HADES
alliance for securing democracy
G|M|F
GLOBSEC
IDEAS SHAPING THE WORLD

2019 | No. 042

Countering Information Operations Demands A Common Democratic Strategy

By Laura Rosenberger and Bradley Hanlon

In a world increasingly interconnected by technology, democratic governments are grappling with how to defend against and counter information operations targeting their societies. Russia has emerged as the most prolific foreign actor engaging in these operations – targeting at least 37 countries across the transatlantic space since 2000[1] – but other states, such as China and Iran, are increasingly adopting these tools. Information operations manifest differently depending on specific opportunities and vulnerabilities in the target country, but they employ many common tactics and exhibit similar manipulative behaviors. In many cases, the same "Advanced Persistent Manipulators" execute operations across a range of countries, and continue to operate despite repeated takedowns of accounts associated with these operations.[2] For example, the Russian Internet Research Agency has targeted at least 10 transatlantic countries with information operations.[3] And in the case of online operations, the same platforms are being exploited as conduits for these campaigns in numerous countries. This means that there are common approaches that governments can adopt to defend against and counter this threat, although different government structures and legal frameworks mean that not all practices will be directly transferrable. But just as malign actors are learning from one another's tactics and operations, democracies need to learn from one another about effective approaches to counter this threat.

This paper explores approaches that democratic countries are adopting to counter these tactics in order to identify common strategies and best practices. Although these approaches are best accompanied by initiatives from the private sector and civil society, this paper focuses specifically on efforts made by democratic governments. These efforts include: creating cross-cutting structures for policy development and analysis of asymmetric threats; engaging and sharing information with technology companies; raising public awareness of the threat; building societal resilience through media literacy programs; constructing and reforming legal frameworks around transparency and election security; deterring malign actors through messaging and cost-raising measures; and finally, facilitating international coordination to identify threats and share best practices.

Cross-Cutting Structures

To adequately counter asymmetric threats to their countries, some democratic governments have established, tasked, or empowered cross-cutting structures and inter-agency bodies. These efforts are intended to facilitate information-sharing and coordination of analysis and policy formulation regarding the threat of foreign interference – including information operations. While several governments have established these types of structures, specific organizational blueprints, authorities, and capabilities

[1] "Authoritarian Interference Tracker," *Alliance For Securing Democracy*, https://securingdemocracy.gmfus.org/toolbox/authoritarian-interference-tracker/.

[2] Clint Watts, "Advanced Persistent Manipulators, Part One: The Threat to the Social Media Industry," *Alliance For Securing Democracy*, February 12, 2019, https://securingdemocracy.gmfus.org/advanced-persistent-manipulators-part-one-the-threat-to-the-social-media-industry/.

[3] "Authoritarian Interference Tracker," *Alliance for Securing Democracy*, https://securingdemocracy.gmfus.org/toolbox/authoritarian-interference-tracker/.

vary. Additionally, these bodies include varied levels of interaction and coordination with local and state authorities, as well as with the private sector.

Perhaps the most well-known example of a cross-cutting government structure for countering information operations is the Swedish Civil Contingencies Agency (MSB). The Swedish government first established the MSB in 2009 as an emergency management organization, though its role was expanded to include disinformation in 2015 and the organization was granted an increased budget to analyze foreign influence in 2017.[4] The MSB is the keystone of Sweden's whole-of-society approach to countering interference, coordinating and convening across government agencies to identify and monitor threats.[5] The MSB also works with local level civil servants and election officials – mostly in an educational capacity – to help improve their ability to identify and counter interference.[6] Ahead of Sweden's September 2018 elections, the MSB trained over 10,000 civil servants on how to spot foreign influence campaigns.[7]

Another example of a cross-cutting structure is the Canadian government's Security and Intelligence Threats to Elections (SITE) Task Force. Established in January 2019 as an "integrated inter-agency body,"[8] the SITE brings together elements of the Canadian intelligence community, law enforcement, and foreign policy establishment to coordinate efforts to identify and analyze foreign threats to Canadian elections – including information operations.[9]

A final example comes from Australia, which has faced foreign interference operations from the Chinese Communist Party (CCP). In April 2018, Australia appointed its first National Counter Foreign Interference Coordinator. The Coordinator oversees a team within Australia's Department of Home Affairs that coordinates across the Australian Security Intelligence Organisation (ASIO), the Australian Federal Police (AFP), the Department of Defence, and the Department of Foreign Affairs and Trade.[10] The Coordinator is intended to provide a "focal point for coordinating policy and program development" regarding countering foreign interference and also leads government engagement with the private sector.[11]

Democratic governments' attempts to establish cross-cutting structures take a variety of approaches. Some – like Canada's SITE – focus heavily on analysis, while Australia's Counter Foreign Interference Coordinator concentrates on policy development and implementation, as well as resiliency-building. Sweden's MSB emphasizes education and awareness, as well as engagement with local officials, to ensure a whole-of-society response to information operations. While the organization and authority of these bodies depends heavily on domestic context, all of these structures maintain a similar and essential purpose – to prevent interference threats from falling into bureaucratic seams, and to help develop a unified understanding of potential threats. By establishing a central body for coordinating counter-interference efforts, democratic governments help policymakers see the full threat picture for interference and ensure that policy responses draw on all tools at decision makers' disposal.

[4] Gabriel Cederberg, *Catching Swedish Phish: How Sweden is Protecting its 2018 Elections*, Belfer Center for Science and International Affairs, Harvard Kennedy School, August 2018, https://www.belfercenter.org/sites/default/files/files/publication/Swedish%20Phish%20-%20final2.pdf, 13; "Sweden to Create New Authority Tasked with Countering Disinformation," *The Local*, January 15, 2018, https://www.thelocal.se/20180115/sweden-to-create-new-authority-tasked-with-countering-disinformation.

[5] Brittany Beaulieu and Steven Keil, "Russia as Spoiler: Projecting Division in Transatlantic Societies," *Alliance for Securing Democracy*, June 2018, https://d2llho1jqyw8vm.cloudfront.net/wp-content/uploads/2018/06/Russia-as-Spoiler.pdf, 12.

[6] Michael Birnbaum, "Sweden Is Taking on Russian Meddling Ahead of Fall Elections. The White House Might Take Note," *Washington Post*, February 22, 2018, https://www.washingtonpost.com/world/europe/sweden-looks-at-russias-electoral-interference-in-the-us-and-takes-steps-not-to-be-another-victim/2018/02/21/9e58ee48-0768-11e8-aa61-f3391373867e_story.html.

[7] Chris Good, "Ahead of Election, Sweden Warns Its Voters against Foreign Disinformation," *ABC News*, September 8, 2018, https://abcnews.go.com/International/ahead-election-sweden-warns-voters-foreign-disinformation/story?id=57694373.

[8] David Salvo and Heidi Tworek, "The Next North American Election: How Canada Is Protecting Itself and What Can Still Be Done," *Alliance For Securing Democracy*, March 5, 2019, https://securingdemocracy.gmfus.org/the-next-north-american-election-how-canada-is-protecting-itself-and-what-can-still-be-done/.

[9] "Security and Intelligence Threats to Elections (SITE) Task Force," Government of Canada, February 7, 2019, https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/security-task-force.html.

[10] "Australian Crack Unit to Ward Off Threats From Espionage," *The Australian*, April 24, 2018, https://www.theaustralian.com.au/nation/crack-unit-to-ward-off-threats-from-espionage/news-story/8409b24c8595bee1bc27e9927f05fbd5.

[11] Australian Department of Home Affairs, "Who We Are – Chris Teal," last modified March 29, 2019, https://www.homeaffairs.gov.au/about-us/who-we-are/our-senior-staff/chris-teal.

Engagement and Information Sharing with the Technology Sector

Given the nature of online information operations, engagement with stakeholders in the tech community is essential for effectively countering foreign interference. Revelations of the Russian Internet Research Agency's manipulation of social media to target the 2016 U.S. presidential election served as a wake-up call for democratic governments around the world that the online information space is a battleground for malign influence.

Coordination with the tech sector has taken a variety of forms in different countries, but information sharing remains largely ad-hoc. For example, ahead of Germany's elections in 2017, Facebook – in close cooperation with German authorities – reportedly removed tens of thousands of fake accounts from its platform. The German Federal Office for Information Security (BSI) also maintained a direct channel for communications with the company regarding potential disinformation targeting the elections.[12] The Swedish Civil Contingencies Agency (MSB) has coordinated in a similar fashion with Facebook, establishing a communication channel to facilitate quick responses to fake accounts identified by the Swedish government.[13] Ahead of European Parliament elections in May 2019, Facebook, Twitter, and Google provided monthly reports on their efforts to combat disinformation to the European Commission, although this communication has been primarily one-way.[14]

In the United States, failure to recognize the threat and lack of coordination with social media platforms hindered government attempts to detect foreign interference online ahead of the 2016 election.[15] Following revelations of online foreign interference, the U.S. Department of Justice called for closer cooperation with social media companies to tackle information operations.[16] Since then, Facebook and Google have reportedly worked with U.S. law enforcement on several occasions to take down information operations linked to Russia and Iran.[17] In April 2019, Director of the Federal Bureau of Investigation (FBI) Christopher Wray noted that the back-and-forth communication between U.S. officials and social media platforms "has gotten dramatically better" since 2016.[18] In September 2019, U.S. officials from the FBI, Department of Homeland Security (DHS), and Office of the Director of National Intelligence (ODNI) met with representatives of Facebook, Google, Twitter, and Microsoft to discuss preparations for the upcoming 2020 election.[19] While one U.S. intelligence official claimed the meeting was "collectively viewed as a positive step," additional reporting revealed that government and tech representatives remain at odds over standards for information sharing.[20]

Although these examples represent important progress in trust-building between governments and the tech community, they remain limited, ad-hoc, and often narrowly focused on elections. Democratic governments need to establish and institutionalize permanent mechanisms for information sharing with technology companies, including protections for privacy, speech, and classified information. Government agencies have the tools to recognize emerging threats and malign foreign actors, while social media companies have a unique view into activity on their platforms. Both sets

[12] Selena Larson, "Facebook Says It Took down 'tens of Thousands' of Fake Accounts before German Election," *CNN Business*, September 27, 2017, https://money.cnn.com/2017/09/27/technology/business/facebook-german-elections-fake-accounts/index.html.

[13] Gabriel Cederberg, *Catching Swedish Phish: How Sweden is Protecting its 2018 Elections*, Belfer Center for Science and International Affairs, Harvard Kennedy School, August 2018, https://www.belfercenter.org/sites/default/files/files/publication/Swedish%20Phish%20-%20final2.pdf, 21.

[14] European Commission, "Code of Practice Against Disinformation: Commission Recognises Platforms' Efforts Ahead of the European Elections," May 17, 2019, http://europa.eu/rapid/press-release_STATEMENT-19-2570_en.htm.

[15] Adam Entous, "The Rise and Fall of a Kremlin Troll," *The New Yorker*, July 19, 2018, https://www.newyorker.com/news/news-desk/the-rise-and-fall-of-a-kremlin-troll.

[16] U.S. Department of Justice, *Report of the Attorney General's Cyber Digital Task Force*, July 2, 2018, https://www.justice.gov/ag/page/file/1076696/download, 12.

[17] Kent Walker, "An Update on State-Sponsored Activity," *Google*, August 23, 2018, https://www.blog.google/technology/safety-security/update-state-sponsored-activity/; "Taking Down More Coordinated Inauthentic Behavior," *Facebook Newsroom*, August 21, 2018, https://newsroom.fb.com/news/2018/08/more-coordinated-inauthentic-behavior/; Nathaniel Gleicher, "Removing Coordinated Inauthentic Behavior from Iran, Russia, Macedonia and Kosovo," *Facebook Newsroom*, March 26, 2019, https://newsroom.fb.com/news/2019/03/cib-iran-russia-macedonia-kosovo/.

[18] "A Conversation With Christopher Wray," *Council on Foreign Relations*, April 26, 2019, https://www.cfr.org/event/conversation-christopher-wray-0.

[19] Salvador Rodriguez, "The FBI visits Facebook to talk about 2020 election security, with Google, Microsoft and Twitter joining," *CNBC*, September 4, 2019, https://www.cnbc.com/2019/09/04/facebook-twitter-google-are-meeting-with-us-officials-to-discuss-2020-election-security.html.

[20] Dustin Volz and Deepa Seetharaman, "Washington, Silicon Valley Struggle to Unify on Protecting Elections," *Wall Street Journal*, September 13, 2019, https://www.wsj.com/articles/washington-silicon-valley-struggle-to-unify-on-protecting-elections-11568392455.

of knowledge are necessary for effectively identifying and countering hostile information operations. Recent coordination is an important positive step, but stronger communications protocols will help democratic governments – and the tech community – shift from reactive to proactive countermeasures against information operations.

Public Awareness and Exposure

Foreign information operations aim to manipulate a target country's domestic population by hijacking public discussion to insert and amplify false, misleading, or inflammatory narratives. In this battle, citizens are on the front lines, and it is therefore not enough for government officials alone to recognize the threat. Democratic governments have a strategic imperative to raise public awareness about this threat in order to build resilience against it. Exposing these operations is also important to reduce their effectiveness and potentially deter them.

Democratic governments have sought to raise public awareness and inform citizens in several different ways. In Sweden, the Civil Contingencies Agency (MSB) coordinates directly with mass media outlets to raise awareness of information operations. In the lead-up to 2018 Swedish elections, MSB reportedly shared information regularly with media outlets to help them understand "how to withstand attempts to influence their reporting and counter disinformation."[21] Outside of the media, Swedish government officials also directly warned the public about the threat of disinformation campaigns.

The Canadian government has taken similar steps to inform and educate its citizens. The Elections Modernization Act, which came into force in June 2019, authorizes Canada's non-partisan chief election official to share unlimited educational and informational material with the public to help inform them of interference efforts.[22] High-level Canadian officials, including Prime Minister Justin Trudeau, have also warned the public about the threat of foreign interference targeting Canada's democratic institutions.[23]

In the wake of the poisoning of Sergei and Yuliya Skripal, the UK government took on Russian disinformation directly, setting up a communications team and using its own social media to warn citizens about the tactics that Moscow was using to manipulate their opinions on the incident.[24] Also, in Australia, high-level officials – including former Prime Minister Malcolm Turnbull – have repeatedly warned the public about the "covert, coercive, and corrupting behavior" that characterizes foreign influence efforts.[25]

In the United States, government officials were reluctant to publicly call out foreign interference during the 2016 election. Since then, the Department of Justice and former Deputy Attorney General Rod Rosenstein have articulated the importance of publicly exposing and attributing foreign information operations in order to educate citizens and undermine the effectiveness of malign influence efforts.[26] Unfortunately, intense partisanship and mixed messaging from U.S. leadership have undermined this initiative – politicizing the threat and hindering attempts to address it.

Information operations target citizens directly to polarize societies and inflame tensions. Promoting public awareness is a key first step to countering these

[21] Gabriel Cederberg, *Catching Swedish Phish: How Sweden is Protecting its 2018 Elections*, Belfer Center for Science and International Affairs, Harvard Kennedy School, August 2018, https://www.belfercenter.org/sites/default/files/files/publication/Swedish%20Phish%20-%20final2.pdf, 24.

[22] David Salvo and Heidi Tworek, "The Next North American Election: How Canada Is Protecting Itself and What Can Still Be Done," *Alliance for Securing Democracy*, March 5, 2019, https://securingdemocracy.gmfus.org/the-next-north-american-election-how-canada-is-protecting-itself-and-what-can-still-be-done/.

[23] "Canadian PM Warns of Russian Interference in Upcoming Parliamentary Elections," *Radio Free Europe/Radio Liberty*, April 6, 2019, https://www.rferl.org/a/canada-warns-of-russian-interference-in-parliamentary-elections/29864687.html.

[24] Elisabeth Braw, "How the British Hit Back Against Russian Agitprop," *Wall Street Journal*, March 11, 2019, https://www.wsj.com/articles/how-the-british-hit-back-against-russian-agitprop-11552344805; U.K. Foreign Office, Twitter post, March 29, 2018, https://twitter.com/foreignoffice/status/979333458131607553?lang=en.

[25] Malcolm Turnbull, "Speech Introducing the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017," December 7, 2017, https://www.malcolmturnbull.com.au/media/speech-introducing-the-national-security-legislation-amendment-espionage-an.

[26] U.S. Department of Justice, *Report of the Attorney General's Cyber Digital Task Force*, July 2, 2018, https://www.justice.gov/ag/page/file/1076696/download, 12; U.S. Department of Justice, "Deputy Attorney General Rod J. Rosenstein Delivers Remarks at the Aspen Security Forum," July 19, 2018, https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-aspen-security-forum.

operations, and democratic governments should act to help their citizens understand how and why they are being targeted by malign foreign factors.

Media Literacy

Democratic governments have also taken steps to support efforts to educate the public on how to safely consume media without being manipulated by malign actors. In several countries, media and digital literacy components have become a large part of efforts to build up long-term resilience to foreign information operations.

In Canada, the government recently established a Digital Citizens Initiative, which aims to support programs that educate citizens on how information operations work and what they can do to “avoid being susceptible to manipulation online.”[27] The program also aims to provide citizens with the skills to critically assess online news and to better understand how algorithms impact their online experience. In a recent white paper, UK policymakers called on the government to construct a similar media literacy strategy to improve education and awareness for citizens of all ages.[28]

In 2014, the Finnish government launched an initiative to educate citizens, students, journalists, and politicians on how to counter disinformation. Finland has also revised its educational curriculum to emphasize critical thinking skills and to instruct students on how to spot false information.[29] In Sweden, the Swedish Media Council – a government agency – launched a similar nationwide curriculum in July 2018 to teach elementary and high school students how to identify false information online.[30] And these efforts are paying off. A recent study by the European Policies Initiative found that, of 35 European countries, Finland ranks first in resilience to the “post-truth phenomenon.” Sweden is ranked fourth.[31]

In the United States, the Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security recently launched a viral campaign to help citizens understand how state-backed information operations target divisive issues to distract online discussions and sow chaos. Numerous other government agencies seized on the initiative, promoting the campaign on social media.[32]

> “Building an informed, digitally literate populace is a long-term investment in resilience against [foreign interference]."

Teaching citizens the steps that they can take to protect themselves against foreign manipulation is the best way to inoculate a society against the effects of malign interference. As information operations continue to grow in complexity and scale through emerging technologies like artificial intelligence and deepfakes, it will only become more difficult to tell fact from fiction online. Building an informed, digitally literate populace is a long-term investment in resilience against this threat.

Legal Frameworks for Transparency and Election Integrity

Authoritarian actors exploit vulnerabilities and loopholes within democratic countries to deploy information operations. To close off these vulnerabilities, some democratic governments have sought to reform legal and regulatory frameworks around online transparency and the integrity of election information.

[27] Government of Canada, “Online Disinformation,” last modified February 5, 2019, https://www.canada.ca/en/canadian-heritage/services/online-disinformation.html.

[28] U.K. Department for Digital, Culture, Media and Sport, “Online Harms White Paper – Executive Summary,” April 30, 2019, https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper-executive-summary--2.

[29] Eliza Mackintosh, “Finland Is Winning the War on Fake News. What It’s Learned May Be Crucial to Western Democracy,” *CNN*, May 2019, https://www.cnn.com/interactive/2019/05/europe/finland-fake-news-intl.

[30] Gabriel Cederberg, *Catching Swedish Phish: How Sweden is Protecting its 2018 Elections*, Belfer Center for Science and International Affairs, Harvard Kennedy School, August 2018, https://www.belfercenter.org/sites/default/files/files/publication/Swedish%20Phish%20-%20final2.pdf, 28.

[31] Eliza Mackintosh, “Finland Is Winning the War on Fake News. What It’s Learned May Be Crucial to Western Democracy,” *CNN*, May 2019, https://www.cnn.com/interactive/2019/05/europe/finland-fake-news-intl.

[32] Jacob Ward, “U.S. cybersecurity agency uses pineapple pizza to demonstrate vulnerability to foreign influence,” *NBC News*, July 26, 2019, https://www.nbcnews.com/news/us-news/u-s-cybersecurity-agency-uses-pineapple-pizza-demonstrate-vulnerability-foreign-n1035296.

Across the transatlantic space, policymakers have sought to reform laws around online political advertising to increase transparency and reduce the potential for manipulation. In the United States, the proposed Honest Ads Act would expand political disclosure rules for online ads and would require platforms to keep a public record of political ad purchases.[33] The Canadian government recently announced a similar provision which will create ad spending limits, as well as stricter reporting and disclosure requirements for online ads during elections.[34] Additionally, in the EU, the European Commission's Code of Practice on Disinformation requires signatories to increase transparency for political and issue-based ads and to strengthen efforts to verify advertisers.[35]

The recent U.S. effort to enforce the Foreign Agents Registration Act (FARA) represents another democratic effort to improve transparency. FARA requires individuals and organizations that undertake political activity and are controlled or funded by foreign governments to register with the Department of Justice.[36] The law is aimed at improving public awareness of foreign propaganda targeting U.S. citizens. Following revelations that Russian state-controlled media outlets RT and Sputnik had been used to spread false information ahead of the 2016 elections, the U.S. Department of Justice requested that the outlets – and their affiliated companies – officially register as foreign agents due to their close ties to the Kremlin.[37]

Another tactic for countering information operations has been to create legal frameworks to ensure the integrity of election information online. For example, Canadian law prohibits the publishing of false statements regarding personal information about a candidate or a political leader during an election period.[38] In 2018, the French Parliament passed a similar law to combat "fake news" by allowing courts to decide if articles published during election periods are manipulative and should be taken down.[39]

More recently, the UK government published a white paper outlining a plan to combat harmful content on social media. The paper calls for an independent regulator that would monitor social media platforms and punish them for failing to quickly remove what it calls harmful content – ranging from terrorist propaganda and cyberbullying to disinformation.[40] Australia passed a similar law earlier this year that threatens social media companies with harsh punishments for failing to quickly remove violent content.[41]

While laws like these intend to raise the costs for spreading misinformation and halt its spread, their focus on content is misguided. Lumping information operations into the same broad bucket as terrorist content or hate speech misunderstands the methods of information operations, which are a unique threat and require their own specific solutions. Information operations are a problem of malicious actors engaging in manipulative behavior; in many instances the content spread in these operations is not demonstrably true or false. Focusing on content also ignores many of the tactics that malign actors are using to influence platforms, such as inauthentic personas and manipulation of search results. Additionally, content-centered approaches are inherently reactive, relying on the detection and removal of material after it has already been posted and spread.[42] And finally, policing content poses significant challenges to free speech

[33] Zach Montellaro, "The Honest Ads Act Returns," *Politico*, May 9, 2019, https://www.politico.com/newsletters/morning-score/2019/05/09/the-honest-ads-act-returns-615586.

[34] David Salvo and Heidi Tworek, "The Next North American Election: How Canada Is Protecting Itself and What Can Still Be Done," *Alliance for Securing Democracy*, March 5, 2019, https://securingdemocracy.gmfus.org/the-next-north-american-election-how-canada-is-protecting-itself-and-what-can-still-be-done/.

[35] European Commission, "Code of Practice on Disinformation," September 26, 2018, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

[36] Natalka Pisnia, "Why Has RT Registered as a Foreign Agent with the US?," *BBC*, November 15, 2017, https://www.bbc.com/news/world-us-canada-41991683.

[37] Josh Gerstein, "DOJ Told RT to Register as Foreign Agent Partly Because of Alleged 2016 Election Interference," *Politico*, December 21, 2017, https://www.politico.com/story/2017/12/21/russia-today-justice-department-foreign-agent-election-interference-312211.

[38] Parliament of Canada, "Bill C-76," December 13, 2018, https://www.parl.ca/DocumentViewer/en/42-1/bill/C-76/royal-assent, 91.

[39] Zachary Young, "French Parliament Passes Law against 'Fake News,'" *Politico*, July 4, 2018, https://www.politico.eu/article/french-parliament-passes-law-against-fake-news/.

[40] U.K. Department for Digital, Culture, Media and Sport and U.K. Home Department, *Online Harms White Paper*, 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf.

[41] Damien Cave, "Australia Passes Law to Punish Social Media Companies for Violent Posts," *The New York Times*, April 4, 2019, https://www.nytimes.com/2019/04/03/world/australia/social-media-law.html.

[42] Laura Rosenberger, "Foreign Influence Operations and Their Use of Social Media Platforms," *Alliance For Securing Democracy*, July 31, 2018, https://securingdemocracy.gmfus.org/foreign-influence-operations-and-their-use-of-social-media-platforms/.

and could easily play into the hands of authoritarian regimes by restricting expression.[43] Attempts to combat information operations by focusing on content are ineffective at best, and counterproductive at worst.

Focusing instead on the deceptive behavior of malign actors offers a better framework for tackling disinformation and allows governments and private companies to act decisively without worrying about attribution. This approach also allows platforms to detect patterns in manipulative behavior that will make future influence operations easier to identify.[44] As governments begin to ponder legal frameworks for combating information operations – as is happening in the UK and France – they should focus on promoting transparency and targeting malign behavior, not policing content.[45]

Deterrence and Cost-Raising

As with any security threat, defense alone is not enough – deterrence is also an important part of countering information operations. Authoritarian actors have turned to information operations not only for their effectiveness, but also due to their low cost. Deterrent messaging, accompanied by the threat or imposition of consequences, raises the costs of undertaking such interference. Some democratic actors have even taken offensive steps to counter malign foreign information operations.

Ahead of elections in 2017, officials in France and Germany issued strong warnings of consequences for potential interference. High-level officials in France warned publicly that they would not tolerate interference in the upcoming elections, and – in the wake of cyber-attacks against the campaign of now-President Emmanuel Macron – outgoing French President François Hollande directly warned Moscow.[46] Officials in Germany took a similar tack, publicly warning about the consequences of interference ahead of the election, particularly if previously hacked material were released publicly.[47] German Chancellor Angela Merkel even addressed the issue directly with Russian President Vladimir Putin in a face-to-face meeting.[48] Ahead of elections in Sweden, Prime Minister Stefan Löfven also warned that his government would "expose [such operations] without mercy."[49]

In reaction to Russian interference in the 2016 presidential election, the U.S. Department of Treasury launched several waves of punitive sanctions targeted at the actors responsible for cyber and information operations. The designees included employees, funders, and companies associated with the Internet Research Agency (IRA), as well as Russian military intelligence officers (GRU) who helped spread stolen information online.[50] Public indictments helped impose additional reputational costs on Moscow and exposed the tactics employed by the IRA and GRU to target the U.S. election. In general, European countries have been slower to turn to sanctions as punishment for information operations – though media regulators in the UK and France have acted to shame and punish Russian state-controlled broadcasters for inaccurate reporting.[51]

[43] Jessica Brandt, "How Global Efforts to Limit Disinformation Could Infringe Speech," *Axios*, April 16, 2019, https://www.axios.com/how-global-efforts-to-limit-disinformation-could-infringe-speech-10cba500-2299-4077-8fc2-4c13e4d4ff86.html.

[44] Laura Rosenberger, "Foreign Influence Operations and Their Use of Social Media Platforms," *Alliance For Securing Democracy*, July 31, 2018, https://securingdemocracy.gmfus.org/foreign-influence-operations-and-their-use-of-social-media-platforms/.

[45] Sam Schechner, "Global Regulators Race to Curb Silicon Valley," *Wall Street Journal*, May 10, 2019, https://www.wsj.com/articles/france-steps-up-global-tech-scrutiny-with-social-media-policing-11557478920.

[46] Erik Brattberg and Tim Maurer, "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks," *Carnegie Endowment for International Peace*, May 23, 2018, https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435.

[47] Ibid.

[48] Patrick Beuth et al., "Cyberattack on the Bundestag: Merkel and the Fancy Bear," *Die Zeit*, May 12, 2017, https://www.zeit.de/digital/2017-05/cyberattack-bundestag-angela-merkel-fancy-bear-hacker-russia/komplettansicht.

[49] Erik Brattberg and Tim Maurer, "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks," *Carnegie Endowment for International Peace*, May 23, 2018, https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435.

[50] U.S. Department of the Treasury, "Treasury Targets Russian Operatives over Election Interference, World Anti-Doping Agency Hacking, and Other Malign Activities," December 19, 2018, https://home.treasury.gov/news/press-releases/sm577; U.S. Department of the Treasury, "Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks," March 15, 2018, https://home.treasury.gov/news/press-releases/sm0312.

[51] Paul Sandle, "UK Media Watchdog Says Russian Broadcaster RT Broke Impartiality Rules," *Reuters*, December 20, 2018, https://www.reuters.com/article/us-britain-russia-ofcom-idUSKCN1OJ1D2.; "Russia Warns French TV After France Calls Out Falsified RT Report," *Radio Free Europe/Radio Liberty*, June 29, 2018, https://www.rferl.org/a/france-warns-rt-claims-broadcast-syrian-chemical-weapons-attack-douma/29326822.html.

Ahead of the 2018 midterm elections, the U.S. government took additional preemptive actions to deter interference from the IRA. In the weeks leading up to the elections, the U.S. Cyber Command (CYBERCOM) reportedly targeted individual IRA operatives and Russian intelligence officers with direct messages warning them that they had been identified and that their activity was being tracked.[52] On the day of the midterms, CYBERCOM also reportedly launched cyber-attacks against the IRA to cut off the organization's Internet access and prevent it from spreading disinformation.[53] Given the long-term nature of information operations – which are ongoing and not limited to election days – the cyber-attacks were far too limited and too late to prevent interference. However, experts and officials have argued that the attacks served as a messaging tool to demonstrate U.S. capability and commitment to protecting its elections.[54]

While it is difficult to assess the direct impact of deterrent measures without delving into counterfactuals, cost-raising, public messaging, and preemptive efforts play an important role in the democratic defense against foreign interference. They serve to punish malign actors, raise the costs of otherwise inexpensive operations, expose and impose reputational damage on foreign governments, and demonstrate resolve and resilience.

Government officials should also articulate a declaratory policy that identifies foreign interference operations as a national security threat that will be met with consequences.[55] Cost-raising efforts are most effective when taken multilaterally, rather than unilaterally. Democratic governments should come together to define principles of unacceptable interference operations that would face punitive responses. The EU's recent decision to impose quick-reaction EU-wide sanctions for cyber-attacks is a positive step and presents a potential model for a unified deterrent mechanism for information operations.[56] Another model for multilateral and cross-sector messaging is the Paris Call for Trust and Security in Cyberspace, which aims to set international norms for the cyber domain and includes provisions on protecting elections from foreign interference and defending accessibility to the internet.[57] The initiative has been endorsed by more than 50 countries, 90 nonprofits and academic institutions, and 130 private companies and groups – including key tech companies.

International Coordination

A final aspect of the democratic response to malign information operations has been the facilitation of information sharing and exchange of best practices through international mechanisms. Authoritarian-backed information operations target democratic countries around the world – often through similar tools and actors, and occasionally with the same narratives. At times, international organizations are the target of authoritarian interference themselves. As a result, governments have launched several initiatives to facilitate international coordination on countering information operations.

Two examples of international coordination mechanisms are the EU's Rapid Alert System and the G7's Rapid Response Mechanism. The EU's Rapid Alert System connects points of contact from all 28 EU member states to exchange best practices, share analysis, flag disinformation campaigns and coordinate responses to information operations. The system utilizes an online platform that allows for real-time information exchange.[58] However, despite intentions, critics have noted that that Rapid Alert System has been underutilized and ineffective thus far, stating, "It's not

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

[53] Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *Washington Post*, February 27, 2019, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

[54] Ibid.

[55] Jamie Fly, Laura Rosenberger, and David Salvo, *Policy Blueprint for Countering Authoritarian Interference in Democracies*, Alliance for Securing Democracy, June 26, 2018, https://securingdemocracy.gmfus.org/the-asd-policy-blueprint-for-countering-authoritarian-interference-in-democracies/.

[56] "Days before Elections, EU Approves New Cyber Sanctions Regime," *Reuters*, May 17, 2019, https://www.reuters.com/article/us-eu-cyber-idUSKCN1SN1FQ.

[57] Louise Matsakis, "The US Sits out an International Cybersecurity Agreement," *Wired*, November 12, 2018, https://www.wired.com/story/paris-call-cybersecurity-united-states-microsoft/.

[58] European External Action Service, "Rapid Alert System Factsheet," March 2019, https://eeas.europa.eu/sites/eeas/files/ras_factsheet_march_2019_0.pdf.

rapid. There are no alerts. And there's no system."[59] The G7's Rapid Response Mechanism aims to achieve similar goals by facilitating information sharing and organizing responses to threats to G7 democracies. The "Coordination Unit" of the mechanism is based in Canada and is tasked as the focal point of information sharing and policy coordination amongst members. Outside of institutional mechanisms, democratic governments have also coordinated responses to information operations on an ad-hoc basis. In the wake of the poisoning of Sergei and Yuliya Skripal by Russian intelligence officers, the UK government worked quickly to rally support from the transatlantic community and to coordinate with allies and partners to identify and debunk disinformation narratives.[60]

While these information-sharing mechanisms are an important step in the right direction, they are limited in their participation and implementation. Another logical venue for a counter-information operations coordinating cell is at NATO. NATO not only brings together a wide range of transatlantic democracies, but is also a frequent target of information operations itself. Creating an international coordinating body within NATO – with engagement from the appropriate levels of member state governments – could allow for a more robust sharing of best practices. Additionally, given the nature of the collective defense organization, NATO could serve as an effective catalyst for mustering powerful, coordinated responses to malign actors.

> *"Democracies are strongest when they work together, and unified punitive actions send a strong message to malign actors..."*

Overall, international coordination plays an extremely important role in countering information operations. As authoritarian tactics grow more sophisticated and are supercharged by emerging technologies, democracies will need to learn from each other how best to defend against and deter interference. Further, democracies are strongest when they work together, and unified punitive actions send a strong message to malign actors about the costs of trying to undermine democratic institutions.

Conclusion

Democratic governments have employed a wide range of approaches to countering and deterring information operations, ranging from offensive cyber-attacks to domestic education programs. Examining these efforts reveals best practices and strategies for securing democratic institutions while protecting freedoms. These strategies include structural reforms, limited legal and regulatory efforts, resilience-building programs, and strong deterrence and cost-raising measures.

Structural approaches that facilitate a whole-of-society defense against interference are key to a successful counter-disinformation strategy. Democracies must act to ensure that threats posed by information operations do not fall between bureaucratic seams, and must enable information exchange between various levels of government – as well as between government agencies and the private sector – to adequately identify and counter disinformation. Structural reforms will also be key for coordinating information sharing and policy responses on an international and transatlantic scale.

Another key takeaway is the limited room for legal and regulatory approaches to countering information operations. While democratic governments have taken varied steps to address the spread of harmful content online, effective action on this front should focus on increasing transparency and hindering manipulative behavior. Approaches that encourage platforms or government regulators to police content present challenges to free speech and risk undermining the values that are democracies' greatest strengths – achieving authoritarian actors' goals for them.

Public awareness and media literacy programs are also essential to building long-term democratic resilience to malign information operations. Exposing the tools and tactics of authoritarian interference is the best way to inoculate citizens against their effects. And investing

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

[60] Elisabeth Braw, "How the British Hit Back Against Russian Agitprop," *Wall Street Journal*, March 11, 2019, https://www.wsj.com/articles/how-the-british-hit-back-against-russian-agitprop-11552344805.

in educating citizens about how they can safely consume information online will help insulate domestic discussion from future interference. As authoritarian actors adopt and adapt emerging technologies to conduct even more sophisticated disinformation campaigns, maintaining an aware and informed public will be even more important.

A final best practice for countering information operations is strong deterrence coupled with cost-raising measures. Democratic governments have the tools to dissuade malign actors from interfering in their countries and will need to recognize their own asymmetric advantages in order to raise costs on authoritarian actors who target their institutions. Deterrent and punitive measures are more effective when they are taken in concert with allies, and democratic governments should band together to demonstrate to authoritarian actors that they will not tolerate malign information operations targeting their institutions.

This paper was produced as part of the
"EXPOSING RUSSIAN INFORMATION OPERATIONS IN FRONTLINE STATES: Automated analysis, monitoring and vulnerability assessment" *project implemented by GLOBSEC.*

G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Washington • Ankara • Belgrade • Berlin
Brussels • Bucharest • Paris • Warsaw

www.gmfus.org