CEPA
digital innovation
initiative

Atlantic Council
DIGITAL FORENSIC
RESEARCH LAB

DEMOCRATIC OFFENSE AGAINST DISINFORMATION

535

154

Share

Music

@apolyakova ✓
@AmbDanFried ✓

#russia #china #EU #US #disinformation

+

CONTENTS

ACKNOWLEDGEMENTS

This three-part series on how democracies can defend against and get ahead of disinformation would not have been possible without help from many colleagues in the United States and Europe. This paper, and the ones before it, would not have become a reality without Geysha González, who remained committed to the work since the first paper was published in 2018. We also received valuable feedback and support from colleagues at the Atlantic Council's Digital Forensic Research Lab and the Center for European Policy Analysis. Many others from the public, private, and nonprofit sectors across the Atlantic lent their expertise in the review process. Alexander Wirth of the Center for European Policy Analysis stepped in at just the right moment to move this project forward. The authors also thank the Delegation of the European Union to the United States for its generous support without which this report would not have been possible. This report is part of CEPA's Digital Innovation Initiative, which receives generous support from Craig Newmark Philanthropies.

All opinions are those of the author(s) and do not necessarily represent the position or views of the institutions they represent or the Center for European Policy Analysis.

Cover: Assets from freepik.com were used.

ABOUT THE AUTHORS

Dr. Alina Polyakova is the President and Chief Executive Officer of the Center for European Policy Analysis (CEPA). She serves on the board of the Free Russia Foundation and the Institute of Modern Russia and is professor of European studies at the Johns Hopkins School of Advanced International Studies (SAIS). Dr. Polyakova was the founding director for global democracy and emerging technology at the Brookings Institution.

Ambassador Daniel Fried is Ambassador Daniel Fried is the Weiser Family Distinguished Fellow at the Atlantic Council. Ambassador Fried served as Assistant Secretary of State for Europe and as NSC Senior Director under President Bill Clinton and President George W. Bush, and as Ambassador to Poland. He most recently served in government as State Department Coordinator for Sanctions under President Barack Obama.

ABOUT CEPA

The Center for European Analysis (CEPA) is a non-partisan think-tank dedicated to strengthening the transatlantic relationship. Headquartered in Washington, D.C. and led by seasoned transatlanticists and young leaders from both sides of the Atlantic, CEPA brings an innovative approach to the policy arena. Our cutting-edge analysis and timely debates galvanize communities of influence while investing in the next generation of leaders to understand and address present and future challenges to transatlantic values and principles.

The intentional use of misleading information to influence societies, or disinformation, presents a serious threat to the integrity of democratic systems. Authoritarian states regularly use it to exploit democracies' open information systems, presenting a significant national security threat that demands a purposeful and concerted response. This paper is the third in a series of papers that deals with how democracies can build resilience against disinformation. The first installment, Democratic Defense Against Disinformation,[1] *and its follow-up,* Democratic Defense Against Disinformation 2.0,[2] *unpacked the challenge of foreign-origin disinformation and suggested practical steps to deal with it, including actions by governments, social media companies, and civil society. The core argument was that defense against disinformation has to be rooted in democratic principles and values: transparency, accountability, and respect for freedom of expression. We must not become them to fight them.*

While domestic-origin disinformation is a more widespread (and growing) challenge, the tools to deal with foreign state-sponsored disinformation are broader. The Russian government was the first mover and innovator in exploiting the digital information environment to carry out influence operations against democracies, targeting the United States, Europe, and countries beyond.[3]

But while Russian interference in the 2016 U.S. elections awoke Americans and Europeans to the threat of disinformation, the response has not deterred the Kremlin, which has extended its efforts globally. Moreover, Russia is no longer the sole threat in the foreign influence game. The Chinese Communist Party (CCP) has far greater resources than Russia and a long track record of information manipulation and aggressive intervention in Taiwan and Hong Kong. With the Covid-19 pandemic, China entered the global disinformation space, targeting Europe, NATO, and the United States, working from the Kremlin's playbook. There is now growing evidence that Russia and China are working together to amplify anti-democratic narratives.[4]

Democracies have aimed to identify, expose, and build greater public awareness of state-sponsored disinformation with the goal of building up greater long-term resilience to information influence operations.[5] *But the adversaries adapt and evolve their strategies and tactics to circumvent exposure and attribution. Companies, researchers, and governments are playing whack-a-mole — responding to each disinformation campaign as it arises while trying (and failing) to keep up with new threats. To get ahead of foreign disinformation, democracies must develop a proactive strategy to prevent state-sponsored information operations in the first place.*[6] *That means getting off our back foot and getting on the offensive. This paper, written principally for the United States but hopefully applicable in adapted form to other countries, is a road map for how countries can get ahead of foreign disinformation. The new U.S. administration should lead the democratic community in this effort.*

Executive Summary

The United States and other democratic countries have made progress defending against foreign and domestic disinformation. Unevenly, but steadily, a structure for democratic defense against disinformation is emerging, consistent with the principles of transparency, accountability, and respect for freedom of expression. It includes:

- a growing network of disinformation detectors (led by civil society sometimes informed by government agencies);
- social media companies (responsive to public and legislative pressure) that constrict disinformation on their platforms;
- an informed media that exposes disinformation; and, potentially at a next stage,
- a regulatory framework that seeks to filter out inauthentic and deceptive behavior.

While defensive measures cannot block all disinformation, they can limit disinformation as more people learn to filter it out on their own ("social resilience").

But defense is working against a moving target. Purveyors of disinformation have grown more sophisticated and their tactics continue to advance. The line between domestic and foreign disinformation has blurred, with Russian agents using local actors as proxies to carry out disinformation operations. "Deepfakes" are progressing beyond the ability to detect such content in real time. China and other foreign players (Iran, for example) have also entered the disinformation game.

Defensive tactics based on democratic values can mitigate the impact of disinformation, but there remains a mismatch between the fast-evolving threat and the slow implementation of efforts to manage it.

We, therefore, recommend supplementing defense with offense. Our recommendations are designed for the United States; some may be adaptable by European governments and the European Union (EU) as well. Offense does not mean spreading disinformation (that would not be consistent with democratic values and democracies aren't good at it anyway). It does mean building up:

- **Cyber tools** to identify and disrupt foreign disinformation operations. The U.S. Cyber Command (USCYBERCOM) has already launched this option — the U.S. military terms it "hunt, surveil, expose and disable." It has the appeal of immediacy and directness, but at its harder-edged end it has drawbacks. The "disable" option needs to be implemented with care.
- **Sanctions (and other financial) tools** against disinformation actors and their sources of funding, and development of contingent retaliatory sanctions as a deterrent. Use of the sanctions tool requires persistence to apply well and its impact will be moderate rather than decisive. It will be more effective if carried out in parallel by the United States, the EU, and the United Kingdom.
- **Support for free media** in the broad sense, including journalists, activists, and independent investigators, can be the most effective tool of counter-disinformation. It is asymmetric — it does not directly counter disinformation — but plays to the greatest strengths of free societies dealing with authoritarian adversaries: the inherent attraction, over the long run, of truth. This was a key lesson of the Cold War, when 20th century methods, e.g., support for independent radio broadcasting at Radio Free Europe/Radio Liberty (RFE/RL), proved

effective in reaching societies inside the Soviet Union and Soviet Bloc. Today, updated technologies, including direct, although unofficial, support for activist journalists working both inside and outside Russia (and China) may become a 21st century equivalent. China's media and internet landscape is more restrictive than Russia's but options exist there as well. These activities can be slow to yield measurable results but can have strategic impact over time, if applied with creativity and determination.

The United States and, to some degree, the EU, NATO, and some European national governments, are already applying versions of these tools, but often haphazardly, without integrating them into a policy framework and with only spotty coordination. For the first two levels of tools, governments will have the lead; for the third, civil society groups will be critical and, in some cases, leading actors.

> While defensive measures cannot block all disinformation, they can limit disinformation as more people learn to filter it out on their own

The new U.S. administration under President-elect Joseph R. Biden Jr. is likely to be more committed to developing a strategic response to disinformation, and be more effective generally, in crafting and implementing policies. U.S. President Donald J. Trump's mixed signals with respect to Russian disinformation, attacks on free media, and distracting fights with European allies prevented a coordinated response and set the United States back[7]. Recovering from these setbacks will not be easy, but the new Biden administration will have a roadmap for what to do.

Defense Against Disinformation: A Mixed Report Card

The good news

Emerging whole-of-society counter-disinformation activities: Transatlantic democracies — governments, researchers, and the private sector/social media companies — have generally moved beyond denying the disinformation challenge (or describing disinformation in awestruck terms as insurmountable) to testing solutions.

- **EU's actions:**
  - **2015:** The European External Action Service (EEAS) established the **EastStratCom Task Force** to identify and raise awareness around Russian disinformation campaigns against EU member states. Initially deeply underfunded with few staff members, the task force finally received significant EU budget support and expanded to 16 members by 2020. The EUvsDisinfo database now holds almost 10,000 examples of disinformation.[8] But the future of the taskforce remains uncertain as it is not a permanent unit and relies on staff seconded from EU member states.
  - **2018:** The European Commission developed an **Action Plan Against Disinformation**[9] and concluded a voluntary **Code of Practice on Disinformation** with major social media companies, which lays out policy norms to restrict disinformation. The enlisted companies, initially including Facebook, Google, Twitter, and Mozilla, now joined by Microsoft and TikTok,[10] have been providing monthly reports to the European Commission. The results appear

France's President Emmanuel Macron gestures as he speaks to the press after a plenary session at the Bellevue centre in Biarritz, France August 25, 2019. Ludovic Marin/Pool via REUTERS.

mixed in terms of the detail of data provided, independent verification, and lack of standard terminology and report structure.[11]

- **2019:** In preparation for the EU parliamentary elections in May 2019, the EU established a **Rapid Alert System** to facilitate information sharing, expose disinformation in real time, and coordinate with other multilateral efforts by the G-7 and NATO. Critics have noted that the system has yet to issue an alert, but EU officials assert that the system is working.

- **2020:** The EU is integrating lessons learned from previous efforts into two broader policy initiatives — the **European Democracy Action Plan** (**EDAP**) and the **Digital Services Act** (**DSA**) — to be finalized at the end of 2020. The former will likely lay out next steps on the Code of Practice and may help turn currently voluntary measures into regulation. The DSA, on the other hand, takes an expansive view of digital regulatory policy, including the likely establishment of an independent body to regulate everything from data use to rules of the road around emerging technologies and e-commerce.

- **Notable actions by European national governments:**

  - **Sweden:** Most European governments have established counter-disinformation teams to coordinate governmental efforts to identify and respond to disinformation operations, but

  Sweden has long been ahead in identifying the threat, analyzing its societal vulnerabilities, committing significant resources, and developing a strategic plan. The Counter Information Influence Section at the Swedish Civil Contingencies Agency (MSB) leads the effort and a newly expanded Psychological Defense Agency is in the process of being established by 2022.[12] The agency has trained more than 14,000 Swedish public servants in the subject of information influence since 2016.

  - **France:** In 2018, French President Emmanuel Macron launched the **Paris Call for Trust and Security in Cyberspace** that seeks to establish international cyber norms. It has, as of this writing, attracted backing from 78 governments, civil society groups, and a number of major European and U.S. corporations (including Facebook, Google, and Microsoft).[13] Notably, Amazon, Apple, and Twitter have not joined the Paris Call. And while the United States opted out of it, its platform provides a valuable space for multi-stakeholder discussions.

    France's domestic initiatives to regulate disinformation through content moderation have been far less successful. In June 2020, a French court struck down as unconstitutional a hate speech law passed by Parliament and supported by Macron's government.[14] The so-called Avia Law would have forced social media platforms to take down content reported by users as hateful within 24 hours or face fines of up to €1.25 million ($1.46 million) among other stringent provisions. The French court's ruling saw the law as infringing on free speech. The ruling was a major blow to the Macron government's counter-disinformation policy.

  - **United Kingdom:** Following the poisoning of former Russian spy Sergei Skripal by Russia's military intelligence service, the GRU, in Salisbury in 2018, the UK government developed a whole-of-government approach to responding to disinformation attacks. The effort is led by the Department for Digital, Culture, Media and Sport (DCMS) which coordinates efforts to expose foreign disinformation, alert the public, and assess appropriate responses through a counter-disinformation cell that engages intelligence agencies, tech experts, the Foreign Office, as well as other government agencies. The UK's broadcast regulator, Ofcom, is involved in an ongoing investigation of China Global Television Network (CGTN) for its broadcasting of illegally obtained "confessions."[15]

- **Multilateral institutions' actions:**

  - **NATO:** The **NATO Strategic Communications Center of Excellence in Riga**,[16] established in 2014, and the **European Center of Excellence on Countering Hybrid Threats in Helsinki**[17] (the Helsinki Hybrid CoE, established in 2017, that works with both the EU and NATO) are active in identifying disinformation among other hybrid threats and sharing best practices for countering them. Both have added Chinese disinformation to their areas of responsibility. Their focus is primarily on research and coordination, however, and neither has the power to affect and mandate policy.

    - **G7:** In 2018, the G7 established the **Rapid Response Mechanism (RRM)** at Canada's initiative. The RRM aims to coordinate information sharing and respond to "malign and evolving threats to G7 democracies" and grew out of the Charlevoix Commitment on Defending Democracies from Foreign Threats.[18]
    - **United Nations:** In the wake of disinformation campaigns around the Covid-19 "infodemic," the United Nations launched an initiative called **Verified** to counter the spread of misleading information on the public health crisis. It relies on individuals to sign up as volunteers to receive verified content and share in their communities and social media. This "crowdsourcing" approach is a public-private partnership and takes on a novel approach that relies on private citizens to be trusted community messengers.[19] Though its sustainability remains in question, the program had recruited 10,000 volunteers worldwide as of July 2020.[20] The U.N. and the World Health Organization (WHO) have also partnered with Facebook, WhatsApp, and other messaging services and telecom operators to deliver accurate information about the pandemic.
- **U.S. actions:**
    - The U.S. government's **Global Engagement Center** (GEC, housed at the State Department) has a mandate to counter state-sponsored disinformation, adding to its original mandate to counter terrorist and Islamist propaganda. With significant congressional funding of $64.3 million and an additional $138 million requested for 2021, the GEC has provided funding to independent research groups in Europe and elsewhere to carry out counter-disinformation research and develop monitoring tools.
    - The **U.S. Cyber Command (USCYBERCOM)** has gained prominence through its actions targeting purveyors of disinformation and a new proactive posture that USCYBERCOM calls "persistent engagement" as part of the Department of Defense's "defend forward" framework.[21]
    - The **U.S. Congress** has been considering legislation that would constrict the space for disinformation. The **2017 Honest Ads Act** would mandate social media platforms to keep a public database identifying purchase of paid political ads while preventing foreign entities from purchasing online political ads (as is the case with non-digital ads). While the bill has stalled in Congress, companies have *de facto* implemented its main provisions through their own policies. The **2019 Digital Citizenship and Media Literacy Act** would allocate $20 million in funding for media and digital literacy education in U.S. public schools. This bill has also not passed Congress.
- **Notable private sector actions:**
    - **Coordination among companies:** Social media companies and others are implementing counter-disinformation policies regarding issue and other political ads, taking down coordinated inauthentic behavior, labeling misleading information and state-sponsored media outlets, working more closely with civil society groups concerned about disinformation, and generally engaging more with researchers and governments.

   - Ahead of the 2020 U.S. elections, LinkedIn, Pinterest, Reddit, Verizon Media, and the Wikimedia Foundation joined Google, Facebook, Twitter, and Microsoft to coordinate with the U.S. intelligence community to identify disinformation campaigns.[22] This led to several takedowns of coordinated inauthentic behavior, including the removal of a network linked to the Kremlin-connected troll farm Internet Research Agency (IRA) from Facebook.[23]

- **Twitter**, once seen as the most problematic of the platforms given the extent of the IRA's activities and the ease of access, is now an industry leader in setting the policy agenda. The company has banned:

   - advertising by all state-controlled media, including RT and Sputnik[24] and

   - all political advertising.

  It has extended and refined policies, including:

   - labeling state-controlled media and key government accounts, initially from the United States, the UK, Russia, France, and China;

   - a framework for labelling and removing manipulated or synthetic media and misleading information intended to undermine public confidence in an election; and

   - a policy framework for limiting coordinated harmful activity, which has reduced the reach of such content.

  Twitter continues to be the only social media company to publish a full archive of the information operations it has removed, including all the tweets and related media. In October 2020, Twitter announced additional policies aimed at reducing disinformation with respect to the 2020 U.S. elections.[25]

A Burgeoning Sector of Disinformation Research Groups

What was once a niche specialty has evolved into a burgeoning field of research, in both the nonprofit and private sectors. Early responders from frontline states, such as the Baltic Elves and Ukraine's StopFake, are now part of a large global network of universities, think tanks, nonprofit research groups, consultancies, and independent media organizations.[26]

Governments and foundations have increased funding for counter-disinformation efforts, while companies and political campaigns now recognize the need to understand the threat and respond. Groups long devoted to counter-disinformation are developing ties with other civil society groups new to the topic, including U.S. domestic civil right groups (e.g., the **Congressional Black Caucus Foundation** and the **Leadership Conference on Civil and Human Rights**) which have discovered that Russian-origin disinformation is linked to U.S. right-wing extremist groups and others with a bigoted policy agenda (e.g., restricting minority voting rights).[27] The ability to monitor, identify, and expose disinformation operations is rapidly improving as information sharing between these groups grows.

A whole-of-society response is still in nascent stages

The abovementioned efforts constitute an emerging structure for democratic defense against disinformation: a growing network of disinformation detectors (led by civil society sometimes informed by government agencies), social media companies (responsive to public and legislative pressure) constricting disinformation on their platforms, informed media alert to disinformation campaigns and exposing them, and a careful regulatory framework (reflecting a developing set of international norms) targeted less at content control and more at filtering out inauthentic and deceptive behavior.

Defensive measures cannot filter out all disinformation. No doubt, some individuals will believe even exposed falsehoods if they tend to confirm preexisting biases. But at their best, defensive measures can limit disinformation as societies slowly learn to filter it.

The bad news

Defensive efforts are still at an early stage, sometimes in sketch form only, and often merely attempting whack-a-mole against an evolving threat.

A rapidly evolving threat: Disinformation campaigns have grown more sophisticated. For instance:

- The production of increasingly credible disinformation content using artificial intelligence (e.g., "deepfakes" or "synthetic media") is rapidly progressing far beyond the ability to detect such content in real time.
- Foreign state-sponsored disinformation operations, no longer restricted to the frontline states of Central and Eastern Europe in the case of Russia or Taiwan and Hong Kong in the case of China, pose a global threat.
- The line between domestic and foreign disinformation has blurred. Working through local proxies, disinformation purveyors are able to hide the true source of online content. In Ukraine, Africa, and Latin America, Russian agents used local actors as proxies to carry out disinformation operations. They set up shell media and social media companies, attempted to convince unsuspecting individuals to "rent out" their social media accounts and contracted local journalists to publish misleading content.[28] Such tactics obfuscate detection by blending in with domestic voices and taking away a telltale sign of foreign interference: the use of foreign-based accounts whose location gives away their true identity.

As China has entered the disinformation game, its approach has not simply copied the Kremlin's playbook. Rather, Beijing is deploying a more far-reaching and deeply embedded set of tools to sway public opinion in democratic societies, using the full scope of China's economic and political power. China's "sharp power" strategy, documented by the National Endowment for Democracy, aims to penetrate the political and information environments in target countries.[29] With China's mishandling of the early stages of the Covid-19 pandemic facing international criticism, Beijing has stepped up its information influence operations aimed at Western democracies, highlighting shortcomings in their public health systems, promoting its own efforts to provide medical and personal protective equipment, and attempting to curb international political contacts with Taiwan.

Policy responses woefully lag

In the meantime, policy steps taken by key players remain uneven.

- Notwithstanding constructive steps, **social media companies have inconsistent approaches to the challenge of disinformation**. For example, Twitter bans political ads while other social media platforms do not. In another inconsistency, when confronted in May 2019 with a deceptively altered

Twitter CEO Jack Dorsey is seen testifying remotely via videoconference as U.S. Senator Chris Coons (D-DE) listens during a Senate Judiciary Committee hearing titled, «Breaking the News: Censorship, Suppression, and the 2020 Election,? on Facebook and Twitter's content moderation practices, on Capitol Hill in Washington, U.S., November 17, 2020. REUTERS/Hannah McKay/Pool.

video of Nancy Pelosi, speaker of the U.S. House of Representatives, YouTube removed the video, Facebook de-ranked it, and Twitter let it stand.[30] Inconsistent standards can be exploited by purveyors of disinformation, who can tailor their tactics to exploit the gaps and opportunities.

Social media companies have concentrated on takedowns of inauthentic content. That is a good (and publicly visible) step but does not address **deeper issues of content distribution** (e.g., micro-targeting), algorithmic bias toward extremes, and lack of transparency. The EU's own evaluation of the first year of implementation of its Code of Practice concludes that social media companies have not provided independent researchers with data sufficient for them to make independent evaluations of progress against disinformation.

- **Implementation of the EU's policy framework for combating disinformation remains spotty.** European critics have characterized the EU's Rapid Alert System (RAS) on disinformation as being neither rapid nor alert nor a system; that may be unfair, but the RAS does seem off to a slow start.

- **The United States still lags the EU** (and many EU member states). While the United States has sometimes acted with strength against purveyors of disinformation, e.g., by indicting IRA-connected individuals,[31] U.S. policy is inconsistent. The U.S. government has no equivalent to the European Commission's Action Plan Against Disinformation and no corresponding Code of Practice on Disinformation, and there remains no one in the

U.S. government in overall charge of disinformation policy; this may reflect the baleful U.S. domestic politics and Trump's mixed or worse messages on the problem of Russian-origin disinformation.

- Aside from funding the State Department's Global Engagement Center, **congressional work on countering disinformation has slowed**, with even the Honest Ads Act stalled.
- Longer-term tools to encourage **public sophistication about disinformation** and thus social resistance to it are being developed in some European countries (e.g., Finland and Sweden), but **barely beginning in the United States.**
- **A lack of coordination between Europe and the United States on policy responses** to disinformation has produced two different tracks: Europe focuses on identifying and exposing disinformation, while the United States investigates, names, and shames, though inconsistently. Neither has sought to develop a regulatory framework to increase authenticity and integrity in the social media space.

A combination of defensive tactics based on democratic values can be effective in at mitigating the impact of disinformation in the short term. But the fast-evolving threat and the slow implementation of policies, practices, and long-term social antibodies (so to speak) to manage it are still mismatched in favor of disinformation; defense needs to be supplemented with offense.

Stop the Whack-a-Mole Approach: Get on the Offense

Democracies also need to go on offense: to take the fight more directly to the purveyors of disinformation and the regimes that sponsor and direct them. Effective offense can take many forms. Some can raise the costs and may change the incentive/risk calculus for governments contemplating disinformation campaigns and perhaps establish a measure of deterrence. Others can weaken technical capabilities to conduct disinformation operations and thus serve as tactical supplements for defense against disinformation. Still other forms of offense can challenge regimes that use disinformation in strategic ways: Vladimir Putin's regime in Russia seems to use disinformation to weaken its democratic adversaries by attacking their social cohesion; democratic countries can answer this through support for free media inside Russia, China, and other purveyors of disinformation, working nationally or together.

Care and caution are still required. **The principle of remaining true to democratic values holds as much for offensive as for defensive options.** We must not become them to fight them. Democracies should not attempt their own version of disinformation. Doing so would undermine the values that democracies seek to defend, creating a moral equivalence (one that would bolster the cynical arguments of Russian propagandists about democracy being mere fraud). Besides, if the history of the Cold War is any guide, democracies are no good at disinformation.

Democratic countries have options. Democratic offense against disinformation can draw on three levels of tools:

- **Cyber tools** to identify and disrupt disinformation operations. This option is already in use and has the appeal of immediacy and directness. It is essential but at its harder-edged end has drawbacks, e.g., the risk of escalation.
- **Sanctions (and other financial) tools** against disinformation actors and their sources of funding, and development of contingent retaliatory sanctions as a deterrent. Use of the sanctions tool

requires persistence to apply well and its impact will be moderate rather than decisive.

- **Support for free media** in the broad sense, including journalists, activists, and independent investigators. With respect to Russia, this could include those operating both inside and outside the country. This option can be slow to yield measurable results but can have strategic impact over time, if applied with creativity and determination.

The United States and to some degree the EU, NATO, and some European national governments are applying versions of these three levels of tools, but often haphazardly, without integration into a policy framework and with only spotty coordination. For the first two levels of tools, governments will have the lead; for the third, civil society groups will be critical and, in some cases, leading actors.

Cyber Options

The Department of Defense's Cyber Strategy summary issued in September 2018 stated that the United States would "**defend forward**" and "**persistently contest**" malicious cyber activity, with specific reference to Russia and China, and emphasized Russian disinformation operations as a particular challenge.[32] The National Security Presidential Memorandum, **NSPM-13**, issued around that time, reportedly gave new authorities to the U.S. military, with USCYBERCOM in the lead, to engage in certain cyber offensive actions below a certain threshold.[33]

While the new cyber strategy covers far more than the disinformation challenge, what the policy could mean with respect to offensive counter-disinformation operations became clear when *The Washington Post* reported that around the time of the 2018 U.S. mid-term elections, **USCYBERCOM had attacked and temporarily disabled the IRA**, the St. Petersburg troll farm which had long been identified as a major source of Russian disinformation targeting the United States.[34] This information, probably leaked by USCYBERCOM itself, remains the United States' most notable publicly reported counter-disinformation offensive operation. USCYBERCOM appears to be continuing such efforts, including reportedly against a criminal Russian botnet.[35]

Democracies should not attempt their own version of disinformation.

Cyber offensive operations (rightly) remain classified, but Gen. Paul Nakasone, simultaneously director of the National Security Agency (NSA) and commander of USCYBERCOM, has outlined the basics of the strategy publicly.[36]

USCYBERCOM has offered a set of offensive actions meant to disrupt and disable the internet infrastructure behind major disinformation operations. The concepts reflect intelligence capabilities, such as reconnaissance, gaining deep access and adversary awareness. Nakasone's statements[37] and people familiar with the program see options for actions on four levels: "hunt, surveil, expose, and disable."

- Hunt includes actively seeking out adversarial activities and entities before an attack takes place.
- Surveil includes probing foreign disinformation systems to identify bad actors and the details of related software, malware, and viruses used in disinformation and related operations.
- Expose includes the release on a selective basis of the details of disinformation operations, including personnel, methods, and specific campaigns. This information could be provided to internet service providers (ISPs), social media companies, and

friendly third countries. Exposure could also include conveying such information to the media or to civil society groups that follow and combat disinformation, either directly or through third parties, to out bad actors and expose networks and operational habits. Exposure will have different outcomes depending on the actor: whereas Russia simply denies any accusations, regardless of the evidence presented, China has, in the past, responded by reducing its attacks on U.S. companies.

- Disable could include disrupting the infrastructure used to wage disinformation operations through a variety of means (e.g., redirecting command and control of adversary malware, degrading the infrastructure of prime Russian disinformation sites, and other means to target or compromise systems). This was the level of attack reportedly chosen against the IRA.

Under NSPM-13, as reported, USCYBERCOM (with additional input from policy agencies) has a degree of latitude regarding which targets to choose. Reportedly, the threshold for targeting Russian government entities, e.g., the GRU cyber units responsible for the hacking operations against the Democratic National Committee's computer system in 2016, is higher than that for nominally non-Russian government bodies such as the IRA or proxies of the Russian government or Kremlin. If accurate, this would be a wise distinction to make, especially with respect to disabling operations.

Opportunities and cautionary notes

The general appeal of applying cyber offense options to go after foreign disinformation targets is clear, more or less on the grounds of "they have it coming," and the capacity for effective action seems to exist. Recognizing that much of the policy and operations is classified, we offer the following assessment and recommendations with respect to the reported cyber tools:

Deploy the "hunt" and "surveillance" tools. Use of the U.S. government's cyber capacity to gain intelligence on state-sponsored disinformation operations, technical details, and actors appears valuable. The leads for such actions might have been placed elsewhere, e.g., in the intelligence community rather than in the military, but it is important that they exist and are being employed.

Expose (with tactical forethought) foreign disinformation operations, especially to friendly governments, ISPs, social media companies that are active and responsible in countering disinformation, and civil society activists. In some cases, it may be advisable to filter such information so it reaches some (e.g., foreign civil society activists) through third parties rather than the U.S. government. USCYBERCOM or the NSA may not always be best placed to do liaison work with non-U.S. (and even some U.S. non-U.S. government) partners, so a smooth interagency process for providing relevant information to outside groups will be important. The NATO Strategic Communications Center of Excellence in Riga and the Helsinki Hybrid CoE, especially by linking up with civil society activists, should organize themselves to act as early warning centers.

Providing U.S., European, and other media with general information about Russian (and Chinese) disinformation operations — exposing operational details, individual bad Russian actors, and Russian organizations and their foreign collaborators — seems like sound policy. The IRA is now widely known and the GRU's cyber units are becoming so, but these are unlikely to be the only Russian entities engaged in disinformation and related activities. The exposure of new names and organizations can limit future disinformation operations.

A subset of exposure can include reaching out directly to individuals engaged in disinformation (as USCYBERCOM is reported to have done with respect to employees of the IRA). According to various reports, many of these individuals are ordinary, tech-savvy Russians not fully aware of the impact or nature of their own activities. Letting them know that their identities are known, that they can be exposed, and that sanctions (e.g., bans on visas to the United States and Europe and/or asset freezes) can be applied may have a deterrent effect.

Such operations must be carried out with care. Decisions about when and how much to reveal about certain individuals associated with disinformation, especially third-country enablers of Russian disinformation operations (either witting or "useful idiots"), should be considered on an interagency basis, incorporating input from regional experts from the State Department about how to make best use of such revelations, especially those involving third-country nationals. In some cases, revelations about Russian disinformation operations can be provided discreetly, in small batches, to credible media. In other cases, it might be more effective to prepare bespoke counter-disinformation campaigns intended to blunt or preempt specific Russian campaigns. Such decisions, and preparation for such campaigns, should likewise be made with strong interagency input.

U.S. intelligence agencies are increasingly cooperating with both social media platforms and researchers to flag suspicious operations. A September 2020 takedown of a (relatively small) IRA operation was an example of successful cooperation between the U.S. government, platforms, and researchers.[38]

Be judicious about disabling and disrupting disinformation targets. Few shed tears over reports that in 2018 USCYBERCOM temporarily shut down the IRA and let some of the individuals working there know that the U.S. government was aware of their activities and identities. That operation received broad support from those who follow disinformation because the target was notorious, unofficial (though a tool of the Kremlin), and had a long track record of disinformation, including in the United States.

It will be important to maintain this relatively high bar for such operations going forward: **targets chosen for active disabling operations should be nefarious** (i.e., major and not peripheral players in disinformation, whether publicly known or not). A high degree of confidence on attribution is key — while the Kremlin (or Beijing) will likely deny any involvement in information influence operations even when presented with undeniable facts, that attempt at plausible deniability should not prevent our ability and intent to act.

While not familiar with the details of the classified NSPM-13, we recommend that senior U.S. government interagency sign off be required for any cyber disabling operation against any foreign target. Using cyber means to go after Russian or other countries' assets carries risks of escalation and retaliation beyond the disinformation realm, potentially into targeting civilian infrastructure more generally. This is not an argument for inaction, but for care and discipline.

Get organized. USCYBERCOM may be the lead element of the U.S. government's cyber action, including counter-disinformation, but it should not be responsible for strategic decision making, including with respect to counter-disinformation. According to many in the U.S. government, the interagency structure for counter-disinformation remains weak, with lines of authority unclear. This is especially true with respect to Russia, for reasons related to Trump's own benign views about Putin and resistance to accepting the facts about Kremlin disinformation operations during the 2016 elections and those ongoing.

Ft Meade, MD - U.S. Cyber Command is employing a new virtual training platform, the Persistent Cyber Training Environment, during Cyber Flag 20-2. Over a period of two weeks, Cyber Flag 20-2 will host more than 500 personnel worldwide, spanning nine different time zones and 17 cyber teams. Credit: U.S. Cyber Command photo by Chief Mass Communication Specialist Jon Dasbach.

No private cyber "disabling" action. Involvement of civil society in countering disinformation — offense as well as defense — can be critical. Civil society and research groups, e.g., Bellingcat, the Atlantic Council's Digital Forensic Research Lab, the Stanford Internet Observatory, EU DisinfoLab, and private companies such as Graphika have played a key role in defense against Russian disinformation by uncovering campaigns and exposing methods. They are already significant actors helping to surveil and expose Russian disinformation operations. As noted above, we recommend robust (and hopefully real-time) exchange of information. Disabling operations initiated by private cyber actors, however, even directed against non-official state disinformation targets, risk triggering unwanted cycles of escalation and should not be part of the menu of offensive tools.

Cyber offense is an essential, not decisive, tool in the counter-disinformation tool kit. The tools of cyber offense, already in play, are apt to be useful to limit the threat and thus worth pursuing. But we also suspect that their effectiveness will be at the margins. This is often as good as it gets, but we should not expect that cyber offense against disinformation will prove decisive. We have entered a shadow world of move and countermove in the cyber realm and its disinformation subset. USCYBERCOM's and other U.S. government cyber tools are useful but, as they themselves would acknowledge, incomplete.

Sanctions (and Other Financial) Tools

Sanctions have been used since the end of the Obama administration against Russian purveyors of disinformation, though not with a focus commensurate with the threat. Headroom remains for additional action using existing authorities and options exist for other forms of financial pressure against purveyors of disinformation. By sanctions, we mean exercise of the Treasury Department's authorities under the International Emergency Economic Powers Act (IEPPA), which essentially allow the U.S. government to freeze the assets of a foreign person — physical or legal — within the United States and to cut off that person from use of and access to the U.S. dollar. Because of the extent of the dollar's use in global finance, being placed under full Treasury blocking sanctions means that the sanctioned person is effectively cut off from the global financial system.

A slow start for sanctions options. Aware of Russian disinformation operations during the 2016 U.S. presidential election, the **Obama administration issued Executive Order 13757 on December 28, 2016 (well after the elections) and used it to impose full blocking sanctions on Russian targets** which had engaged in malicious activities against the United States, including election interference. These targets included three small Russian cyber companies, four Russian individuals, the Russian intelligence service (FSB), and the GRU.[39] These latter targets are prominent, but unlikely to suffer much due to sanctions. Around the same time, **the U.S. government also imposed full blocking sanctions on Yevgeny Prigozhin**, nicknamed "Putin's chef," who has functioned as a conduit for funding aggressive Russian operations in Ukraine, Syria, and (more recently) Africa.[40] The Obama administration designated (i.e., sanctioned) Prigozhin using separate Ukraine-related sanctions authorities, but by that time Prigozhin was publicly known to be a supporter of the IRA. EO 13757 was more usable than its 2015 predecessor, EO 13694, which it amended, but still provided a high bar to sanctions against malicious cyber actors engaged in disinformation operations.

The Trump administration has had its own challenges addressing Russian disinformation directed against the United States (not least due to Trump's reluctance to acknowledge its existence). Nevertheless, in **September 2018, the Trump administration issued EO 13848 providing broader authority for the U.S. government to impose sanctions against those interfering in a U.S. election** (EO 13848's preamble explicitly notes "covert distribution of propaganda and disinformation" as part of the national security threat that the EO seeks to address).[41] One year later, the Trump administration imposed its first sanctions using this EO: it designated the IRA as a whole, six of its employees (four of whom had been previously designated under EOs 13694 and 13757), and identified some Prigozhin-owned companies and property, such as luxury aircraft and a yacht.[42]

To escalate pressure on purveyors of disinformation, we recommend the following:

- Intensify the use of existing sanctions authorities after the 2020 election cycle. EO 13848 should be deployed as post-election analysis reveals the extent of disinformation operations. Potential targets should include individuals engaged in disinformation operations, organizations that generate disinformation (the IRA is probably not the only such Russian outfit), and their funding sources. Any financial dealings with already-sanctioned individuals and organizations would provide grounds for derivative sanctions against such persons. So, collaborators, agents, funders, and business partners of disinformation operators or operations, whether Russian, U.S., or third-country nationals, would be subject to being sanctioned. Discretion, especially when contemplating third-country or U.S. individuals, is wise; sanctioning on auto pilot would not be. The net result of a such a Russia-focused sanctions program, if applied rigorously (at the level of the current Iran sanctions program, for example), could be to expose and isolate the Russian disinformation apparatus.

To implement such a program, resources at Treasury's Office of Foreign Asset Control (OFAC), which administers financial sanctions, would need to be increased to allow for targeting research. The intelligence community and USCYBERCOM could also furnish OFAC with potential targets, as could the State Department, drawing on its contacts with civil society groups that monitor the Russian disinformation network.

- Develop new sanctions authorities. Pending legislation, including the Defending Elections from Threats by Establishing Redlines Act [**DETER**, introduced by U.S. Sens. Marco Rubio (R-FL) and Chris Van Hollen (D-MD)]; and the Defending American Security Against Kremlin Aggression Act [**DASKA**, introduced by U.S. Sen. Lindsey Graham (R-SC) and Robert Menendez (D-NJ)] include provisions for escalating sanctions and other economic pressure in response to interference in the 2020 U.S. elections.[43] DETER explicitly includes disinformation in its definition of election interference. DASKA, in its current iteration, does not. Instead, it focuses more on the administration of elections, though its definition could include certain forms of disinformation, e.g., if it impeded voting rights. New versions of these acts are likely to be introduced in the next session of Congress, which starts in January 2021.

DETER and DASKA mandate strong financial and other sanctions should the administration determine that election interference has taken place. DETER mandates sanctions on major Russian state banks and energy companies (potentially including Gazprom), new sovereign debt, and Russian oligarchs. DASKA (in the version approved in December 2019 by the Senate Foreign Relations Committee) includes sanctions on individuals with corrupt ties to Putin, their family members who benefit from such dealings and persons who facilitate such ties; investments in Russian LNG projects outside Russia; new sovereign debt; and financial institutions that support election interference.

In general, DASKA's sanctions provisions seem more practical than DETER's. DETER's full blocking sanctions against major Russian state banks risk financial blowback and its full blocking sanctions against Russian energy companies could disrupt world energy flows and expose European customers. The sanctions authorities should be refined if and as the bills advance.

- Establish powerful but contingency sanctions to deter future Russian and Chinese election interference. This is a sound approach (and a better practice than imposing sanctions for past malicious behavior). But while election interference, the target of these bills, can include disinformation, it is a far bigger and broader category of malicious action than disinformation. Strong sanctions can be imposed for the first time only once, and to establish deterrence, the bar for action should either be placed high or with some flexibility to impose some sanctions in response to disinformation and more in response to additional, aggressive election interference, such as attacks on election infrastructure.

- Apply additional tools of financial statecraft**.** Sanctions are not the only options in the offensive arsenal against disinformation. Putin's ruling elite and their supporters are known to keep their personal wealth hidden in offshore accounts. Those who attack the democratic West appear to have more confidence in it and its financial system than that of their own country. Working with the UK and the EU, the United States should develop and implement authorities to restrict hidden Russian wealth flowing anonymously to high-end real estate (in London, Miami, New York, and other locations) and through anonymous limited liability companies (LLCs) into the United States. For reasons of good financial practice and anti-corruption, the United States, together with key allies (the UK, especially), should develop and enforce standards of transparency. The United States and key allies could, however, prioritize identifying and exposing the funds and money flows of key players in the Kremlin disinformation world and respond asymmetrically to disinformation campaigns by constricting Putin and his cronies' financial freedom. Financial forensics can also reveal proxy networks and infrastructure preparations for future influence campaigns, which can enhance preemptive measure to disable such networks before an attack is carried out.

'The Truth Shall Set You Free': Support for Free Media

Support for free media — in this case for the purpose of fighting Russian and Chinese disinformation with support for true information — may sound naïve. It shouldn't. In fact, of the offensive options we regard it as having the greatest long-term potential against disinformation. Cyber offense and sanctions can put pressure on disinformation networks and may provide a measure of deterrence against election interference that includes disinformation. Support for free media, if sustained, can be a strategic tool that challenges the brittleness, and exposes the corruption and brutality of the Russian and Chinese systems that use disinformation in aggression abroad and to sustain themselves at home. Disinformation is a weapon of authoritarians; support for freedom of information is part of the arsenal of democracy. We have options, but they must be curated to each country's media landscape.

Russia's media landscape. One of Putin's first steps as he imposed authoritarian governance on Russia was to seize control of independent television networks, forcing some of its leaders out of the country. [44] State-owned/Kremlin-controlled media, both television and radio, dominate broadcasting and have for many years. The last remaining independent television network — Dozhd (rain in Russian) — is under pressure from Russian authorities but has not yet been shut down. Some independent (or semi-independent) radio stations, such as Ekho Moskvy (Echo of Moscow in Russian), continue to function, also under pressure. Print journalism has greater latitude for free expression, e.g., *Moskovskiy Komsomolets* and especially *Novaya Gazeta* (recalling to some extent the Soviet practice of allowing some publications somewhat greater editorial latitude in an effort to limit disaffection).

The internet in Russia, however, remains a space of contested freedom, with independent journalists and civil society struggling with state attempts to exert control and massive state trolling operations. Using social media platforms (YouTube is currently popular), a new generation of Russians is creating a proliferating community of pointed, independent, and investigative online journalism. For example, Roman

Dobrokhotov, editor in chief of the online publication *The Insider*, has published exposes on some of the hottest topics imaginable: the GRU's attempt to assassinate Skripal, the former Russian spy, in the United Kingdom in March 2018 using a nerve agent; the shootdown of Malaysian Airlines flight MH17 over Ukraine in July 2014 by Russian-controlled separatists; and, in cooperation with Bellingcat, the UK-based investigative journalism group, the role of the GRU in hacking e-mails of then French presidential candidate Macron. Each of these stories was a major embarrassment to the Kremlin. Dobrokhotov is only one of many Russian online journalists currently active.[45] As Russian state control intensifies, former journalists from once-independent traditional media have been migrating to online journalism, deepening its expertise and experience.

While analogies are inexact, **Russia's digital space can be considered the new "samizdat,"** or self-published, the term of art for underground publications during the Soviet period. It is decentralized, nimble, widespread, and more resistant to suppression.[46] It is thus the most promising element of Russia's remaining free media to support. While offensive tools against disinformation, such as cyber offense, sanctions, and other financial policy tools, are principally official, support for free media under Russia's current conditions must involve civil society as much as governments.

China's media landscape. Unlike in Russia, where the internet penetrated society in an open and relatively unencumbered way in the 1990s, in China, state-controlled media has dominated the information landscape since 1949. Large state-run media agencies, including Xinhua, China Central Television (CCTV), and *People's Daily*, are leading outlets in radio broadcasting, television, and print news. While private media exists in China, it must comply with government regulations that effectively prohibit content deemed sensitive, including content critical of the government of China and the CCP. As a result, China is one of the most restrictive countries in the world for press freedom, and Beijing has only accelerated its repression of independent voices in the internet age while clamping down on access to Western independent media.[47] This year, in retaliation for U.S. limits on the number of Chinese journalists in the country, China expelled journalists employed by *The New York Times*, *The Washington Post*, and *The Wall Street Journal*.[48]

Still, the advent of digital communications opened the door for a diversity of information sources to enter the Chinese public sphere. Chinese vloggers sometimes command a huge audience at home and increasingly abroad. Diversity of information should not be mistaken for freedom of expression, however: private companies and individuals must work within the CCP's defined lines. Crossing these redlines, which shift frequently and randomly, carries severe consequences.[49]

China is ushering in the era of "splinternet" with its control of digital information at home and export of digital authoritarianism abroad. The "Great Firewall of China" — a series of governmental efforts to control digital information flows — was launched in parallel with the arrival of the commercial internet in China in the 1990s. Rather than providing opportunities for independent voices and dissent, as is the case in Russia, in China the internet has become an arena to further censorship, root out dissent, and develop sophisticated digital surveillance tools. Content on popular Chinese social media apps such as WeChat, Sina Weibo, and Baidu Tieba is filtered through algorithmic and human review. News aggregation applications such as Toutiao limit content not only as it pertains to politics, but also subjects deemed "generally degrading" to society.[50] The result is a Chinese-specific internet, which is blocked to many Western companies

Russian President Vladimir Putin (R) and Chinese President Xi Jinping attend an energy and business forum on the sidelines of the St. Petersburg International Economic Forum (SPIEF), Russia June 7, 2019. REUTERS/Maxim Shemetov.

such as Facebook, Twitter, and Google, and functions outside any international norms or rules around human rights or freedom of expression. Beijing's model is an enviable one to other autocracies, including Putin's Russia, that are actively importing Chinese surveillance technology with the hope of reproducing Beijing's digital authoritarianism.

Abroad, the Chinese government has expanded its reach in foreign languages. English-language publications, such as *The Global Times*, push messaging developed by the CCP's Propaganda Department (and, at times, go beyond the official line to take on an extremely nationalistic tone). China Radio International broadcasts from more than a dozen radio stations in the United States. Chinese newswires, which compete with Western newswires such as the Associated Press, have pushed state-controlled media into local news around the world by entering into creative partnerships with local news stations. CGTN, the international branch of CCTV, broadcasts around the world in five languages.[51] Chinese state-controlled media is widespread and easily accessible in many parts of the developing world where CCTV is included in the cheapest television packages, while other international news services are not.[52] The Chinese media make particular use of "cooperation agreements" with Western media outlets, which can seem innocent (e.g., sharing picture libraries and sports results) but easily become vectors for influence.

The tools for countering the CCP's grasp on information flows in China domestically are limited, and certainly more so than in Russia. Still, there is an expanding toolkit for trying.[53] Despite restrictive policies, citizens in Hong Kong and Taiwan are finding ways to maneuver around government censors. Hong Kong's independent media has been the target of police investigations following the passage of the so-called Hong Kong national security law, but sales of Hong Kong's *Apple Daily* still skyrocketed after the arrest of owner Jimmy Lai in August 2020.[54]

Taiwan has been a prime target of Chinese influence efforts for decades, just as Ukraine has been for Russia. Following Chinese disinformation campaigns around the 2018 Taiwanese elections[55] and a 2019 investigation that found Taiwanese news outlets to be taking editorial direction from the Chinese mainland,[56] the Taiwanese government passed legislation that heightens the penalties for attempted Chinese influence of elections. Under tech-savvy government officials such as Audrey Tang, Taiwan has also worked to revamp its technology governance, and built dedicated channels for disinformation reporting and volunteer groups of fact-checkers, meme-makers, and designers.[57]

Lessons learned. The long-term benefit of support for free media emerged from the U.S. experience contending with the Soviet Union. The United States sustained free media outside the Soviet Bloc, famously at the Radio Free Europe/Radio Liberty (RFE/RL) headquarters then in Munich, which employed journalists originally from Soviet-dominated Central and Eastern Europe and the Soviet Union to act as surrogates for free media forbidden inside their own countries. The United States supplemented these efforts with support for independent, underground journalism inside the Soviet Bloc, increasingly in the 1980s and especially in Poland after the rise of the dissident trade union Solidarity. These efforts were suited to the technology of the age: radio broadcasts and, occasionally, primitive technological support (e.g., provided through a variety of channels parts for mimeograph machines for use by the Polish underground press). The information provided to people of the Soviet Union and Soviet Bloc was vulnerable to interruption and outnumbered by the regime-controlled print and electronic media. Free media support programs were frequently derided in the United States and Europe as being of no consequence because of the then-consensus that communist regimes in Europe were effectively beyond challenge and that dissidents, the presumed, numerically small audience for such efforts, were and would be of no significance. Soviet propaganda and disinformation (the term of art of the time was "active measures") were regarded as more effective. As it turned out, however, support for free media was a significant factor in the fall of communism, as leaders of the new, democratic governments that came to power after 1989 often told U.S. diplomats.[58]

Recommendations

We recommend the following:

- Build on U.S. government "media support" programs. In the 1990s, U.S. government media support programs reflected the then-reasonable but ultimately mistaken assumption that Russia was on a path of systemic democratization. As Putin's authoritarian system emerged in the first decade of the 21st century, however, individual U.S. government agencies slowly adapted their thinking and programs. This, for the most part, remained the case during the Trump administration, despite mixed signals from Trump himself about Russia policy and even about media freedom.
- **The U.S. government should expand programs and agencies to support a sustained and top-level commitment to back free media.** Appointing new leadership at the U.S. Agency for Global Media (USAGM) that is

committed to its mission and not to the imposition of partisan controls seems a first step. In combination, these U.S. government programs, which grew independently, would be critical elements of a strategy of offense against Russian disinformation and part of a more consistent Russia policy. The incoming Biden administration will likely be prepared to push back against Russian aggression generally and would implement the programs noted above with greater consistency, especially given the damage the Trump administration inflicted on USAGM and its constituent elements.

The Biden administration should mobilize the individual agencies already active in support of Russian and Chinese-language free media to advance that objective. These efforts will need top-level leadership. The State Department's currently empty position of under secretary for public diplomacy, once filled, could play a role in leading the disparate interagency elements involved, working with a National Security Council staff likely to be stronger, particularly on Russia and China.

The U.S. government should **avoid short-term thinking or the trap of false metrics and impatience**. Investment in free media is long-term and impact is unlikely to occur in even increments and almost never on an annual budgetary cycle. By way of analogy: from 1983-86 the usual metrics suggested that media (and democracy support) programs in Central and Eastern Europe were failures. From 1987-90, the metrics indicted spectacular success. In fact, investment early led the way to eventual success, but outside the usual time cycle of program evaluation. Political support for such programs needs to be steady enough to avoid abandoning them prematurely, while operational management needs to be flexible enough to direct and redirect resources to what works best.

The U.S. government should expand programs and agencies to support a sustained and top-level commitment to back free media

Russia

- Increase media support funding. In Russia, such support would allow for a greater commitment across the board, and especially to more technical training, in anticipation of intensified efforts by the Russian regime to control access to the internet, and support for bringing together sometimes isolated individual online journalists in remote Russian towns and cities.

- **USAGM**, the successor to the Broadcasting Board of Governors, which oversaw RFR/RL and other U.S. broadcasting arms, has a mandate that includes support for independent journalists from authoritarian countries operating both offshore and in-country. Unfortunately, its current leadership seems focused on imposing partisan conformity to the detriment of independent journalism (its core mandate) and has replaced capable leaders of RFE/RL, Voice of America (VOA), and Radio Free Asia.[59]

- In November 2019, USAGM elevated the **Open Technology Fund** (OTF), created during the Obama administration by then Secretary of State Hillary Clinton, to a self-standing unit under USAGM with a $15 million budget. OTF's mandate includes support for technologies to help independent media actors evade censorship and other forms of contemporary internet blockage (The Trump administration has cut

OTF's funding, however.) **In-Q-Tel** (IQT), a high-tech venture capital firm chartered by the Central Intelligence Agency with a mandate to support the U.S. intelligence community with high technology, especially information technology, and the **Defense Advanced Research Projects Agency** (DARPA), which helped fund basic research that made the modern internet possible, may be able to contribute to this process.[60]

- **RFE/RL's television program, "Current Time,"** is an ambitious program to offer Russian-language television content produced by Russian journalists (along the old RFE/RL radio model), directed at Russian speakers inside Russia (in Russia it is available through satellite or the internet) and in neighboring countries. The audience of "Current Time" inside Russia is relatively small (estimates range from 1.9 million to just under four million), though once entering the Russian digital conversation stream, its reach is likely larger than the direct audience numbers.[61]

- **USAID's** Bureau for Europe and Eurasia has launched an initiative, "Countering Malign Kremlin Influence." In recent years, it has also increased its support for investigative journalism outlets and digital security programs. This includes support for local and international investigative reporting organizations that focus on exposing corruption with links to the Kremlin and its impact in the region. USAID's programs include training in financial viability of media outlets, audience analysis, and digital security, among others. Organizations such as the **Organized Crime and Corruption Reporting Project** (OCCRP), the private, investigative journalism organization which focuses on exposing corruption and has a broad mandate and deep expertise on Russian and former Soviet Bloc corruption, deserves further support.

- Civil society groups should have the operational lead inside Russia. We define civil society broadly, including groups with a mandate to advance free media and civil society, such as the National Endowment for Democracy,[62] public interest media groups such as OCCRP and online analysts with a public interest purpose, such as Bellingcat and the Atlantic Council's Digital Forensic Research Lab.

- Experience suggests that such groups, and their European counterparts such as the European Endowment for Democracy, are generally more nimble than the U.S. government. They have advantages in working one-on-one with free Russian media and activist journalists, especially those inside Russia, who are understandably sensitive to receiving U.S. government support and for whom any foreign support needs to be discreet. As the regime intensifies its effort to lock down the internet, these and other civil society groups with technical expertise should be enlisted to provide technical support to Russian journalists — such as support for Virtual Private Networks (VPNs), platforms accessible on mobile phones, and techniques to evade attempts at internet controls and even shutdowns (that are in fact now being prepared and tested by the Putin regime).

- Increase support for offshore Russian-language media platforms. A number of Russian independent journalists have relocated their activities to neighboring countries, e.g., Latvia, which have Russian-speaking populations and cultural familiarity (even if the result of Soviet occupation) with Russia. They have been welcomed and are able to set up free media platforms available to Russian speakers inside and outside Russia. The online news portal Meduza[63] is one of the best regarded of these free media platforms, which in a sense are independent, civil society counterparts of the old RFE/RL model of offshore free media.

Support can take a number of forms, including journalistic collaboration, technical and security support, and financial support through grants. Civil society groups can collaborate more closely on substance; the U.S. government should maintain a distance from journalist output.

- Support free Russian-language media in Ukraine. Ukraine is a bilingual country and, despite the growing use of Ukrainian as a national language, is likely to remain so. Ukraine thus has advantages as a platform for free Russian-language media. Kremlin propaganda (and common Western misunderstandings) aside, speaking Russian in Ukraine is not necessarily an indication of pro-Kremlin sympathies.

  The United States (and European countries and the EU) could expand support for Russian-language media in Ukraine — both traditional and online — with two objectives: to target Russian-speaking Ukrainian citizens in occupied Donbas and Crimea to compete with Russian propaganda there and to target Russians both inside and outside Russia.

  Free Russian-language media based in Ukraine and the welcoming of Russian journalists fleeing Russia, as Latvia does with respect to Meduza, could have a special appeal to a Russian audience. In invading Ukraine in 2014, Putin sought to forestall Ukraine's potential future as a free, successful and free-market democracy integrating with Europe. Because Putin claims that Ukraine is not in fact a separate nation, a democratic Ukraine would be an especially powerful blow against Putinism. Working with Ukraine and Ukrainian institutions to promote (but not control) Russian-language free media based in Ukraine and directed at Russian audiences could be a powerful element of democratic offense against Russian disinformation.

China

- Prepare for a sophisticated tech-driven China. Learning from the experience in Russia in the 1990s, we should be wary of repeating the same mistakes in China. Beijing sees the use and abuse of information as a vector for control at home and influence abroad. The CCP's efforts to control information flows have grown rapidly in their sophistication in the last 5-10 years. To stay ahead, democracies cannot afford a failure in imagination. Rather, the United States and its allies must plan to be better prepared for where China will be in the medium and long term.[64]
- Radio Free Asia's (RFA) current work in Mandarin is greatly underfunded at approximately $20 million when compared with China's multibillion global media operations through CGTN, Voice of China, United Front institutions, and many other actors. The U.S. Congress should expand RFA's domestic language media efforts targeting Chinese, Tibetan, and Uighur audiences and invest in a digital Chinese-language platform on the model of "Current Time" to counter CCP efforts at targeting young Mandarin speakers abroad.
- While it is difficult, if not impossible, to support independent media in China, support for independent media around the world where China is actively working to co-opt and influence the media space should be a top priority.
- Invest in public diplomacy efforts in Taiwan by establishing a center of excellence in combatting disinformation based on the model

Protesters rally to remember the deaths and injuries during the months of protests, in Edinburgh Place in Hong Kong, China, December 30, 2019. REUTERS/Lucy Nicholson.

of the Centers of Excellence in Europe. As the primary target of Chinese information operations and a Mandarin-speaking country, Taiwan could be a bright example of how to counter Chinese influence beyond China's borders.[65]

- Congressional leaders and the new U.S. administration should raise public awareness in and beyond the United States about China's human rights abuses with respect to Beijing's repression of Uighurs in Xinjiang and other minorities (notably Tibetans and Mongolians), as well as the nature of China's censorship activities.

- Develop a comprehensive strategy to expose and counter China's efforts to dominate international organizations. The United States should coordinate with its allies and partners to unify their diplomatic messaging in order to challenge and disavow Beijing's deception. While the Covid-19 pandemic is causing enough immediate problems and challenges for the world, ignoring Beijing's disinformation efforts could haunt the United States and the world once this health crisis ends.[66]

- Increase support for independent Chinese-language media. U.S. and allied support for media development should include Chinese-language media organizations outside of China, including organizations that cater to diaspora communities and outlets that offer independent content. Support could include direct partnerships, increased access for interviews or exclusive coverage, or resources such as technical or financial support. Governments should increase work to resist Chinese government efforts to sideline or co-opt independent Chinese-language media.[67]

- Facilitate increased collaboration between advocacy groups. Specialized advocacy organizations and campaigns already work in several issue areas, including support for oppressed groups such as Uighurs, Tibetans, and Christians. The United States and its allies should endeavor to act as a convening agent for advocacy groups to share best practices and information on respective organizations, efforts, and tactics, and support efforts to increase independent advocacy within China.[68]

- Push back against Chinese global state media. The United States and its allies should seek to halt abuses by Chinese state media and related organizations, particularly as they expand further into the global sphere. For example, media regulators can amend broadcasting rules to limit certain ownership practices, or to forbid activities such as airing forced confessions. The U.S. Congress could pass new legislation increasing transparency requirements for state-owned media, and could hold hearings or otherwise scrutinize the scope and activities of state-owned media within their jurisdictions.[69] Governments can support civil society approaches to documenting state-owned media activity — for example, the ChinfluenCE project seeks to map Chinese state influence in several Eastern European countries.[70]

- Send consistent messages with respect to U.S. government support for media freedom, in general, and in Russia and China, specifically. The Biden administration will be more credible and consistent in this regard than was the Trump administration.

- Finnish journalist Jessikka Aro was one of the first journalists to report on the workings of the IRA, the St. Petersburg troll farm. This is precisely the sort of investigative journalism directed against the Russian disinformation apparatus that the U.S. government should be supporting. For uncovering this story, in cooperation with independent Russian journalists,[71] Aro was subjected to Russian trolling and otherwise harassed. In 2019, to honor her work, the State Department offered her its International Women of Courage Award but rescinded the award upon learning that Aro had criticized Trump. The State Department's decision was a shameful act that undercut the policy purpose behind U.S. government's support for media freedom.[72]

- The U.S. government should recognize and honor those fighting to maintain an independent voice to expose the CCP's repression. Lai, the Hong Kong entrepreneur and founder of *Apple Daily* who was arrested amidst pro-democracy protests, should be considered for such an honor.

Conclusion

The United States and its democratic allies have started tackling the disinformation challenge. The Biden administration will be well placed to do so with far greater consistency than the Trump administration managed. To be sure, much more needs to be done for democracies to get off the back foot and actively push back against foreign influence, more broadly, and information influence operations, in particular. Offensive measures, as they are framed here, are not a substitute for investment in long-term societal resilience, but our short-term defensive efforts thus far have not deterred Russia, China, and others. The suggestions above are intended as a menu for U.S. policymakers and, hopefully, of use to Europeans as well.

Endnotes

[1] Daniel Fried, Alina Polyakova, "Democratic Defense Against Disinformation", Atlantic Council, February, 2018, https://www.atlanticcouncil.org/wp-content/uploads/2018/03/Democratic_Defense_Against_Disinformation_FINAL.pdf

[2] Daniel Fried, Alina Polyakova, "Democratic defense against disinformation 2.0", Atlantic Council, June 13, 2019, https://www.atlanticcouncil.org/in-depth-research-reports/report/democratic-defense-against-disinformation-2-0/

[3] Lara Jakes, "As Protests in South America Surged, So Did Russian Trolls on Twitter, U.S. Finds," New York Times, January 19, 2020, https://www.nytimes.com/2020/01/19/us/politics/south-america-russian-twitter.html

[4] Jakub Kalenský, "Russian Disinformation in 2019- Review" Disinfo Portal, January 7, 2020, https://disinfoportal.org/russian-disinformation-in-2019-review/

[5] Today, the broadly accepted industry term for disinformation activities, foreign or domestic, is "information influence operations," which captures the malign intent and comprehensive nature of such activities. In the interest of readability, we use the terms (disinformation and information influence operations or information operations) interchangeably throughout.

[6] Laura Rosenberger, "Making Cyberspace Safe for Democracy," Foreign Affairs, April 13, 2020, https://www.foreignaffairs.com/articles/china/2020-04-13/making-cyberspace-safe-democracy

[7] Daniel Fried and Alina Polyakova, "Europe is starting to tackle disinformation. The U.S. is lagging.," Washington Post, June 17, 2019, https://www.washingtonpost.com/opinions/2019/06/17/europe-is-starting-tackle-disinformation-us-is-lagging/

[8] Link to the EUvDisinfo database: https://euvsdisinfo.eu/disinformation-cases/

[9] Action Plan Against Disinformation § (2018)., https://eeas.europa.eu/sites/eeas/files/action_plan_against_disinformation.pdf.

[10] Assessment of the Code of Practice on Disinformation - Achievements and areas for further improvement § (2020)., https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=69212; James Pamment, "EU Code of Practice on Disinformation: Briefing Note for the New European Commission," Carnegie Endowment for International Peace, March 3, 2020, https://carnegieendowment.org/2020/03/03/eu-code-of-practice-on-disinformation-briefing-note-for-new-european-commission-pub-81187

[11] James Pamment, "EU Code of Practice on Disinformation: Briefing Note for the New European Commission," Carnegie Endowment for International Peace, March 3, 2020, https://carnegieendowment.org/2020/03/03/eu-code-of-practice-on-disinformation-briefing-note-for-new-european-commission-pub-81187

[12] Christina la Cour, "Governments countering disinformation: The case of Sweden" Disinfo Portal, August 9, 2019, https://disinfoportal.org/governments-countering-disinformation-the-case-of-sweden/

[13] Link to the Paris Call for Trust and Security in Cyberspace: https://pariscall.international/en/

[14] Aurelien Breeden, " French Court Strikes Down Most of Online Hate Speech Law," New York Times, June 18, 2020, https://www.nytimes.com/2020/06/18/world/europe/france-internet-hate-speech-regulation.html

[15] Alex Hern, " UK-based Chinese news network CGTN faces possible ban," The Guardian, July 6, 2020, https://www.theguardian.com/media/2020/jul/06/uk-based-chinese-news-network-cgtn-faces-possible-ban

[16] Link to NATO Strategic Communications Center of Excellence in Riga: https://www.stratcomcoe.org/

[17] Link to the European Center of Excellence on Countering Hybrid Threats in Helsinki: https://www.hybridcoe.fi/

[18] Link to the Rapid Response Mechanism website: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/human_rights-droits_homme/rrm-mrr.aspx?lang=eng

[19] Abdarahmane Wone, "VERIFIED: UN launches new global initiative to combat misinformation," United Nations, May 21, 2020, https://www.un.org/africarenewal/news/coronavirus/covid-19-united-nations-launches-global-initiative-combat-misinformation

[20] Amy Lieberman, "UN enlists 10,000 digital volunteers to fight COVID-19 misinformation," devex, July 2, 2020, https://www.devex.com/news/un-enlists-10-000-digital-volunteers-to-fight-covid-19-misinformation-97615

[21] Paul M. Nakasone and Michael Sulmeyer, “How to Compete in Cyberspace: Cyber Command’s New Approach,” Foreign Affairs, last modified August 25, 2020, https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity; Michael Sulmeyer, “How the U.S. Can Play Cyber-Offense: Deterrence Isn’t Enough,” Foreign Affairs, last modified March 22, 2018, https://www.foreignaffairs.com/articles/world/2018-03-22/how-us-can-play-cyber-offense.;

[22] Mike Isaac and Kate Conger, “Google, Facebook and Others Broaden Group to Secure U.S. Election,” New York Times, https://www.nytimes.com/2020/08/12/technology/google-facebook-coalition-us-election.html.

[23] Ben Nimmo, Camille François, C Shawn Eib, Léa Ronzaud,“IRA Again: Unlucky Thirteen,” Graphika, September 1, 2020, https://graphika.com/reports/ira-again-unlucky-thirteen/.

[24] “Updating Our Advertising Policies on State Media,” Twitter, last modified August 19, 2019, https://blog.twitter.com/en_us/topics/company/2019/advertising_policies_on_state_media.html.

[25] Vijaya Gadde and Kayvon Beykpour, “Additional Steps We’re Taking Ahead of the 2020 US Election,” Twitter, last modified October 9, 2020, https://blog.twitter.com/en_us/topics/company/2020/2020-election-changes.html.

[26] Notable organizations in this space include: Stanford’s Internet Research Observatory, the German Marshall Fund’s Alliance for Securing Democracy, the Atlantic Council’s DFRLab, the Center for European Policy Analysis’s democratic resilience program, EUDisinfoLab, and private sector firms such as Graphika.

[27] Žilvinas Švedkauskas, Chonlawit Sirikupt, and Michel Salzer, “Russia’s Disinformation Campaigns Are Targeting African Americans,” Washington Post, last modified July 24, 2020, https://www.washingtonpost.com/politics/2020/07/24/russias-disinformation-campaigns-are-targeting-african-americans/.

[28] Alina Polyakova, “The Kremlin’s Plot against Democracy: How Russia Updated Its 2016 Playbook for 2020,” Foreign Affairs, September/October 2020, https://www.foreignaffairs.com/articles/russian-federation/2020-08-11/putin-kremlins-plot-against-democracy.

[29] Laura Rosenberger of the German Marshall Fund and Christopher Walker of the National Endowment for Democracy have described this in detail in this and the following footnote: Laura Rosenberger, “Laura Rosenberger on Chinese Information Operations,” June 18, 2020, in Lawfare’s Arbiters of Truth, podcast, audio, https://www.lawfareblog.com/lawfare-podcast-laura-rosenberger-chinese-information-operations.; Juan Pablo Cardenal et al., Sharp Power: Rising Authoritarian Influence, December 5, 2017, https://www.ned.org/sharp-power-rising-authoritarian-influence-forum-report/.

[30] Makena Kelly, “Distorted Nancy Pelosi Videos Show Platforms Aren’t Ready to Fight Dirty Campaign Tricks,” The Verge, last modified May 24, 2019, https://www.theverge.com/2019/5/24/18637771/nancy-pelosi-congress-deepfake-video-facebook-twitter-youtube.

[31] United States v. Internet Research Agency, 2018 D.C. Dist.

[32] 2018 Department of Defense Cyber Strategy, September 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

[33] Ellen Nakashima, “In Georgia, a Legal Battle over Electronic Vs. Paper Voting,” Washington Post, last modified September 16, 2018, https://www.washingtonpost.com/world/national-security/in-georgia-a-legal-battle-over-electronic-vs-paper-voting/2018/09/16/d655c070-b76f-11e8-94eb-3bd52dfe917b_story.html.

[34] Marwa Eltagouri, “The rise of ‘Putin’s chef,’ the Russian oligarch accused of manipulating the U.S. election,” Washington Post, February 17, 2018, https://www.washingtonpost.com/news/worldviews/wp/2018/02/16/the-rise-of-putins-chef-yevgeniy-prigozhin-the-russian-accused-of-manipulating-the-u-s-election/

[35] Ellen Nakashima, “Cyber Command Has Sought to Disrupt the World’s Largest Botnet, Hoping to Reduce Its Potential Impact on the Election,” Washington Post, last modified October 10, 2020, https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-a166-dc429b380d10_story.html#click=https://t.co/eVm0zAnZbI.

[36] Paul M. Nakasone, “A Cyber Force for Persistent Operations,” Joint Force Quarterly 92 (Spring 2019): https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_10-14_Nakasone.pdf. ; Statement of General Paul M. Nakasone Commander United States Cyber Command before the Senate Committee on Armed Services (2019) (statement of Paul M. Nakasone).

[37] Nakasone and Sulmeyer, “How to Compete,” Foreign Affairs.

[38] Ben Nimmo, Camille François, C Shawn Eib, Léa Ronzaud,“IRA Again: Unlucky Thirteen,” Graphika, September 1, 2020, https://graphika.com/reports/ira-again-unlucky-thirteen/.

[39] "3 CFR 13757 - Executive Order 13757 of December 28, 2016. Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities," govinfo, last modified on January 1, 2017, https://www.govinfo.gov/app/details/CFR-2017-title3-vol1/CFR-2017-title3-vol1-eo13757/summary.

[40] "Treasury Sanctions Individuals and Entities In Connection with Russia's Occupation of Crimea and the Conflict in Ukraine," Press Center, Department of the Treasury, December 12, 2016.

[41] "Executive Order on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election," White House, issued on September 12, 2018, https://www.whitehouse.gov/presidential-actions/executive-order-imposing-certain-sanctions-event-foreign-interference-united-states-election/.

[42] "Treasury Targets Assets of Russian Financier who Attempted to Influence 2018 U.S. Elections," Press Releases, U.S. Department of the Treasury, September 30, 2019, https://home.treasury.gov/news/press-releases/sm787.

[43] Daniel Fried and Brian O'Toole, "Pushing Back Against Russian Aggression: Legislative Options," Atlantic Council, March 16, 2020, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/pushing-back-against-russian-aggression-legislative-options/.

[44] Alan Cullison, "Two Russian Media Moguls Summoned for Questioning," The Wall Street Journal, November 2, 2000, https://www.wsj.com/articles/SB97311271799579685.

[45] Nataliya Rostova, "Saving Their Profession: Russian Journalists and Their New Media," The Wilson Center, December 17, 2019, https://www.wilsoncenter.org/blog-post/saving-their-profession-russian-journalists-and-their-new-media.

[46] Recent amendments to Russia foreign agents law applies registration requirements to individual Russian journalists who receive funding from abroad or distribute foreign-sourced material, a law that may have a chilling effect on some journalists, but past experience suggests that haphazard enforcement and habits of social resistance will mean that this latest regime leverage will have a marginal rather than decisive impact. "Russia's New 'Foreign Agent' Law, Explained," The Moscow Times, December 2, 2019, https://www.themoscowtimes.com/2019/12/02/russias-new-foreign-agent-law-explained-a68311.

[47] "China," Countries & Regions, Reporters Without Borders, https://rsf.org/en/china.

[48] Marc Tracy, Edward Wong, and Lara Jakes, "China Announces That It Will Expel American Journalists," The New York Times, March 17, 2020, https://www.nytimes.com/2020/03/17/business/media/china-expels-american-journalists.html/.

[49] "The Long Arm of China: Exporting Authoritarianism With Chinese Characteristics," Congressional-Executive Commission on China, December 13, 2017, https://www.cecc.gov/sites/chinacommission.house.gov/files/CECC%20Hearing%20-%2013%20Dec%202017%20-%20Long%20Arm%20of%20China%20-%20Kalathil.pdf.

[50] Raymond Zhong, "A Saucy App Knows China's Taste in News. The Censors Are Worried," The New York Times, January 2, 2018, https://www.nytimes.com/2018/01/02/business/china-toutiao-censorship.html.

[51] Glenn Tiffert, Renee DiResta, Carly Miller, Vanessa Molter, John Pomfret, "Telling China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives," The Hoover Institution, July 21, 2020, https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/sio-china_story_white_paper-final.pdf.

[52] Sarah Cook, "Beijing's Global Megaphone," Freedom House, https://freedomhouse.org/report/special-report/2020/beijings-global-megaphone#footnote28_6sjbbeq.

[53] "Tiananmen at 30: Examining the Evolution of Repression in China," Congressional-Executive Commission on China, June 4, 2019, https://www.cecc.gov/sites/chinacommission.house.gov/files/documents/Kalathil%206-4-19%20CECC%20testimony%20_0.pdf.

[54] Tiffany May and Austin Ramzy, "'We Will Persevere': A Newspaper Faces the Weight of Hong Kong's Crackdown," The New York Times, August 12, 2020, https://www.nytimes.com/2020/08/12/world/asia/hong-kong-apple-daily-jimmy-lai.html.

[55] Chris Horton, "Specter of Meddling by Beijing Looms Over Taiwan Elections" The New York Times, November 22, 2018, https://www.nytimes.com/2018/11/22/world/asia/taiwan-elections-meddling.html.

[56] Nick Aspinwall, "Taiwan Passes Anti-Infiltration Act Ahead of Election Amid Opposition Protests," The Diplomat, January 3, 2020, https://thediplomat.com/2020/01/taiwan-passes-anti-infiltration-act-ahead-of-election-amid-opposition-protests/.

57 Rorry Daniels, “Taiwan’s Unlikely Path to Public Trust Provides Lessons for the US,” The Brookings Institution, September 15, 2020, https://www.brookings.edu/blog/order-from-chaos/2020/09/15/taiwans-unlikely-path-to-public-trust-provides-lessons-for-the-us/.

58 Daniel Fried was Polish Desk Officer at the Department of State from 1987-90, Political Counselor at Embassy Warsaw from 1990-93, and NSC Director and Senior Director for Central and Eastern Europe from 1993-97; and was told this by numerous visiting Poles and others from Central and Eastern Europe and the Baltic States.

59 Josh Lipsky, Daniel Fried, “US Government Broadcasters Have Long Advanced the Cause of Freedom. Now They’re Under Threat,” Atlantic Council, June 23, 2020, https://www.atlanticcouncil.org/blogs/new-atlanticist/us-government-broadcasters-have-long-advanced-the-cause-of-freedom-now-theyre-under-threat/. ; Jackson Diehl, “Trump’s Continuing Vandalism of the Voice of America,” The Washington Post, October 11, 2020, https://www.washingtonpost.com/opinions/global-opinions/trumps-continuing-vandalism-of-the-voice-of-america/2020/10/11/82799d5a-0984-11eb-859b-f9c27abe638d_story.html.

60 “In-Q-T,” In-Q-Tel, https://www.iqt.org/; “DARPA,” Defense Advanced Research Projects Agency, https://www.darpa.mil/.

61 The smaller estimate is from “Current Time,” Current Time TV Channel, https://www.currenttime.tv/; The larger from “Current Time” staff.

62 Daniel Fried is a member of the NED Board

63 “Meduza,” Meduza, https://meduza.io/en.

64 The authors would like to thank Christopher Walker of the National Endowment for Democracy for this idea.

65 Dan Blumenthal, “China’s Censorship, Propaganda and Disinformation,” American Enterprise Institute, March 5, 2020, https://www.aei.org/wp-content/uploads/2020/03/DBlumenthal-Testimony-on-Chinese-Censorship-1.pdf.

66 Mathew Ha, Alice Cho, “China’s Coronavirus Disinformation Campaigns Are Integral to Its Global Information Warfare Strategy,” Foundation for Defense of Democracies, April 30, 2020, https://www.fdd.org/analysis/2020/04/30/chinas-coronavirus-disinformation-campaigns-are-integral-to-its-global-information-warfare-strategy/.

67 “Policy Recommendations: China,” Freedom House, https://freedomhouse.org/policy-recommendations-china.

68 “Policy Recommendations: The Battle for China’s Spirit,” Freedom House, https://freedomhouse.org/report/2017/policy-recommendations-battle-china-spirit-religious-freedom.

69 “Policy Recommendations: China,” Freedom House, https://freedomhouse.org/policy-recommendations-china.

70 “About the Project,” ChinfluenCE, https://www.chinfluence.eu/about/.

71 Jessikka Aro, “Yle Kioski Traces the Origins of Russian Social Media Propaganda – Never-before-seen Material from the Troll Factory,” Yle, 20 February 2015, https://kioski.yle.fi/omat/at-the-origins-of-russian-propaganda

72 Jennifer Haslan, “State Department revoked award for journalist over social media posts critical of Trump and lied about it, watchdog finds,” CNN, September 25, 2020, https://www.cnn.com/2020/09/25/politics/jessikka-aro-iwoc-trump-state-department/index.html

CEPA

Center for European Policy Analysis
1275 Pennsylvania Ave NW, Suite 400
Washington, DC 20004
info@cepa.org | www.cepa.org