The US Army War College Quarterly: Parameters

Volume 50
Number 3 *Parameters Autumn 2020*

Article 4

8-14-2020

Enduring Information Vigilance: Government after COVID-19

Nina Jankowicz

Henry Collis

COVID-19

Enduring Information Vigilance: Government after COVID-19

Nina Jankowicz and Henry Collis

ABSTRACT: The framework of Enduring Information Vigilance will help ally and partner governments deny advantages adversaries gain through their use of information operations in our new global perpetual information environment. This approach recognizes the persistent threat, unifies responses within and between governments, and resolves societal fissures toward a more global democratic information environment.

A clear pattern of opportunism has emerged across Russian and Chinese information operations. Exacerbated by the pandemic, this adversarial activity will continue to characterize the information space in the future. In an era of perpetual information competition, and given the persistent nature of the information threat, current paradigms and structures for countering hostile-state disinformation in Western governments are inadequate. Western democracies should instead organize their responses around what we have deemed "Enduring Information Vigilance," which recognizes the perpetual nature of the threat, addresses societal fissures bad actors exploit, overcomes bureaucratic hurdles to cross-government and cross-sector collaboration, and fosters international cooperation toward a more democratic information environment.

Hostile-state information operations, which Herbert Lin defines as "the deliberate use of information (whether true or false) by one party on an adversary to confuse, mislead and ultimately to influence the choices and decisions that the adversary makes," continue to confound democracies.[1] The use and manipulation of information as a tool of influence began long before the 2016 US presidential election. But information operations have become more potent in an increasingly networked world, aided by the ubiquity of online targeting tools and the anonymity and credibility the Internet provides.

Since 2016, the American public and private sectors have struggled to address this challenge, stymied by domestic politicization of the topic and legitimate concerns about balancing social media regulation

1. Herbert Lin, "On the Organization of the U.S. Government for Responding to Adversarial Information Warfare and Influence Operations," *I/S: A Journal of Law and Policy for the Information Society* 15, no. 1–2 (Spring 2019): 2, https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/lin.pdf.

with First Amendment rights.[2] As a result, disinformation has thrived during the COVID-19 pandemic and left the country vulnerable to manipulation through hostile-state information operations.

Perpetual Information Competition

Since the end of the Cold War and the resurgence of great-power competition, Western democracies have conceptualized hostile-state information operations as one-off occurrences—explained away by societal peculiarities, tensions, and events such as elections—that provide inflection points hostile states can attempt to manipulate. Rather than organizing crosscutting, proactive, whole-of-government responses, most Western governments stand-up extra capabilities only when necessary, such as election *war rooms* before events like the 2018 US midterms or the UK government's response to the Russian poisonings of Sergei and Yulia Skripal on British soil.[3]

In the United States, countering information operations has been largely securitized, primarily involving elements of the Defense, Homeland Security, and State Departments, in addition to the Intelligence Community, but rarely, if ever, focused on domestic audiences or involving the softer side of government, such as the Department of Education. As the development of Russian and Chinese information operations over the past decade-plus into the COVID-19 era demonstrates, this lack of whole-of-government approach misses the bigger picture and inhibits an effective response.

Russia, China, and other authoritarian states have recognized the utility of engaging in perpetual information competition, utilizing a strategic-level integrated approach to information operations and "are already contesting this domain and exploiting democracies' inaction."[4] Hostile states understand information competition is the new normal, and they are constantly probing for and exploiting societal fissures such as ethnic or racial tension, pandemic uncertainty, and political polarization to drive their ongoing campaigns. They use all channels available—government and nongovernment, online and offline—when engaging in perpetual information competition. Finally, hostile-state perpetual information competition does not adhere neatly to international borders, but rather exploits them, attempting to undermine the unity of alliances and international organizations.

---

2. Karen Kornbluh and Ellen P. Goodman, *Safeguarding Democracy against Disinformation*, DIDI Roadmap no. 4 (Washington, DC: German Marshall Fund of the United States, 2020), 9, https://www.gmfus.org/sites/default/files/Safeguarding%20Democracy%20against%20Disinformation_v7.pdf.

3. Jonathan Owen, "Kremlin's Web of Lies on Novichok Exposed by Government's Security Comms Team," *PR Week*, July 25, 2018, https://www.prweek.com/article/1488558/kremlins-web-lies-novichok-exposed-governments-security-comms-team.

4. Laura Rosenberger and Lindsay Gorman, "How Democracies Can Win the Information Contest," *Washington Quarterly* 43, no. 2 (Summer 2020): 77, https://cpb-us-e1.wpmucdn.com/blogs.gwu.edu/dist/1/2181/files/2020/06/RosenbergerGorman_TWQ_43-2.pdf.

Russian Information Operations

Building on the long history of Soviet active measures in the pre-Internet era, Russia has used the online information environment and levers of offline information manipulation to drive division and distrust abroad and undermine democratic processes for at least 13 years. The first example of these modern information operations occurred in Estonia in 2007 when the Kremlin exploited the ethnic Russian population's latent grievances toward the Western-oriented Estonian government. "Putin's regime started to consciously restore and rehabilitate the Soviet symbols and Soviet version of history" through the primarily state-backed Russian-language media in Estonia, creating a flash point at a statue to Soviet World War II dead.[5] The statue became the site of violent demonstrations, and Tallinn became a target of cyberattacks. According to Estonia's internal security service, Russia carried out these information campaigns "towards the Baltic States in order to prevent anti-Russian moods and secure [an] increase in Russia's influence in foreign policy in the world."[6]

Russia's information operations continued. The next year, during the five-day conflict between Russia and Georgia, cyberattacks—seemingly emanating from Kremlin-encouraged *patriotic* hackers—crippled parts of the Georgian government.[7] Moscow also launched an all-out information campaign that sought to call into question Russia's role in provoking the conflict and inspire fear and capitulation among Georgians, to varying degrees of success.

Russia's information operations in Estonia and Georgia occurred before social media platforms developed the worldwide ubiquity they enjoy today. If Estonia and Georgia were the beta versions of the Kremlin's online information operations, Ukraine felt their full effect beginning in 2013–14 with the Euromaidan protests and the Revolution of Dignity, illegal annexation of Crimea, incursions of Russian-backed forces into eastern Ukraine, and the downing of the passenger airliner Malaysia Airlines Flight 17 on July 17, 2014 with a Russian BUK missile.[8] Russia's infamous *troll factory*, the St. Petersburg-based Internet Research Agency, had an entire unit focused on undermining Ukrainian sovereignty, the legitimacy of the post-Maidan government, and international support for Ukraine.[9]

---

5. Kadri Liik, "The 'Bronze Year' of Estonia-Russia Relations," in Estonian Ministry of Foreign Affairs, *Estonian Ministry of Foreign Affairs Yearbook 2007* (Tallinn: Estonian Ministry of Foreign Affairs, 2007), https://vm.ee/sites/default/files/content-editors/web-static/053/Kadri_Liik.pdf.

6. Estonian Internal Security Service, *Annual of the Security Police Board 2007* (Tallinn: Estonian Internal Security Service, 2007), 4, https://www.kapo.ee/en/content/annual-reviews.html.

7. John Markoff, "Georgia Takes a Beating in the Cyberwar with Russia," *Bits* (blog), *New York Times*, August 11, 2008, https://bits.blogs.nytimes.com/2008/08/11/georgia-takes-a-beating-in-the-cyberwar-with-russia/.

8. NATO StratCom Center of Excellence (CoE), *Analysis of Russia's Information Campaign against Ukraine* (Riga, Latvia: NATO StratCom CoE, September 2014), https://www.stratcomcoe.org/analysis-russias-information-campaign-against-ukraine.

9. David Patrikarakos, "The Troll: The Empire Strikes Back," in War in 140 Characters (New York: Basic Books, 2017).

Like the Kremlin-sponsored information operations in Estonia, Georgia, and Ukraine that preceded it, Russian online interference surrounding the 2016 US presidential election had the goal of "provok[ing] and amplify[ing] political and social discord in the United States."[10] Through fake accounts and pages, illegally purchased online advertisements, monetary support of authentic American activists and protests, the hack-and-leak of the emails of Democratic political operatives, and billions of organic online engagements, Russian operatives were able to influence America's democratic discourse ahead of the 2016 vote.[11] They built community and trust through positive messaging and later used this influence to launch more ambitious and divisive campaigns, including in-person protests.[12]

Due to the insufficient and tardy response of the social media platforms and the US government in the wake of the 2016 election interference campaign, Russia's information operations targeting the United States continue as the 2020 presidential election approaches.[13] The Kremlin and its channels of influence have adapted their information operations' tools and tactics to the responses that have been implemented, finding innovative ways around regulations in the United States and beyond. In 2019 and 2020, Ukraine's security service uncovered evidence Russian operatives *rented* Facebook accounts from Ukrainian users and organized a bot network utilizing 40,000 Ukrainian and European SIM cards to field 10,000 accounts across the country.[14]

Chinese Information Operations

Understanding the Chinese Communist Party's (CCP) approach to the role of information in great-power competition starts with the regime's ideological basis, which shaped the instruments of power and led to the development of capabilities designed specifically for political warfare. The regime relies on propaganda in all its forms to legitimize itself, maintain support, and undermine its adversaries' will.[15] The People's Liberation Army (PLA) invested in studying the impact

10. Robert S. Mueller III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election* (Washington, DC: US Department of Justice, 2019), 1:22, https://www.justice.gov/storage/report.pdf.

11. Philip N. Howard et al., "The IRA, Social Media and Political Polarization in the United States, 2012–2018" (working paper, Project on Computational Propaganda, University of Oxford, UK, 2018), https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/The-IRA-Social-Media-and-Political-Polarization.pdf.

12. Nina Jankowicz, "The Top Three Trends We Miss When Discussing Russian Ads," Alliance for Securing Democracy, May 15, 2018, https://securingdemocracy.gmfus.org/the-top-three-trends-we-miss-when-discussing-russian-ads/.

13. *Worldwide Threat Assessment of the US Intelligence Community: Hearings before the Select Committee on Intelligence of the United States Senate*, 116th Cong. (2019) (statement of Daniel R. Coats, Director of National Intelligence), 7, https://www.intelligence.senate.gov/sites/default/files/documents/os-dcoats-012919.pdf.

14. SBU, "СБУ блокувала роботу розгалуженої мережі ботоферм, якою керували з РФ," June 16, 2020, https://ssu.gov.ua/novyny/7698.

15. See the Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China* (Washington, DC: Department of Defense, 2019), iv–v, https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019%20CHINA%20MILITARY%20POWER%20REPORT%20(1).PDF.

of information technology on the nature of conflict and learned from US and allied experiences, incorporating doctrinal developments into its approach.

Operation Desert Storm provided an ideal case study for the US approach to a modern conflict against Russian and Chinese equipment; it underlined the importance of using better technology to integrate battlefield systems in order to create strategic advantage. But Chinese strategists were also impressed by how the United States shaped the narrative around the conflict, using Iraqi aggression as the justification for military operations and employing psychological operations to break the will of the Iraqi army.[16] China implemented these lessons, combining integrated network electronic warfare in close coordination with influence components, such as propaganda and psychological operations, in a single doctrine to achieve information dominance.

But it was in 2003 that the approach most associated with CCP influence activities, the "three warfares," was formally adopted by the former General Political Department of the PLA.[17] "Three warfares" emphasizes three areas of impact for influence activity referred to in political manuals dating back to Mao Zedong: public opinion or media warfare, psychological warfare, and legal warfare.[18]

Public opinion or media warfare uses the full breadth of traditional and social media to influence overseas audiences. From state-linked television and print outlets to paid advertising and senior figures' op-eds in major newspapers, media activity is supported by public outreach organizations and efforts including Confucius Institutes, PLA-run or civilian government-run visits, and exchange initiatives.[19]

The psychological warfare component aims to undermine the will of adversaries to fight as well as promote division among and between leadership, populations, and allies. Techniques might include media activities, diplomatic levers, military deployments or tests, and the use of front organizations such as government-linked think tanks.

The legal warfare component aims to establish the basis for competition or the illegality of an adversary's position. Examples see Chinese government-linked delegates engaging in academic conferences and legal debates about issues of strategic interest to China, including nuclear issues, the sovereignty of space, or the application of international norms in cyberspace.

---

16. James C. Mulvenon and Richard H. Yang, *The People's Liberation Army in the Information Age* (Santa Monica, CA: RAND Corporation, 1999), https://www.rand.org/pubs/conf_proceedings/CF145.html.

17. Larry M. Wortzel, *The Chinese People's Liberation Army* (Carlisle, PA: Strategic Studies Institute, US Army War College Press, 2014), 29, https://publications.armywarcollege.edu/pubs/2263.pdf.

18. Peter Mattis, "China's Three Warfares in Perspective," War on the Rocks, January 30, 2018, https://warontherocks.com/2018/01/chinas-three-warfares-perspective/.

19. Ethan Epstein, "How China Infiltrated U.S. Classrooms," *Politico*, updated January 17, 2018, https://www.politico.com/magazine/story/2018/01/16/how-china-infiltrated-us-classrooms-216327.

The three warfares, however, are not the sole preserve of the PLA. Other state bodies contribute to China's efforts to influence the world and discreetly assert political power over competitors. The Ministry of Education leads efforts to instrumentalize the large number of Chinese students studying overseas, the Ministry of State Security runs fake think tanks and uses academic bodies to influence discourse, the United Front Work Department leverages the Chinese diaspora for political purposes, and the Ministry of Foreign Affairs, among others, uses targeted advertising and media to promote the CCP position abroad.[20]

Despite some similarities in tactics, Chinese and Russian information operations diverge in their intent; China does not opportunistically sow division and inflame internal conflict in an ideologically agnostic way as the Kremlin does, nor has the CCP been linked to attempts to interfere in democratic processes as Russia has.[21] China's objectives focus on the nation's image and ensuring their point of view is heard, even through subversive means. When Beijing has engaged in more aggressive operations such as using fake content or instances of inauthentic online behavior, these efforts have related to the CCP's top foreign policy priorities such as Hong Kong and Taiwan.[22]

Exploiting the COVID-19 Infodemic

In a state of perpetual information competition, the uncertainty, fear, and distrust that characterize the coronavirus pandemic present an opportunity Moscow, Beijing, and other hostile-state actors have exploited. For China, as the origin of the virus, this opportunity was a foreign policy imperative requiring a response at scale and pace. For Russia, however, the pandemic provided multiple new vulnerabilities to exploit for sowing discord, spreading doubt, and subverting discourse. Although news from mainstream outlets achieved greater distribution overall than information from state-backed outlets, Oxford Internet Institute researchers found Russian and Chinese state-backed content among the most engaging content shared in late June 2020.[23] This trend underlines a key strategy of perpetual information competition: relentless and opportunistic exploitation of security vulnerabilities, societal fissures, and highly emotive content intended to drive engagement, decrease trust in institutions, and further amplify division.

---

20. Mattis, "China's Three Warfares"; and Amy Searight, "Countering China's Influence Operations: Lessons from Australia," Center for Strategic and International Studies (website), May 8, 2020, https://www.csis.org/analysis/countering-chinas-influence-operations-lessons-australia.

21. Larry Diamond and Orville Schell, eds., *China's Influence and American Interests: Promoting Constructive Vigilance* (Stanford, CA: Hoover Institution Press, 2018), https://www.hoover.org/research/chinas-influence-american-interests-promoting-constructive-vigilance.

22. Jean-Baptiste Jeangène Vilmer and Paul Charon, "Russia as a Hurricane, China as Climate Change: Different Ways of Information Warfare," War on the Rocks, January 21, 2020, https://warontherocks.com/2020/01/russia-as-a-hurricane-china-as-climate-change-different-ways-of-information-warfare/.

23. "Coronavirus Misinformation Weekly Briefing," The Computational Propaganda Project (website), June 29, 2020, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2020/06/ComProp-Coronavirus-Misinformation-Weekly-Briefing-29-06-2020.pdf.

Russian Exploitation of COVID-19

Using practiced tactics, Russian officials and state-run media were quick to seize on the pandemic to drive further division in Western democracies. The COVID-19 opportunity was particularly appealing in the United States, where another divisive presidential election campaign had just begun, and US government missteps could be amplified and exploited to influence political discourse. According to the Alliance for Securing Democracy, the pandemic was the most discussed topic throughout the "Russian media ecosystem" for 14 weeks, from mid-January to late April 2020.[24] Narratives featured on Russian state-run propaganda outlets have mimicked and amplified those in the US domestic information space. Claims COVID-19 might be a US-created bioweapon, or a future vaccine against the virus would be used to microchip and track Americans were among the most popular coronavirus stories on the Sputnik news website in January to March 2020.[25]

As yet, there are no confirmed instances of coordinated inauthentic Russian campaigns around coronavirus, that is, campaigns utilizing false personae or organizations, placing false ads, or employing bots for inauthentic amplification of content. But narratives in Russian state-run media have broadly tracked with those pushed by covert Russian online properties in the past, suggesting such inauthentic campaigns may yet be uncovered.

Russia has also utilized the coronavirus crisis for more traditional influence campaigns as well as cybercrime. Like China, the Kremlin sent aid, including personal protective equipment and ventilators, to hard-hit nations. Moscow's April aid shipment to the United States provided President Vladimir Putin a domestic propaganda coup at home.[26] An earlier shipment to Italy—emblazoned with the words "From Russia with Love" was part of a wider influence operation to undermine NATO and EU unity, according to reporting by Italian newspaper *La Stampa*.[27] Russian operatives have also used the panic and disruption of routine cybersecurity amid the pandemic to launch widespread cyberattacks against at least 31 companies, "including major American brands and Fortune 500 firms."[28]

---

24. Amber Frankland, Bret Schafer, and Matt Schrader, "Hamilton Weekly Report: April 18–24, 2020," Alliance for Securing Democracy (website), April 27, 2020, https://securingdemocracy.gmfus.org/hamilton-weekly-report-april-18-24-2020/.

25. Andrew Rettman, "Russia's Top Coronavirus 'Fake News' Stories," EU Observer, March 27, 2020, https://euobserver.com/coronavirus/147905.

26. Anton Troianovski, "Turning the Tables, Russia Sends Virus Aid to U.S.," *New York Times*, April 2, 2020.

27. Natalia Antelava and Jacopo Iacoboni, "The Influence Operation behind Russia's Coronavirus Aid to Italy," Coda Story, April 2, 2020, https://www.codastory.com/disinformation/soft-power/russia-coronavirus-aid-italy/.

28. David E. Sanger and Nicole Perlroth, "Russian Criminal Group Finds New Target: Americans Working at Home," *New York Times*, June 25, 2020, https://www.nytimes.com/2020/06/25/us/politics/russia-ransomware-coronavirus-work-home.html.

As the pandemic persists, so have Russian hacking efforts; according to a joint US-UK-Canadian intelligence advisory released in July 2020, the same Russian group responsible for some of the 2016 breaches at the Democratic National Committee attempted to steal coronavirus vaccine intellectual property and supply-chain information.[29] The full effect of Russian COVID-19 information operations is difficult to ascertain, as their narratives converge with authentic grievances in American society surrounding the virus and the US response to the virus. Regardless of their source, over time, these narratives weaken confidence in authority and trust in the government.

Chinese Exploitation of COVID-19

Since news about COVID-19 first emerged from the city of Wuhan, the Chinese government has been actively trying to manage the narrative and protect the legitimacy and interests of the Chinese Communist Party, both domestically and abroad. In the early stages of the pandemic, this strategy focused on suppressing narratives inside China. The government-imposed nationwide quarantine was used as a messaging opportunity to demonstrate the effectiveness of the Chinese system and President Xi Jinping's leadership.[30]

The suppression of virus information, however, ran afoul of the Chinese public. Outrage developed in February and March about the degree to which information was suppressed, including the crucial understanding of human-to-human transmission. Normally strong adherence to the party line by the Chinese people wavered with the widespread coverage of the death of Li Wenliang, a doctor who had been accused of rumormongering when trying to warn fellow medical professionals about the virus on social media in December. The story made the front pages, even of official outlets, provoking widespread criticism of the Wuhan authorities and a political backlash from Beijing as the CCP sought to reassert control over the narrative.[31]

While suppression and censorship sought to maintain the domestic legitimacy of the CCP, this type of activity did not represent a departure from the party's usual practice at home. These actions did, however, set the stage for a fundamental change in the use of information internationally in attempts to demonstrate the strength of China's response and the superiority of the Chinese system and to cast doubt on the origins of the virus.[32] This change in approach to international

29. "UK and Allies Expose Russian Attacks on Coronavirus Vaccine Development," National Cyber Security Centre (website), July 16, 2020, https://www.ncsc.gov.uk/news/uk-and-allies-expose-russian-attacks-on-coronavirus-vaccine-development.

30. Joshua Kurlantzick, "China and Coronavirus: From Home-Made Disaster to Global Mega-Opportunity," Globalist, March 16, 2020, https://www.theglobalist.com/china-soft-power-coronavirus-covid19-pandemic-global-health/.

31. Minxin Pei, "Will the Coronavirus Topple China's One-Party Regime?," *Strategist* (blog), Australian Strategic Policy Institute, March 5, 2020, https://www.aspistrategist.org.au/will-the-coronavirus-topple-chinas-one-party-regime/.

32. Laura Rosenberger, "China's Coronavirus Information Offensive," *Foreign Affairs*, April 22, 2020, https://www.foreignaffairs.com/articles/china/2020-04-22/chinas-coronavirus-information-offensive.

messaging was combined with a significant and high-profile effort to provide aid and advice to countries affected, initially to Europe and later to a vast majority of countries in Africa and in Latin America. As domestic fatalities from the disease fell, China positioned itself as a global leader on public health, engaging multichannel messaging activity to promote its humanitarian stance.

Throughout the pandemic, China has used a variety of means and tactics to engage audiences, including targeted ads by Chinese state media to build a long-term audience through content focused on positive cultural stories. In early 2020, these ads changed, reflecting significantly enhanced efforts aimed at promoting articles related to COVID-19. The content of the ads promoted China's transparency and leadership in the global response including so-called mask diplomacy, while also promoting the personal role played by Xi. This positive messaging then evolved into "misleadingly reframed events, and amplification of conspiracy theories."[33]

The shift apparently sought to cast doubt on the origins of the disease by sowing multiple explanations in a manner similar to Russian obfuscation efforts after the shooting down of Malaysia Airlines Flight 17 and the attempted assassination of Sergei Skripal. These efforts promoted US culpability for the coronavirus, claiming specifically that US military personnel taking "part in the Military World Games in Wuhan in November 2019" brought the virus to China, thereby trying to deflect blame and responsibility for the pandemic.[34]

In addition to the use of state-linked outlets to amplify false narratives and conspiracy theories, other elements of the CCP's international communications during COVID-19 indicate a new appetite for sustained engagement.[35] Chinese diplomats rapidly increased their use of Western social media platforms throughout 2019 but accelerated these efforts in early 2020, including the Ministry of Foreign Affairs launching an official Twitter account in late 2019.[36] US government analysis of the followers of these accounts found a large number of them were identical and had been created in the same six-week period, indicating the coordinated inauthentic use of fake accounts.[37] The analysis also pointed to Chinese

33. Vanessa Molter and Renee DiResta, "Pandemics and Propaganda: How Chinese State Media Creates and Propagates CCP Coronavirus Narratives," in "Covid-19 and Misinformation," special issue, *Harvard Kennedy School Misinformation Review* (June 2020), https://misinforeview.hks.harvard.edu/wp-content/uploads/2020/06/Ipedits_FORMATTED_PandemicsandPropaganda_HKSReview.pdf.

34. Molter and DiResta, "Pandemics and Propaganda," 12.

35. Jessica Brandt and Bret Schafer, "Five Things to Know about Beijing's Disinformation Approach," Alliance for Securing Democracy (website), March 30, 2020, https://securingdemocracy.gmfus.org/five-things-to-know-about-beijings-disinformation-approach/.

36. Abhishek G. Bhaya, "China Gives a Nod to Twiplomacy: MOFA Launches Twitter Account," CGTN, January 14, 2020, https://news.cgtn.com/news/2020-01-14/China-gives-a-nod-to-Twiplomacy-MOFA-launches-Twitter-account-NfiQHr2slW/index.html.

37. Laura Kelly, "U.S. Says China, Russia Cooperating to Spread Coronavirus Disinformation," *Hill*, May 8, 2020, https://thehill.com/policy/international/496880-us-says-china-russia-cooperating-to-spread-coronavirus-disinformation.

messaging piggybacking off Iranian and Russian disinformation online to amplify divisive or conspiratorial false narratives.

Inauthentic activity in support of Chinese messaging has not been limited to fabricating followers of newly created official social media accounts. Independent researchers have also found significant evidence of covert activity promoting China's interests and conducting messaging in support of CCP objectives; investigations by Propublica since August 2019 have revealed a number of different social media manipulation techniques.[38] These techniques include Chinese-based marketing companies using Twitter to boost the following of government-run news services; creating inauthentic user networks to boost the following of state-linked media outlets; hijacking Twitter accounts to tweet Chinese-language content critical of the Hong Kong protests and COVID-19 conspiracy theories; and offering bribes to prominent Chinese language Twitter users to post pro-CCP misinformation.

Using a platform such as Twitter that is largely inaccessible from China to engage Chinese-speaking audiences indicates this sudden flurry of online activity was apparently intended to engage diaspora audiences. Other investigations detected inauthentic accounts amplifying Chinese government talking points across multiple platforms including YouTube, Facebook, and Twitter.[39] As a result of this activity, Twitter took down a network of accounts and attributed them as an information operation run by the Chinese government.[40]

While the CCP's appetite for using disinformation and online deception to build strategic influence and interfere in other nations may have changed, its inauthentic activity has so far been easily detected and exposed. If, however, PRC activity were to influence its target audiences successfully, three messages could damage international perceptions of the United States as they relate to the pandemic: criticism of the US domestic response versus Chinese response to claim the superiority of their system; the use of mask diplomacy to promote CCP leadership and benevolence while US and allied roles in supporting other nations is ignored; and a belief of conspiracy theories that the United States is responsible for the pandemic.

As the fallout from COVID-19 becomes clearer, the relationship between China and the West could change rapidly, exacerbating competition and potentially triggering an economic decoupling between

38. Jeff Kao and Mia Shuang Li, "How China Built a Twitter Propaganda Machine Then Let It Loose on Coronavirus," ProPublica, March 26, 2020, https://www.propublica.org/article/how-china-built-a-twitter-propaganda-machine-then-let-it-loose-on-coronavirus.

39. Benjamin Strick, "Uncovering a Pro-Chinese Government Information Operation on Twitter and Facebook: Analysis of the #MilesGuo Bot Network," Bellingcat, May 5, 2020, https://www.bellingcat.com/news/2020/05/05/uncovering-a-pro-chinese-government-information-operation-on-twitter-and-facebook-analysis-of-the-milesguo-bot-network/.

40. "Transparency Report: Information Operations," Twitter, accessed July 31, 2020, https://transparency.twitter.com/en/information-operations.html.

the United States and China.[41] And in such a scenario, China's vastly increased pace and scale of information operations are likely to persist.

Enduring Information Vigilance

To respond effectively to this *new normal* of perpetual information competition, governments must recognize and understand its characteristics in terms of the doctrine and institutions at its source and the fact that information competition has developed with the specific goal of projecting influence and waging political warfare. Governments should configure institutions, develop capability, and drive activity in the framework of what we have dubbed "Enduring Information Vigilance." The framework explains how governments, through capability building, coordinating via holistic and inclusive government structures, and international cooperation, can work more effectively to detect the vulnerabilities adversaries exploit, manage those attempts, and ultimately deny adversaries any benefit. If effective, the denial of benefit is a powerful tool, alongside the imposition of cost, in supporting an approach based on modern threat deterrence.[42]

Capability: Beyond Discrete Campaigns

As the exploitation of the uncertainty surrounding the coronavirus pandemic has shown, there is a rising baseline of activity to which Western governments must be attuned. Developing situational awareness requires ongoing monitoring, detection, and analysis of the information environment to paint a threat picture of hostile influence activity and warrants investing in the capability building necessary to keep that picture current. Given the vast changes in the scale of both misinformation and disinformation from ideological, commercial, and other nonstate actors during COVID-19, governments will find it harder than ever to identify hostile-state activity; indeed, legitimate grievances across the whole political spectrum in democratic nations are a particular target for Russian online activity. Ensuring hostile states do not exploit divisive, but legitimate discourse requires building government capability and understanding.

Tools for detecting online campaigns and inauthentic activity have developed rapidly in recent years, and parts of the national security infrastructure have adopted them. But none of these tools is a panacea, and the military adage about the importance of having skilled personnel is particularly relevant: "Don't operate the equipment, equip the operator." Enduring Information Vigilance relies on skilled people with a nuanced understanding of the threat, who are capable of applying

41. Patrick M. Cronin, Michael Doran, and Peter Rough, "Geopolitical Implications of the Coronavirus," Hudson Institute (website), March 13 2020, https://www.hudson.org/research/15816-geopolitical-implications-of-the-coronavirus.

42. Vytautas Keršanskas, *Deterrence—Proposing a More Strategic Approach to Countering Hybrid Threats*, Hybrid CoE Paper 2 (Helsinki, Finland: European Center for Countering Hybrid Threats, 2020), https://www.hybridcoe.fi/publications/hybrid-coe-paper-2-deterrence-proposing-a-more-strategic-approach-to-countering-hybrid-threats/.

the full range of tools and techniques for monitoring, detecting, and responding to information operations.

Several governments have already started raising awareness and enhancing the relevant skills of their personnel: the Swedish Civil Contingencies Agency produced a handbook for countering information influence activities, and the UK government published currently train public sector communications personnel on the "RESIST" toolkit, which emphasizes the importance of understanding the objectives of information activities when formulating appropriate and effective responses.[43]

Moreover, building capability for Enduring Information Vigilance should not be limited to traditional national security-focused departments; hostile states have configured their institutions to deliver across multiple channels, and the US response must be equally coordinated. Training on detecting and responding to hostile-state information operations should be required of all civil servants as a part of their regular professional development, with more specific and tailored development programs required for communications professionals and those focusing on hostile states.

Coordination: All Sectors, At All Times

The breadth of activity under Russian information operations or China's "three warfares" approach spans the remit of multiple government agencies; Western governments must break out of siloed national security thinking, coordinate more effectively, and provide space for cross-sector cooperation. From hard security and defense to cultural activity and media, as well as many other realms of society not typically situated at the forefront of foreign interference, hostile states have the potential to exploit the inability of Western governments to work effectively across traditional departmental boundaries. This "bureaucratic vulnerability" can lead to poor information flow, competition for resources and influence, or the exclusion of key stakeholders.[44]

Information operations comprising the use of multiple tools, vectors, and activities in coordination (with malign intent), challenge bureaucratic coherence and cohesion, exploiting blind spots and targeting vulnerabilities. Bureaucratic vulnerability lies in the range of ministries in which different states choose to place counter-information operations efforts. Some nations focus on security institutions considering adversary information operations a counterintelligence challenge; some nations respond through ministries of interior—an

43. Swedish Civil Contingencies Agency, *Countering Information Influence Activities: A Handbook for Communicators* (Karlstad, Sweden: Swedish Civil Contingencies Agency, 2019), https://rib.msb.se/filer/pdf/28698.pdf; and UK Government Communications Service, *RESIST Counter Disinformation Toolkit* (London: Government Communications Service, 2020), https://gcs.civilservice.gov.uk/publications/resist-counter-disinformation-toolkit/.

44. European Center of Excellence for Countering Hybrid Threats, *Tackling the Bureaucratic Vulnerability: An A to Z for Practitioners*, Hybrid CoE Paper 3 (Helsinki, Finland: European Center for Countering Hybrid Threats, 2020), https://www.hybridcoe.fi/publications/hybrid-coe-paper-3-tackling-the-bureaucratic-vulnerability-an-a-to-z-for-practitioners/.

approach centered on protection and resilience; and some nations place their efforts within the offices of prime ministers to reflect the crucial need for coordination. And some nations have created entirely new structures that face branding, communications, and legitimacy challenges.[45]

These shortcomings emphasize the need to work more effectively across government. Newly built capabilities required for monitoring, detecting, and understanding the multiple elements of hostile information activities—and associated intelligence and analysis—must be integrated to advance a shared view of what adversaries are doing, whom they are targeting, and whether these activities are effective. Further, this information must be shared with nontraditional security departments via leads with the necessary security clearances.

Building this situational awareness across the government will enable the prioritized coordination of effective responses in the short term and beyond, including the exploitation of vulnerabilities. Policy and operational levers for ameliorating vulnerabilities and building resilience against information threats in the long term lie with ministries of education, health, and local government; they require policies that ensure a thriving and pluralistic media, societal awareness of the threat, robust media and digital literacy, and an understanding of civics.[46]

In addition to a truly whole-of-government approach, Enduring Information Vigilance requires governments to initiate and create space for a whole-of-society response to the problem. Governments should convene regular meetings and establish communication and collaboration channels across the public, private, nonprofit, media, and academic sectors. Ideally, governments would facilitate cross-sector cooperation and trust through grant programs requiring collaboration and cost-sharing among grantees, eliminating duplication and competition that exists between many organizations in the counterinformation operations space. Particularly in the social media space, these programs would place special emphasis on information sharing to detect and combat cross-platform information campaigns. Such partnerships would build societal resilience to information operations, investing in awareness building and media and digital literacy programming, and identify trusted third parties to deliver these messages to the general public. Ultimately, healing societal fissures takes an ethos of understanding and service across systems, which a persistent, wide-reaching strategy like Enduring Information Vigilance can build over time.

45. Nina Jankowicz, *Avoiding the Band-Aid Effect in Institutional Responses to Disinformation and Hybrid Threats*, Policy Paper no. 21 (Washington, DC: Alliance for Securing Democracy, The German Marshall Fund of the United States, August 2019), https://securingdemocracy.gmfus.org/wp-content/uploads/2019/08/Jankowicz-Bandaid-Effect-paper.pdf.

46. Nina Jankowicz, "The Disinformation Vaccination," *Wilson Quarterly* (Winter 2018), https://www.wilsonquarterly.com/quarterly/the-disinformation-age/the-disinformation-vaccination/.

Cooperation: International Partnership

Hostile influence activities have never occurred at such a scale before. Any deterrent effect of Enhanced Information Vigilance is augmented by demonstrating resolve and denying benefit to adversaries through a collective stance against their activities, including better sharing of information and knowledge to identify threats, tactics, tools, and procedures and the formulation of effective responses. In the wake of the attempted assassination of Sergei Skripal in the United Kingdom in 2018, the coordinated expulsion of over 140 Russian diplomatic personnel from allied nations demonstrates how a well-coordinated response can impose costs on a threat actor.[47] Building cross-border resilience and reducing vulnerability to deny benefit, however, requires enduring cooperation and demonstrations of shared capability and resolve.

Allies and partners can support Enduring Information Vigilance in multiple ways: sharing analysis and assessments to understand and counter threats; developing ongoing joint strategic communications to engage hostile states' target audiences; joint exercising of contingencies; and creating issue-specific plurilateral groups allowing partners to respond or put pressure on adversaries in specific regions or on specific topics, such as a wildlife commission into wet markets.

Finally, adversaries use information operations to exploit open societies and undermine shared democratic values; therefore, they must remain the center of gravity for any approach to countering hostile interference. Preserving these values and the transparency, openness, and commitments to freedom of expression and human rights through a community of democracies will ensure our societies continue to provide an alternative to the authoritarian regimes of hostile states.

Conclusion

The coronavirus pandemic has underscored the West's patchwork response to hostile-state information operations and the need for change. Western democracies must reorganize and reorient themselves to address this threat through Enduring Information Vigilance by investing in nuanced capability building, casting aside turf and funding wars to coordinate more effectively across government, and actively driving cooperation with allies and partners worldwide. These structures cannot be built overnight; they require a long-term commitment that will likely outlast the political class initiating them. But the result will be a more resilient society that reassures its populations and denies adversaries benefit, deterring malign attempts to exploit the openness of democracy.

47. UK Government, "PM Commons Statement on National Security and Russia," March 26, 2018, https://www.gov.uk/government/speeches/pm-commons-statement-on-national-security-and-russia-26-march-2018/.

Nina Jankowicz

Nina Jankowicz, author of *How to Lose the Information War: Russia, Fake News, and the Future of Conflict*, studies the intersection of technology and democracy at the Wilson Center and holds a master's degree from Georgetown University's School of Foreign Service.

Henry Collis

Henry Collis, a national security strategic communications specialist in UK Government, recently served as Deputy Director for International Security and Defence Projects in the Prime Minister's Office and Cabinet Office Communications Team.