The Global Engagement Center's Response to the Coronavirus Infodemic

Major Neill Perry

INTRODUCTION

COVID-19 has underscored the shortcomings of the US government's (USG) approach to disinformation. Throughout the pandemic, adversary nations attacked both foreign perceptions of the US abroad as well as Americans' confidence in their own institutions. The US failed to execute a robust and coherent response against these spurious narratives. This article will review the federal government's actions with a particular focus on the Global Engagement Center (GEC), the agency nominally tasked to coordinate the federal government's response to foreign disinformation.

The US Retools After the Russian Influence Campaign

The USG's current approach to disinformation evolved in response to recent foreign overtures. In 2016, the Russian government directed an influence campaign to sway the outcome of the US presidential election and to "undermine public faith in the US democratic process."[1] Under Kremlin direction, Russia's Internet Research Agency created online personas and inauthentic social media accounts to exacerbate a polarized American electorate. After the Russian interference campaign became public, the USG reorganized its fight against disinformation.

After the election in December 2016, Congress established the Global Engagement Center (GEC) "to lead, synchronize, and coordinate the USG's response to foreign state and non-state propaganda."[2] Congress further tasked GEC with coordinating with allies and partner nations, identifying which populations are the most susceptible to disinformation, analyzing current and emerging trends, and disseminating fact-based narratives to counter propaganda.[3] To foster interagency cooperation with the GEC, Congress authorized government agencies to detail their employees to the new agency.

Major Neill Perry, a U.S. Air Force Reserves intelligence officer assigned to the 446 Airlift Wing at Joint Base Lewis-McChord, Washington. As a civilian, he is a software engineer.

Congress organized this agency under the State Department because of the latter's traditional roles in official communication and foreign engagement.[4] In fact, the GEC is the latest iteration of a series of State Department agencies dedicated to countering foreign influence. The GEC itself replaced the Center for Strategic Counterterrorism Communications, which had replaced the Global Strategic Center, which replaced the Counterterrorism Communication Center.[5] However, these predecessor agencies focused on countering influence campaigns by violent extremist groups, such as ISIS. In the aftermath of the 2016 presidential election, GEC took on the much broader mission of leading the USG's fight against all disinformation.[6]

Despite the expansive congressional mandate, the GEC retreated towards a supporting role. "If I could really use one word to characterize the whole philosophical approach of the Global Engagement Center, it's partnerships,"[7] stated Daniel Kimmage, principal deputy coordinator at the GEC.[8] Mr. Kimmage explained that this approach is driven by the assumption that the USG is often "not the most effective communicator with most audiences." Instead, the agency focuses on identifying and supporting other organizations that are on the front line of disinformation. To support partner groups, the GEC distributes grants to local news agencies and civil society groups[9] and maintains an online platform–Disinfo Cloud–where groups can showcase their tools for fighting disinformation.[10]

The problem with the GEC's approach is that it is ill-suited for disinformation intended for American audiences. Instead, the GEC's approach seems to be a holdover from its predecessor agencies, which focused on countering ISIS propaganda.[11] The difference between the two types belies the GEC's principal assumption. To recruit new members, ISIS targeted Muslims, most of whom were not American.[12] From the perspective of a foreign audience, the USG was "not the most effective communicator."[13] Therefore, it made sense to let other entities and partners take the lead role against terrorist propaganda.

However, the GEC's assumption does not hold when the target audience is American. As the Senate Select Committee noted in its report, the operational focus of the 2016 Russian influence campaign was to "push Americans further away from one another, and foment distrust in government institutions."[14] The target audience for that influence campaign was the American people at large, not foreign nationals. And from the perspective of the domestic audience, the federal government would be a more effective communicator than civil groups. In this context, it is mistake for the GEC to remain quiet.

The COVID Infodemic

The coronavirus ignited a global pandemic that has infected tens of millions and killed over one million people. It also sparked what the World Health Organization (WHO) labelled an "infodemic," a surfeit of lies and half-truths that undermine the public health response.[15] Like the COVID-19 virus, the infodemic has also infected millions of people and has cost lives.

COVID-19 has provided an ideal accelerant for disinformation. First, it is novel. Most people are unacquainted with the family of coronaviruses. Unlike maladies that have afflicted humanity for millennia, human coronaviruses were not identified until the 1960s.[16] Even experts have struggled to understand the new virus and its transmission vectors. From the outbreak, the public received conflicting and changing messages on the risks and the prophylactics of the virus. Second, the virus has inspired strong emotional reactions. It is lethal. As a new disease that threatens millions of people, it inspires anxiety.[17] News media showed images of patients on ventilators, overflowing hospitals, and numerous siren-blaring vehicles in lockdown cities. In sum, people fear the unknown and they fear death. These powerful emotional responses are a fertile environment for disinformation to flourish—and flourish it did.

The Empirical Studies of Conflict Project identified over 3,500 incidents of coronavirus-related disinformation.[18] There are hoaxes, scams, and fraudulent claims that coconut water, Clorox, breast milk, and vodka prevent or cure the disease. Many of these are perpetuated by charlatans and quacks; others are spread by leaders stoking ethnic or racial tension. Political leaders exploited the pandemic to continue their policies of blaming political opponents and ethnic minorities as a means of distracting from their own failures.[19]

Authoritarian governments also spewed disinformation. They did so in an effort to preserve their own power, curtail US and other Western influence, and erode confidence in democracy as a form of government.[20] Russia has engaged in disinformation campaigns targeting Western audiences to undermine trust in public health institutions.[21] Russia aims to "erode trust in institutions, such as host governments and traditional media, often by proliferating multiple false narratives."[22] Iran blames Israel and the US for creating the virus.[23] In a notable development, Chinese actors have begun to adopt Russian smear tactics, namely employing trolls and fake social media accounts to disseminate their message.[24] According to the GEC report, China, Russia, and Iran influence campaigns now echo one another.[25] Their common theme

is that the US shoulders responsibility for the pandemic because the disease originated as an American biological weapon.

GEC's Leadership of the Government Response

GEC's actions during the pandemic have not measured up to the magnitude of the problem or the weight of GEC's responsibilities. For an entity responsible for coordinating USG's response to disinformation, the GEC has been strangely anonymous and has no social media presence. Without a Twitter or Facebook account, it relies on other government agencies to tweet out links to its reports.[26] The GEC's reticence stands in contrast to the Cybersecurity and Infrastructure Security Agency (CISA), which posts regularly to its Twitter, Facebook, LinkedIn, and YouTube accounts. CISA, a Department of Homeland Security component, aggressively used its social media accounts to counter disinformation during the 2020 presidential elections.

GEC has also been reluctant to share its expertise publicly. In February 2020, the Center identified a Russian disinformation campaign that involved thousands of social media accounts disseminating over two million tweets in multiple languages.[27] Allegedly, this campaign attributed the coronavirus to a diabolic ploy of American philanthropists, but GEC never released its report or otherwise shared its findings.[28] Silence in the fight against disinformation, is not a virtue. The global pandemic was an opportunity for the GEC to step up and warn the American people about ongoing foreign influence campaigns, but it failed to do so.

Other federal agencies have stepped in to counter the infodemic. The CISA created a COVID-19 Disinformation Toolkit to help state, local, and tribal governments combat disinformation.[29] The National Security Agency warned about foreign adversaries spreading disinformation online.[30] The Federal Bureau of Investigation (FBI) warned of coronavirus-related scams[31] and Chinese network intrusions against COVID-19 research organizations.[32] The Centers for Disease Control and Prevention (CDC) cautioned about coronavirus-related misinformation.[33] The Federal Emergency Management Agency (FEMA) established a Coronavirus Rumor Control website to provide authoritative information.[34] As other federal agencies reached out to the American people directly, the GEC seems to prefer to look inward towards its agency partners.

Experts who study disinformation recommend a bevy of solutions to stop disinformation, the most relevant to this article is the need for a whole of government approach.[35] This approach accepts the reality that no single agency can do it alone: "No single department or agency possesses the clout, expertise, or resources to make things happen across the USG on the scale needed to counter Russian disinformation."[36] Each federal agency has its own unique tools. For instance, Department of Defense (DoD) can disrupt botnet armies that disseminate misinformation, which is what U.S. Cyber Command (USCYBERCOM) did during the 2020 election season.[37] The Department of Justice (DOJ) is empowered to prosecute those who spread disinformation on behalf of foreign governments under the Foreign Agent Registration Act, which it did against the Internet Research Agency for its role in the 2016 elections.[38]

Déjà Vu All Over Again

In 2019, just as the coronavirus pandemic was beginning, Congress created another center dedicated to fighting disinformation.[39] This time, Congress directed the Office of the Director of National Intelligence (ODNI) to create a Foreign Malign Influence Response Center (FMIRC). This new center will "serve as the primary organization in the United States Government for analyzing and integrating all intelligence possessed or acquired by the United States Government pertaining to foreign malign influence."[40] The FMIRC will also provide assessments and reports about foreign malign influence to Congress and federal agencies,[41] and the director of the FMIRC may recommend "potential responses by the United States to foreign malign influence."[42]

The decision to create a new agency is puzzling for two reasons. First, the FMIRC duplicates the mission of the GEC. The GEC already produces assessments on influence operations, including a team of thirty data scientists who monitor the public information environment and share their analysis with the State Department and interagency partners.[43] Second, Congress did not elaborate on how the FMIRC would work with the GEC. In passing this legislation, Congress did not eliminate the GEC or reduce its mission. Not only does the GEC continue to exist, it may soon wield greater resources. In May 2021, the Senate passed legislation that would double the GEC's annual budget[44] and would encourage the GEC to exchange liaison officers with the National Counterterrorism Center, the combatant commands, and other federal agencies.[45]

At this point, any discussion of how the two agencies will cooperate is academic. Congress passed the enabling legislation in 2019, but at the time of this article's publication, the FMIRC does not yet exist. The Trump administration did not create the agency during the last year of its term,[46] and the Biden administration still has not done so. In April 2021, the new Director of National Intelligence, Avril Haines, testified she was "moving with alacrity towards" establishing the FMIRC. Director Haines indicated that she wanted the FMIRC to avoid duplicating existing efforts within the USG.[47]

Nations and private actors exploited the coronavirus pandemic to publish disinformation to support their preexisting agendas.[48] Authoritarian regimes sought to undermine US world standing and to erode Americans' confidence in their government. The USG mounted a scattershot response against these narratives even as some federal agencies used their social media accounts and websites to warn about the presence of disinformation and redirect citizens to trustworthy sources. Although tasked with coordinating the USG's response to disinformation, the GEC remained in the background. The GEC's recent performance reifies one critique that the GEC "essentially operates as a grant-making body."[49] Congress and the Biden administration should reform both the GEC and the federal government's response as a whole. Although the pandemic will eventually subside, disinformation will endure.◉

NOTES

1. U.S. Senate Select Committee on Intelligence, Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia's Use of Social Media with Additional Views, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

2. U.S. Congress, National Defense Authorization Act for Fiscal Year 2017, https://www.congress.gov/bill/114th-congress/senate-bill/2943/text.

3. U.S. Congress, National Defense Authorization Act for Fiscal Year 2017, https://www.congress.gov/bill/114th-congress/senate-bill/2943/text.

4. Lumpkin, M., "Countering Adversarial Propaganda Hearing for Members of the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, October 22, 2015, https://docs.house.gov/meetings/AS/AS26/20151022/104086/HHRG-114-AS26-Wstate-LumpkinM-20151022.pdf.

5. Office of the Spokesperson, U.S. State Department, "The Global Engagement Center" (July 6, 2016), https://2009-2017.state.gov/r/pa/prs/ps/2016/07/259376.htm.

6. LaGraffe, M., "Global Engagement: Center Seeks to Counter Terror Groups," *State Magazine* (Issue 616) October 2016.

7. Vincent, B., "How State's Disinformation-Fighting Arm Uses Artificial Intelligence," *Nextgov* (April 16, 2021), https://www.nextgov.com/emerging-tech/2021/04/how-states-disinformation-fighting-arm-uses-artificial-intelligence/173401.

8. Daniel Kimmage's LinkedIn page, accessed August 28, 2021, https://www.linkedin.com/in/danielkimmage.

9. Taylor, G., "State Department Global Engagement Center Targets Russian Propaganda, 'Deep Fakes,'" *The Washington Times* (December 12, 2018), https://apnews.com/article/9f7892a163582b5fd0297e2a81124c35.

10. U.S. State Department, "Disinfo Cloud," https://www.state.gov/disinfo-cloud-launch/.

11. Daniel Kimmage, "Policy Forum: Countering and Exposing Terrorist Propaganda and Disinformation," (February 17, 2021), https://www.youtube.com/watch?v=HTUHW9ldyzY.

12. Koerner, B.I., "Why ISIS Is Winning the Social Media War," Wired, (March 2016), https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat.

13. Katz, R., "The State Department's Twitter War with ISIS Is Embarrassing," Time (September 14, 2014), https://time.com/3387065/isis-twitter-war-state-department.

14. Senate Intelligence Committee, Report on Russian Active Measures Campaigns, Volume 2.

15. World Health Organization, "Managing the COVID-19 Infodemic: Promoting Healthy Behaviors and Mitigating the Harm from Misinformation and Disinformation" (September 23, 2020), https://www.who.int/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation.

16. Centers for Disease Control and Prevention, "Human Coronavirus Types" (February 15, 2020), https://www.cdc.gov/coronavirus/types.html.

17. P. Beaumont, et al., "Malicious Forces Creating 'Perfect Storm' of Coronavirus Information," *The Guardian* (April 24, 2020), https://www.theguardian.com/world/2020/apr/24/coronavirus-sparks-perfect-storm-of-state-led-disinformation.

18. J. Shapiro, et al., "ESOC COVID-19 Disinformation Tracking Report," (2020), https://esoc.princeton.edu/publications/esoc-covid-19-disinformation-tracking-report.

19. T. Erdemir, et al., "Usual Suspects: Iran and Turkey's Scapegoating of Minorities During Covid-19," Anti-Defamation League (June 11, 2020), https://www.adl.org/blog/usual-suspects-iran-and-turkeys-scapegoating-of-minorities-during-covid-19.

20. K. Stricklin, "Why Does Russia Use Disinformation?," Lawfare (March 29, 2020), https://www.lawfareblog.com/why-does-russia-use-disinformation.

21. G. Corn, "Coronavirus Disinformation and the Need for States to Shore Up International Law" (April 2, 2020). https://www.lawfareblog.com/coronavirus-disinformation-and-need-states-shore-international-law.

22. T. Helmus, et al., "Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe," Rand Corporation, 2018, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2237/RAND_RR2237.pdf.

23. K. Aarabi, "Iran Knows Who to Blame for the Virus: America and Israel," *Foreign Policy* (March 19, 2020), https://foreignpolicy.com/2020/03/19/iran-irgc-coronavirus-propaganda-blames-america-israel/

24. J. Kurlantzick, "How China Ramped Up Disinformation Efforts During the Pandemic," Council on Foreign Relations, September 10, 2020, https://www.cfr.org/in-brief/how-china-ramped-disinformation-efforts-during-pandemic.

NOTES

25. B. Swan, "State Report: Russian, Chinese and Iranian Disinformation Narratives Echo One Another," Politico (April 21, 2020), https://www.politico.com/news/2020/04/21/russia-china-iran-disinformation-coronavirus-state-department-193107.

26. National Counterintelligence and Security Center (August 5, 2020), https://twitter.com/NCSCgov/status/1291146503499767809.

27. L. Kelly, "US Paints Murky Picture of Russian Disinformation on Coronavirus," *The Hill* (March 12, 2020), https://thehill.com/policy/international/487150-us-paints-murky-picture-of-russian-disinformation-on-coronavirus.

28. Swan, "State Report: Russian, Chinese and Iranian Disinformation Narratives Echo One Another."

29. Cybersecurity and Infrastructure Security Agency, "Coronavirus," https://www.cisa.gov/coronavirus.

30. National Security Agency (October 9, 2020), https://twitter.com/NSAGov/status/1314656984084418560.

31. Federal Bureau of Investigation, "Federal Agencies Warn of Emerging Fraud Schemes Related to COVID-19 Vaccines," (December 21, 2020), https://www.fbi.gov/news/pressrel/press-releases/federal-agencies-warn-of-emerging-fraud-schemes-related-to-covid-19-vaccines.

32. Federal Bureau of Investigation, "FBI and CISA Warn Against Chinese Targeting of COVID-19 Research Organizations," (May 13, 2020), https://www.fbi.gov/news/pressrel/press-releases/fbi-and-cisa-warn-against-chinese-targeting-of-covid-19-research-organizations.

33. Centers for Disease Control and Prevention (March 23, 2020), https://twitter.com/CDCgov/status/1242115861114163201.

34. Federal Emergency Management Agency, Coronavirus Rumor Control, last updated August 25, 2020, https://www.fema.gov/disasters/coronavirus/rumor-control.

35. A. Polyakova, et al., "Democratic Defense Against Disinformation 2.0," Atlantic Council Eurasia Center (June 2019), https://www.atlanticcouncil.org/wp-content/uploads/2019/06/Democratic_Defense_Against_Disinformation_2.0.pdf.

36. J. Farwell, "Countering Russian Meddling in US Political Processes," *Parameters* (Spring 2018): 39.

37. E. Nakashima, "Cyber Command Has Sought to Disrupt the World's Largest Botnet, Hoping to Reduce Its Potential Impact on the Election," *The Washington Post* (October 9, 2020), https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-a166-dc429b380d10_story.html.

38. U.S. Department of Justice, "Recent FARA Cases," (February 26, 2021), https://www.justice.gov/nsd-fara/recent-cases.

39. 116th Congress, S. 1790 §5322, National Defense Authorization Act for Fiscal Year 2020, https://www.congress.gov/bill/116th-congress/senate-bill/1790.

40. 50 U.S.C §3059(b)(3).

41. 50 U.S.C §3059(b)(4).

42. 50 U.S.C §3059(c)(2)(C).

43. Daniel Kimmage, "Policy Forum: Countering and Exposing Terrorist Propaganda and Disinformation," Washington Institute (February 17, 2021), https://www.youtube.com/watch?v=HTUHW9ldyzY.

44. Office of U.S. Senator Rob Portman, "Press Release: Portman, Murphy Applaud Inclusion of Provision to Fight Global Propaganda and Disinformation in Senate Passage of U.S. Innovation and Competition Act" (June 8, 2021), https://www.portman.senate.gov/newsroom/press-releases/portman-murphy-applaud-inclusion-provision-fight-global-propaganda-and.

45. 117th Congress, S.1260 § 3137(c), United States Innovation and Competition Act of 2021, https://www.congress.gov/bill/117th-congress/senate-bill/1260/text.

46. Office of U.S. Senator Amy Klobuchar, "Press Release: Klobuchar, Reed, Peters Urge National Security Officials to Take Steps to Counter Foreign Influence Campaigns," (February 25, 2021), https://www.klobuchar.senate.gov/public/index.cfm/news-releases?ID=1EDA4FBA-8E2B-4ADD-8AFA-5D762856B20B.

47. *Worldwide Threats: Testimony before the Committee on Armed Services,* 117th Congr., (2021)(testimony of Avril Haines, Director of National Intelligence).

48. U.S. State Department, *GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem* (August 2020), https://www.state.gov/russias-pillars-of-disinformation-and-propaganda-report.

49. N. Jankowicz, *How to Lose the Information War* (London: I.B. Tauris, 2020), 196.