuals, and local servers to mask their origins. This greatly limits our ability to identify and expose covert information operations and de facto erases the line between authentic and inauthentic actors or domestic and foreign content.

The U.S. response must be calibrated to meet these and future challenges as Russia and other state actors will continue to use multi-faceted influence operations to undermine U.S. credibility and global leadership.

How the United States has responded

The greatest challenge facing the U.S. government as it has sought to craft a counter disinformation strategy has been identifying the appropriate coordinating body able to carry out a politically empowered policy agenda. Coordination, both on operations and policy, has been slow. Some European countries, such as Sweden, identified the appropriate agency to coordinate and set policy and quickly

[27] Lara Jakes, "As Protests in South America Surged, So Did Russian Trolls on Twitter, U.S. Finds." The New York Times, January 19, 2020.https://www.nytimes.com/2020/01/19/us/politics/south-america-russian-twitter.html
[28] Candace Rondeaux, "Decoding the Wagner Group: Analyzing the Role of Private Military Security Contractors in Russian Proxy Warfare." New America, 2019. https://www.newamerica.org/international-security/reports/decoding-wagner-group-analyzing-role-private-military-security-contractors-russian-proxy-warfare/
[29] Sergey Sukhankin, "Russian Mercenaries Pour into Africa and Suffer More Losses (Part One)." The Jamestown Foundation, January 21, 2020. https://jamestown.org/program/russian-mercenaries-pour-into-africa-and-suffer-more-losses-part-one/
[30] Sergey Sukhankin, "Russian Mercenaries Pour into Africa and Suffer More Losses (Part One)." The Jamestown Foundation, January 21, 2020. https://jamestown.org/program/russian-mercenaries-pour-into-africa-and-suffer-more-losses-part-one/
[31] Eric Schmitt and Thomas Gibbons-neff, "Russia Exerts Growing Influence in Africa, Worrying Many in the West." The New York Times, January 28, 2020. https://www.nytimes.com/2020/01/28/world/africa/russia-africa-troops.html
[32] Tim Lister and Clarissa Ward, "Putin's Private Army Is Trying to Increase Russia's Influence in Africa." CNN. Cable News Network. Accessed 2019. https://edition.cnn.com/interactive/2019/08/africa/putins-private-army-car-intl/
[33]Maria Tsvetkova and Anton Zverev, "Exclusive: Kremlin-linked contractors help guard Venezuela's Maduro - sources." Reuters, January 25, 2020. https://www.reuters.com/article/us-venezuela-politics-russia-exclusive/exclusive-kremlin-linked-contractors-help-guard-venezuelas-maduro-sources-idUSKCN1PJ22M

established interagency communication. In the United States, responses have been decentralized across multiple governmental agencies, groups, and centers. As a result, it has been difficult to assess who in the U.S. government owns the problem. One reason for this is the sheer size, complexity, and compartmentalization of the U.S. government, which makes coordination slow and difficult for a problem that cuts across multiple regions and touches on issues of public diplomacy, election security, and foreign interference. This remains a problem for crafting a sophisticated and well executed response to the disinformation challenge.

The Global Engagement Center

The 2017 National Defense Authorization Act (NDAA) expanded the function and mandate of the State Department's Global Engagement Center (GEC) to counter state-sponsored disinformation. By design, the GEC, as a State Department center in the public diplomacy bureau, has no mandate to address disinformation attacks in the United States. While the Department of Homeland Security (DHS) is the appropriate agency to address threats to the United States, its main focus has been on securing the infrastructure of elections. U.S. Cyber Command began operations ahead of the 2018 congressional elections to deter Russian operatives from potential interference.[34] 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).[35] Cyber Command's mandate to develop offensive response capabilities[36] is a welcome shift in U.S. policy. But on the whole, the lack of a defined long-term strategy to counter disinformation abroad and at home will leave the U.S. vulnerable to future attacks.

The GEC, which has the mandate to coordinate operational interagency responses, has been hampered in carrying out its task in several ways:

1. The funding mechanism established in 2017 NDAA in which the Department of Defense would transfer GEC ear-marked funding to the State Department, while seemingly straightforward, led to bureaucratic wrangling between State and DoD, which slowed the GEC's ability to ramp up operations immediately.
2. The nature of U.S. federal guidelines for hiring personnel has also led to a lag in building capacity. The Russia team of the GEC only became strategically operational in the summer of 2019.
3. While the GEC has the mandate to coordinate operationally, there is no politically empowered (i.e. Congressionally confirmed) position in the U.S. government responsible for establishing the policy and ensuring interagency coordination to respond to disinformation. Such a position would need to be at the Undersecretary level.
4. Multiple seemingly duplicative interagency groups have been established within the U.S. government, which likely limit the GEC's ability to serve as the coordinating body intended by Congress. For example, there is an interagency group, the RIG, for coordinating Russia related responses. The 2020 NDAA authorized the establishment of a Social Media Data and Threat Analysis Center within the Director of National Intelligence (DNI) to enable better information sharing between the government and social media companies to

[34] 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.
[35] 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.
[36] National Cyber Security Strategy of United States of America, September, 2018. https://www.whitehouse.gov/wpcontent/uploads/2018/09/National-Cyber-Strategy.pdf

"institutionalize ongoing robust, independent, and vigorous analysis of data related to foreign threat networks within and across social media platforms [which] will help counter ongoing information warfare operations against the United States, its allies, and its partners." 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).[37] It is imperative that U.S. government efforts are led by an agency with a clear politically endorsed mandate rather than dispersing and decentralizing efforts across multiple task forces, fusion cells, or centers.

Still, despite the slow start, the GEC has been actively funding independent civil society groups on the frontlines of Russian information operations. It has also sought to coordinate efforts with allied governments, work closely with researchers to expose Russian disinformation campaigns, provide direct support, and develop the capacity to follow the threat as Russian operations have gone further afield. Most recently, the GEC worked to expose Russian disinformation around COVID-19 (the Coronavirus).[38]

The GEC should be the USG body that develops a threat assessment framework for the U.S. government. Such a framework would identify clear baselines and metrics for appropriate response. Not all disinformation campaigns require a governmental response, and in some cases, a response may serve the opposite function of amplifying a disinformation campaign. In cases that threaten national security and public safety, a USG response is not only warranted, it is essential.

The GEC should build information sharing relationships with social media companies. Recognizing that there is a trust gap between governments and the companies means that this will take time to develop, but the companies must be part of the process for USG efforts to counter disinformation campaigns. Precedent for such public-private information sharing exists in the law enforcement space and the counter-terrorism space.

What the United States should do

- **Ensure consistent and continuous funding for the GEC.** 2020 was the first year that the GEC was funded directly through the State Department rather than via the DoD transfer. This should continue.

- **Ensure scalability of GEC efforts to respond to a global, rather than a regional threat**. The GEC received approximately $62 million in 2020. The President's proposed 2021 budget includes an additional $76 million in funding for the GEC. An increase of this level would allow the GEC to scale up its operations.

- **Require regular reporting by the State Department on state-sponsored information operations** across the world, including sensitive information to be shared in a classified setting on the

[37] 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.
[38] AFP, "Russia-linked disinformation campaign fueling coronavirus alarm, US says," Radio France Internationale, February 22, 2020.http://www.rfi.fr/en/wires/20200222-russia-linked-disinformation-campaign-fueling-coronavirus-alarm-us-says

operational capacities, command-and-control structure, and funding for covert Russian operations including those carried out by the GRU.

- **Consider establishing an Undersecretary level position for information operations** to establish and coordinate the whole of U.S. government responses that is outside of the public diplomacy bureau at State.

- **Develop an ecosystem approach** to an ecosystem threat. The GEC should work in close cooperation with U.S. government agencies tracking Russian illicit finance, private military group activities, and support for disruptive political groups to identify high threat areas where the GEC should provide direct support and expand resources.

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

- **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.

- **Continue to impose sanctions** on foreign officials, 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).

- **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 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 toolkit 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 (A.I.) 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

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.