Statement by Ambassador Daniel Fried (retired)
Distinguished Fellow, the Atlantic Council
Hearing on Russian Disinformation Campaigns
House Committee on Foreign Affairs
Subcommittee on Europe, Eurasia, Energy, and the Environment
July 16, 2019

Chairman Keating, Ranking Member Kinzinger, Members of the Committee, I appreciate the opportunity to appear before you today. The topic is relevant and timely.

The Putinism Problem

President Trump has noted that it would be nice if the United States got along with Russia. He's right. Both Presidents Bush and Obama tried to sustain constructive relations with Putin's Russia. They failed because Russia's conditions for good relations with the US are those that no US administration should accept: US deference to Russian domination of its neighbors, including through intimidation and war, and US indifference to Russia's repression at home.

Some in this country and in Europe might accept these Russian conditions. But hard experience in the 20th century – through two World Wars and the Cold War – show that a country's repression inside its borders indicates that it will be aggressive abroad, and that spheres of influence established through force and repression, Russia's usual methods, are neither stable nor self-limiting.

Putin's system of rule combines political authoritarianism and economic kleptocracy; it is a regime dedicated to enriching its members, not the nation it supposedly serves. Economically, it depends on control of raw materials which it can export. It is a value-extracted, not value-added, economy. Putinism thus keeps Russia relatively backward. Policies to develop Russia would require respect for the rule of law, property rights, independent institutions both in and out of government, and freedom of speech and assembly; in short, free market, democratic reforms. But such reforms would mean an end to Putinism.

As a corrupt system by design, lacking democratic legitimacy and, increasingly, economic results, the Putin regime is insecure. It thus relies on repression mixed with chauvinistic campaigns directed against various made up outside enemies. That is not all. The regime seeks to prevent its democratic rivals — what we used to call the Free World — from challenging Putin's regime by the power of their example. Putin, like Soviet leaders before him, seeks not just to weaken the European Union and NATO, he seeks to discredit the very idea of democracy as a potentially appealing alternative for Russia.

Russia's Disinformation Challenge

Russia's use of disinformation to interfere in the US presidential elections in 2016, documented in the Mueller Report and attested to by numerous intelligence community assessments, is only

one piece of a broad Russian effort to destabilize Western societies. While many Americans became aware of such Russian tactics only in 2016, many Europeans, particularly Ukrainians, Georgians Estonians, Latvians, and Lithuanians, have faced such Russian methods for years. Spain, Greece, Germany, France, and the UK have faced intense Russian disinformation campaigns more recently. Some Western Europeans who believed that Russian aggression and disinformation had nothing to do with them have discovered their error.

Russian use of hostile propaganda and what used to be called "active measures" against the West date back to the Soviet period; we've dealt with this before. As the US government's first Soviet specialist George Kennan wrote from Moscow in 1946[1], the Kremlin seeks through covert means "[t]o *undermine general political and strategic potential of major western powers. Efforts will be made in such countries to disrupt national self-confidence, to hamstring measures of national defense, to increase social and industrial unrest, to stimulate all forms of disunity…[p]oor will be set against rich, black against white, young against old, newcomers against established resident, etc*."

In those years, the Soviets manipulated print media. On the ground, they infiltrated local groups, slowly taking them over. But such operations were "analogue." What then took many weeks or months now takes minutes.

Moscow's disinformation tactics — use of bots, state-sponsored trolls, inauthentic online accounts and false personas, and potential use of emerging AI technologies that enable "deep fakes" and more — is cutting edge. As explained in the Department of Justice Special Counsel report[2] and the investigation's related indictments from February 2018[3] and July 2018[4] against the Internet Research Agency (IRA, the St. Petersburg troll farm) and military intelligence (GRU), the Kremlin's disinformation system combines computer hackers, overt propaganda such as *RT* and *Sputnik*, covert social media presence, and skilled trolls, with assistance by enablers in the West (in my day, we called them "useful idiots").

The IRA has been funded through the Kremlin-connected businessman and operative Yevgeny Prigozhin. Prigozhin also serves as a channel for Kremlin funding of Ukrainian separatists (for which the Obama Administration sanctioned him in late 2016), the mercenary "Wagner Brigade" which has put Russian soldiers in Syria and Venezuela, and, according to press reports, various operation in Africa. This gives a sense of the priority the Kremlin places on its disinformation efforts, and how they stand as the cutting edge of its aggressive foreign policy.

---

[1] The "Long Telegram," reprinted in Kennan's "Memoirs"

[2] 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.

[3] 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.

[4] 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.

These elements combine to produce what my colleague Alina Polyakova calls a concert of chaos: intelligence officers and hackers can steal e-mails and send them to friendly sites which will disseminate them; RT and Sputnik will pick up and push the stories; bots and trolls will amplify these messages. In the 2016 US elections, Russian disinformation techniques used automated bots, impersonation accounts, microtargeting tactics, and online ads.

More recent analysis suggests that disinformation techniques are shifting toward sophisticated interaction with (and manipulation of) domestic groups, extremist and otherwise, through various forms of impersonation and amplification of organic posts by domestic persons. Deceptive sites can steer initially authentic social media conversations, promoting extreme views and inflaming opinion, and sometimes even taking both sides of a divisive issue, ramping up the rancor. The IRA uses impersonation accounts to infiltrate public discourse online, often using initially non-political content and issues to build a social media audience on Facebook, Twitter, Instagram and elsewhere. Disinformation's next stage may involve "deep fakes," which are rapidly improving in technical quality, creating and disseminating falsified images faster than fact checkers can catch up.

The Russians may be leaders in state-sponsored disinformation, but they will not be the last. China, Iran, and other state and non-state actors are learning from the Russian tool-kit. The democratic community — aka the Free World — needs to face the challenge of Russian and other forms of contemporary disinformation, and to do so while remaining true to our democratic values and norms of freedom of expression. As we learned during the Cold War, we must not and need not become them to fight them.[5]

Europe Seeks Solutions[6]

For many years, European nations were divided about whether Russian disinformation constituted a significant problem. Starting in 2018, stung by repeated Russian disinformation campaigns, European opinion moved toward action. The emerging European Union policy is outlined in four documents: "Tackling Online Disinformation, a European Approach," prepared by the EU Commission and published on April 26, 2018; a voluntary "Code of Practice on Disinformation" prepared by the Commission, published on September 26, 2018 and agreed to on October 16, 2018 by Facebook, Google, Twitter, and Mozilla, as well as the European trade associations representing online platforms and the advertising industry; an EU Commission "Progress Report" published on December 5, 2018; and the "Action Plan against Disinformation" jointly prepared by the EU Commission and European External Action Service (the EU "foreign ministry") also published on December 5, 2018.

[5] See "Democratic Defense Against Disinformation," February 2018, The Atlantic Council, Ambassador Daniel Fried (Ret.) and Alina Polyakova. This testimony draws on this report and on Dr. Polyakova's own congressional testimony, as well as our joint appearances on this topic in Europe and the United States.

[6] For a detailed assessment of the EU response to Russian disinformation, see https://www.atlanticcouncil.org/images/publications/Democratic_Defense_Against_Disinformation_2.0.pdf

The major policy elements of the emerging EU approach include:

- **Strengthening EU capacity to identify and expose disinformation.** This includes a recommendation to double the budget for strategic communications. The EU's EastStratCom unit, based in Brussels, has a mandate to identify and expose Russian disinformation. EastStratCom's staff is dedicated and skilled but has lacked consistent political support and adequate funding. This hopefully will change.

- **Establishment of an EU Rapid Alert System (RAS) to expose disinformation in real time.** This was set up before the May EU Parliamentary elections and was intended to link each EU member state government and allow for passing of alerts about disinformation campaigns.

  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 fully operational.[7] Hopefully, it will improve in effectiveness.

- **The Code of Practice on Disinformation** marks a significant step forward. Under its terms, social media companies have agreed to scrutiny of ad placements; transparency of political and issued-based advertisements; integrity of service (meaning social media companies have committed to identify and remove fake accounts, including bots); empowering consumers, a general commitment by social media companies to "help people make informed decisions"; and empowering the research community, meaning that social media companies will support research on disinformation. The Code provides for the social media companies to make monthly progress reports to the EU and notes that if progress is not satisfactory, regulation could follow.

  The progress reports issued under the Code of Practice suggest a mixed picture. Social media platforms have provided details of their efforts 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 the EU Commission has 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.[8]

---

[7] https://www.nytimes.com/2019/07/06/world/europe/europe-russian-disinformation-propaganda-elections.html

[8] European Commission, "Code of Practice against disinformation: Commission calls on signatories to intensify their efforts," (European Commission, Brussels, 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, Brussels, 2019), https://ec.europa.eu/digital-single-market/en/news/second-monthly-intermediate-results-eu-code-practice-against-disinformation. Latest report at time of writing: http://europa.eu/rapid/press-release_STATEMENT-19-2174_en.htm.

- **Improving social resilience against disinformation,** including creating a European network of independent fat checkers; launching a secure online platform addressing disinformation; exploring means of reliable identification of information suppliers; and support long-term social media literacy.

  It remains unclear, however, how and whether these efforts have been implemented.

Individual European national governments have also taken steps to address the disinformation challenge:[9]

- **France** has taken a lead, perhaps in reaction to Russian hacking at the end of the French Presidential election in 2017 into the Macron campaign computers and dissemination of purloined e-mails. In this case, the Russian disinformation operation was detected and exposed in real time by European and US civil society groups. The hostile French social reaction to this attempt to manipulate the elections drowned out whatever impact the Russian disinformation operation hoped to trigger. *It was an outstanding success story in the fight against Russian disinformation.*

  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 cyberattacks and manipulation.[10] France has also led the "Paris Call for Trust and Security in Cyberspace," established in November 2018.[11] In relation to security of the information space, the Call includes commitments to:
  - increase prevention against and resilience in the face of malicious online activity;
  - protect the accessibility and integrity of the Internet;
  - cooperate to prevent interference in electoral processes; and
  - 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 US is not a signatory.

- **Sweden** has created a new "Psychological Defense" agency tasked with countering disinformation and increasing societal resilience to disinformation. The Swedish Civil Contingencies Agency (MSB), with mandate similar to the US Department of Homeland Security, has worked closely with local Swedish authorities to establish lines of communication, conduct training, and analyze potential systemic weaknesses. Ahead of the Swedish national elections last fall, the MSB mailed leaflets to households explaining

[9] https://www.brookings.edu/wp-content/uploads/2019/07/Alina-Polyakova-House-Appropriations-Testimony-July-10-2019.pdf

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

[11] 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

the threat of information influence and outlining how to respond.[12] Swedish schools have also received information and materials to help teach students how to identify disinformation.[13]

- The **Czech Republic, Denmark, Estonia, the Netherlands**, among others, have established a cross-agency teams tasked with coordinating governmental efforts to identify and respond to disinformation operations.

The good news is that the European Union and some individual European national governments are focused on addressing the disinformation challenge. The EU action plan, especially the Code of Conduct, is a solid start, consistent with the values of freedom of expression, that provides a set of norms and objectives to which social media companies can be held. The bad news is that EU implementation of its own plan has been uneven. This effort is only beginning.

The US Tries to Get a Grip

The United States lags behind the EU, both in conceptual framing of the issue and systemic actions to deal with it. This is not due to lack of sophistication or awareness of the problem inside the Administration. But leadership has been uneven; the USG approach to Russia-sourced disinformation appears hampered by what could be called partisan reactions to the problem. Perhaps as a result, it remains unclear who in the U.S. government owns this policy challenge.

Nevertheless, work in ongoing within the Administration:

- 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.[14]

- **US Cyber Command** began operations ahead of the 2018 congressional elections to deter Russian operatives from potential interference.[15] 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

[12] https://rib.msb.se/filer/pdf/28698.pdf

[13] Dr. Polyakova and I have worked closely with the Swedish MSB in our counter-disinformation work, and the Swedish government has sponsored our efforts.

[14] See the written testimony of Lea Gabrielle, Special Envoy and Coordinator for the GEC, before the House Appropriations Subcommittee on State, Foreign Ops, and Related Programs, July 10, 2019

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

(DHS).[16] The operation followed the Department of Justice indictments of Russian individuals, intelligence officers, and companies involved in the Internet Research Agency and cyber operations against the US elections.[17] Cyber Command has reportedly sent messages to specific individuals active in disinformation operations, de facto outing them and their activities. While I have no special knowledge of its intentions, the press reporting of these activities may have reflected a considered strategy.

- **USAID**, working with State (including the European Bureau) has launched a set of programs titled "Countering Malign Kremlin Influence," which include supporting local media and civil society in some of the European countries most vulnerable to Russian disinformation. The intent is to support social resilience and resistance to such campaigns.

- The **Department of the Treasury** has used existing authorities to impose sanctions on Russian entities tied to disinformation efforts, including those directed at the 2016 US presidential election. This included the sanctions designations 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 US 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. At this time, *Current Time*, lacks the resources to compete with the production values and the reach of RT.

- The **2019 National Defense Authorization Act (NDAA**) added significant (albeit second-order) provisions on countering disinformation for US national security.[18] It cemented the role of the GEC by linking its counter-disinformation task to US national security, hopefully securing the center's longer-term funding. 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."

---

[16] David Ignatius, "The U.S. military is quietly launching efforts to deter Russian meddling," 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.

[17] US Department of Justice, "Internet Research Agency Indictment" (US Department of Justice, Washington, DC, 2018), https://www.justice.gov/file/1035477/download; "Indictment" (US Department of Justice, Washington, DC, 2018), https://www.justice.gov/file/1080281/download.

[18] US Government Publication Office, "National Defense Authorization Act For Fiscal Year 2019" (US Government Publication Office, Washington, DC, 2018), https://www.govinfo.gov/content/pkg/CRPT-115hrpt874/pdf/CRPT-115hrpt874.pdf.

- The Senate has reintroduced the **Defending American Security from Kremlin Aggression Act of 2019 (DASKAA**). While mostly devoted to sanctions, DASKAA 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). [19]

These are all laudable steps. But they lack the scope of what the EU has already tried to launch. So far, for example, there is no USG equivalent to the EU Code of Practice involving US social media companies. Moreover, these steps do not seem to be integrated into an all-of-government approach with the backing of the President.

Next Steps

The following might serve as a US action plan:

- The **US government** needs to ***get organized*** to contend with Russian and other disinformation. DHS, FBI, and the State Department (especially the Global Engagement Center) have expertise and mandates of different kinds. The USG needs to designate a lead agency and a senior official to own the problem, and perhaps stand up an interagency body such as a **national counter-disinformation center** (which could act as a rapid alert system, hopefully in concert with the emerging European RAS). Those responsible for counter-disinformation policy need to have the explicit, unambiguous backing of the President and the White House. Mixed messages will not do.

- The **USG needs to work with its friends**, starting with the European Union and key member states. A best-case initiative could include standing up a ***"counter-disinformation coalition"*** of like-minded governments and including social media companies and civil society groups. The Coalition's purpose would be to pool knowledge, including in real time; and set common approaches, including regulatory standards as needed. The US could join the Code of Practice, formally if possible or otherwise, or help negotiate a broader such Code, possibly in a G7 context. The point is to combine standards and pool leverage, including with social media companies to encourage their diligence in addressing disinformation.

- ***Social media companies*** have moved beyond their initial denial of the problem, but need to keep cleaning up their platforms, including by establishing common transparency standards to deal with suspicious accounts or deceptive sites, and reassessing online anonymity. We have learned that "Angry Bob from Boise" may in fact be Ivan from the St. Petersburg troll farm (the Internet Research Agency) and we may not want to permit deception of this sort. Social media companies need to address the problem of algorithmic bias toward extremism. But because this may challenge their established business model, it may require regulation applied evenly to all social media companies to get them to move. We ought not have our

[19] US 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.

social media companies acting as unwitting research arms or enablers for Russian intelligence.

- ***The Administration and Congress*** *s*hould follow the principles of ***transparency and authenticity*** on social media, not heavy content control. That means, for example, requiring full disclosure of the funders of political and issue ads, pressing social media companies to remove inauthentic accounts, mandating standard definitions of impersonator and inauthentic accounts across social media companies, and exploring ways to deal with the algorithmic bias toward sensational content, which leads social media users to extremism.

- ***Regulation of social media*** should be an iterative process rather an effort at a one-time act. We need to learn as we go. Congress and the Administration should start with low-hanging fruit and proceed with care to greater challenges. Recommendations include:
    - ***Regulation of advertisement and sponsored content,*** among the easier challenges (though not "easy"), as precedent exists for limits on commercial speech. The Honest Ads Act is one such example. Social media companies can be required to post accurate information about ad sponsors, rather than euphemistic or misleading self-descriptions.
    - ***Mandatory identification of bots*** under certain conditions (e.g., if disguised as persons, following the principle of transparency).
    - ***Regulatory mandates to disclose or remove inauthentic foreign accounts or impersonators.*** These raise issues of definition and the principle of on-line anonymity, but should be principal elements of a regulatory regime. Using a pseudonym online may be legitimate, but deceptive identification could be part of a disinformation operation, and there may be ways to address this challenge.
    - ***Mandating standard terms of service,*** including common definitions of impersonator and inauthentic accounts, and standards for removing bots.
    - ***Algorithmic bias*** if related to content would be among the most controversial and difficult regulatory issues (what would a "fairness doctrine" look like when applied to social media?). However, targeted fixes addressing behavior or provenance (e.g., RT, Sputnik) and involving de-ranking may be worth exploring.

- ***Civil society groups*** in Europe and the United States could be the heroes of counter-disinformation. Groups such as the Atlantic Council's Digital Forensic Research Lab or the Baltic Elves, Ukraine's Stop Fake, or EU DisinfoLab and others have proven themselves adept at exposing Russian disinformation campaigns, e.g., Russian hacking into the 2017 French elections and Russian lies about its 2014 shootdown of a Malaysian airline over Ukraine. Civil society activists — bot hunters, troll spotters, and digital Sherlocks — may be far more capable than most governments, and their work can be made public fast. They are natural partners and should be supported and brought into discussions of solutions.

Fighting disinformation *can work, but long-term social resilience will work best.* There will be no complete solution, no set of policies which can eliminate disinformation. But this need not be our objective. Actions by democratic governments, social media companies, and civil society can circumscribe and constrict disinformation. Doing so starting now can give time for democratic societies to develop greater sophistication at recognizing disinformation. Teaching everyone — from civil servants to children — how to spot disinformation ought to be standard practice as much as public health classes.

Lead and help fix the Free World

I want to end with a larger thought: a strong Russia policy – with counter-disinformation efforts one of its elements -- should be linked to an American Grand Strategy, which recognizes that a rules-based world that favors freedom is in the United States' national interest. At our best, we have recognized that our interests and our values advance together or not at all. The United States was different from previous great powers, exceptional, if you will, because we understood that our nation would do well when, and only when, other nations also did well. We were not interested in merely guarding a sphere of influence, like great powers of the past. Instead, in a breathtaking display of confidence and vision, we understood that we could make the world a better place and do well for ourselves in the process.

Putin, and likeminded nationalists and despots, stand instead for nothing more than power. We saw the results of such thinking in the first half of the 20th century. The United States can do better. In fact, when the United States' time to lead came in 1945 and again after 1989, we did do better. And so did the world. Despite our mistakes, inconsistencies, and downright blunders, the United States' leadership in the world has generated the longest period of general great power peace in human history, alongside unprecedented global prosperity.

Past success gives us no basis for complacency. Our current problems are severe, some of our own making.

But at the end of our current national debate about the United States' purposes in the world, I hope and believe that we will recall the values and purposes which have propelled America's world leadership and produced so much good for so many.