Statement of

NINA JANKOWICZ

Woodrow Wilson International Center for Scholars

Science and Technology Innovation Program

BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES

ARMED SERVICES COMMITTEE

Subcommittee on Cyber Innovative Technologies and Information Systems

Concerning

“Technology and Information Warfare:
The Competition for Influence and the Department of Defense”

April 30, 2021

Chairman Langevin, Ranking Member Stefanik, and distinguished Members of the subcommittee, thank you for the opportunity to discuss technology, information warfare, and the competition for influence with you.

I am the daughter of a veteran. My father—an aerial reconnaissance officer in Vietnam—died in 2010 after complications from multiple myeloma, which he contracted as a result of his exposure to Agent Orange during his service. I know he would be thrilled to see me testifying before this committee in the service of truth.

I have spent my career on the front lines of the information war. I worked on Russia and Belarus programs at the National Democratic Institute, a target of authoritarian information operations (IO) including from Moscow and Beijing. Under a Fulbright Public Policy Fellowship, I advised the Ukrainian Ministry of Foreign Affairs on strategic communications. I spent the last four years researching how our allies in Central and Eastern Europe dealt with Russian online aggression long before the United States even recognized it as a threat.[1]

Since I began studying this topic, I have observed incremental improvements in the way social media companies, the press, the American people, and government have responded to the threat of disinformation. Now, at least, we seem to all recognize the threat *exists*. But as I told your colleagues on the Appropriations Committee at a 2019 hearing on responding to disinformation, "the United States has been a tardy, timid, or tertiary player...stymied by domestic politicization."[2]

Unfortunately, the same conclusion holds true today, nearly two years later. So it also bears repeating: **disinformation is not a partisan issue. As we witnessed throughout the COVID-19 pandemic and especially on January 6, it is a democratic one, affecting public health, public safety, and the very processes by which the United States is governed.** It is critical that Congress understand this; otherwise, we remain vulnerable to information warfare, and the policy changes I am recommending today cannot be successful.

How did we get here? In part, our understanding of the problem is to blame.[3] Since the end of the Cold War and the resurgence of great power competition, the United States has conceptualized hostile-state information operations as one-off occurrences—explained away by societal peculiarities, tensions, and events such as elections—that warrant attention only in the moment. Rather than organizing cross-cutting, proactive, whole-of-government responses, we have mostly stood up ad hoc capabilities only when necessary, such as election war rooms before events like the 2018 and 2020 elections.

Furthermore, US government efforts to counter information operations have been largely securitized, primarily involving elements of the Defense, Homeland Security, and State Departments, in addition to

[1] Nina Jankowicz, *How to Lose the Information War: Russia, Fake News, and the Future of Conflict* (London: Bloomsbury/IBTauris, 2020).

[2] Nina Jankowicz, Testimony before the House Appropriations Committee, State and Foreign Operations Subcommittee, July 10, 2019.

[3] Adapted from Nina Jankowicz and Henry Collis, "Enduring Infomation Vigilance: Government after COVID-19," *Parameters* 50, no. 3 (2020).

the Intelligence Community. They rarely focus on building broader resilience. Even within the national security establishment, there is too little recognition of the need to shore up domestic vulnerabilities as part of a winning Counter-IO strategy.

Russia, China, and other authoritarian states, however, know these vulnerabilities are the key to gaining ground in the information war. **Adversaries like Moscow and Beijing utilize an integrated approach to information operations** and take advantage of American inaction on the issue. They have recognized the utility of engaging in **"perpetual information competition,"** which has three main characteristics:[4]

1. They understand **information competition is the new normal and are constantly probing for and exploiting societal fissures**. We have observed this in the past year as both countries amplified conspiracies about the origins of the COVID-19 pandemic and the efficacy of Western-made vaccines.[5] Russian Internet Research Agency (IRA) employees were instructed to instigate "political intensity" by "supporting radical groups, users dissatisfied with [the] social and economic situations and oppositional social movements."[6] Their accounts have pushed the Qanon conspiracy theory and augmented racial tensions around the Black Lives Matter movement in the United States.[7]

2. They **use all channels available—government and nongovernment, online and offline—to engage in this behavior**. China, for example, has utilized the "three warfares"—public opinion or media warfare, psychological warfare, and legal warfare—to shape international opinion since 2003. A wide range of state bodies—not just the traditional national security sector—are involved in China's efforts to influence 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 social media to promote the CCP position abroad.[8] This has included efforts to influence Western opinions about the protests in Hong Kong,[9] and, more recently, campaigns likely connected to the CCP attempting to paint a positive picture of life in Xinjiang.[10]

3. Finally, they know that **perpetual information competition does not adhere neatly to international borders, but rather exploits them**, **attempting to undermine the unity of**

[4] Jankowicz and Collis, 18.

[5] Bret Schafer et al, "Influence-enza: How Russia, China, and Iran Have Shaped and Manipulated Coronavirus Vaccine Narratives," Alliance for Securing Democracy, March 6, 2021.

[6] United States v. Elena Alekseevna Khusyanynova, 1:18-MJ-464 (E.D. Va 2018), 24.

[7] Ben Collins and Joe Murphy, "Russian troll accounts purged by Twitter pushed Qanon and other conspiracy theories," NBC News, February 2, 2019.

[8] Peter Mattis, "China's Three Warfares in Perspective," *War on the Rocks*, January 30, 2018; and Amy Searight, "Countering China's Influence Operations: Lessons from Australia," Center for Strategic and International Studies, May 8, 2020.

[9] Katie Paul and Elizabeth Culliford, "Twitter, Facebook accuse China of using fake accounts to undermine Hong Kong protests," *Reuters*, August 19, 2019.

[10] Raffi Khatchadourian, Twitter Post, April 23, 2021, 10:53 AM.

alliances and international organizations. Many of Russia's information operations, especially those targeting Ukraine's aspirations to join the Euro-Atlantic community, seek to denigrate Western political and military alliances, such as NATO, the European Union, and even the OSCE, of which Russia is a member. In 2016, when Ukraine sought to ratify an Association Agreement with the European Union, Russia saw an opportunity to undermine both Ukraine's EU aspirations and the European Union's cohesion by influencing the discourse about the Agreement in the Netherlands, which held a referendum on its ratification. Through fabricated videos,[11] alleged funding of fringe political movements,[12] state-sponsored propaganda, and the use of government-organized NGOs to launder information, Russia exploited and amplified Dutch citizens' unfavorable opinions about the EU and Ukraine.[13] Ultimately, voters rejected the Association Agreement and Ukraine was forced to find a diplomatic solution to get it ratified.

In these examples alone, we have observed hostile states engaged in muddying authentic discourse, influencing the outcome of elections and referenda, and pitting Americans against one another. These operations *increase* domestic tension and *decrease* American resilience, our capacity to protect our national security, and our ability to respond to foreign policy and defense policy crises.

To meet the challenge of perpetual information competition, the Department of Defense and broader United States Government should organize themselves around a posture of **Enduring Information Vigilance.** This framework sets out how the USG, through the "three Cs"—capability building, inter-office and interagency coordination, and international cooperation—can work more effectively to detect the vulnerabilities that adversaries exploit, manage those attempts, and ultimately deny adversaries any benefit.[14]

1. **Capability: Beyond Discrete Campaigns**
   In ensuring that the DoD workforce is capable of proactively monitoring and identifying informational vulnerabilities that U.S. adversaries might use in information operations, the old military adage "don't operate the equipment, equip the operator" is prescient. 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 without skilled staff and a baseline of resilience in the general population.

   Enduring Information Vigilance relies on skilled people with a nuanced understanding of the threat who are capable of applying the full range of tools and techniques for monitoring, detecting, and responding to information operations. Section 589E of the 2021 NDAA, which "establish[es] a program for training members of the Armed Forces and civilian employees of the Department of Defense regarding the threat of foreign malign influence campaigns targeted at such individuals and the families of such individuals, including such campaigns carried out through social media" is an excellent starting point for these efforts, given that active-duty

[11] Bellingcat, "Behind the Dutch Terror Threat Video: The St. Petersburg "Troll Factory" Connection," Bellingcat Website, April 3, 2016.
[12] Eline Schaart, "Dutch far-right leader Baudet had ties to Russia, report says," *POLITICO Europe*, April 17, 2020.
[13] Jankowicz, *How to Lose the Information War*, 123-153.
[14] Jankowicz and Collis, 27.

personnel and veterans have both been targets of state-sponsored information operations in the recent past;[15] veterans were also a key contingent among those who stormed the Capitol on January 6.[16] As this program is implemented, it is critical that training is produced together with nonpartisan subject matter and pedagogical experts and is engaging and well-resourced. This broad-based training, which would reach the 2.75 million active-duty, reserve, and civilian employees of the Department of Defense, and could also be rolled out to all civil servants and their families across the Federal Government; a bill providing for such a program is being spearheaded by the Task Force on Digital Citizenship and the Office of Congresswoman Jennifer Wexton.

Beyond such a broad resilience-building program, it is critical to equip specialists with the training and tools they need. The National Security Commission on Artificial Intelligence (NSCAI) suggests the establishment of a "Digital Service Academy to train current and future employees,"[17] though other nations' efforts suggest such training need not be relegated to a standalone body. Instead, a more agile and responsive training program might be integrated into employees' regular professional development activities. U.S. allies have adopted a similar approach; The UK Government trains its public-sector communications personnel on the "RESIST" toolkit, which emphasizes the importance of understanding the objectives of information operations when formulating appropriate responses.[18] Critically, the toolkit points out:

The speed and agility of your response is crucial in countering disinformation. This can mean working to faster deadlines than is usual and developing protocols for responding that balance speed with formal approval from senior officials.[19]

This is not DoD—or the Federal Government's—strong suit. Proactive, creative communications are often stymied and stifled by government clearance processes, resulting in ineffective and even embarrassing products that have little chance at countering sometimes-slick adversarial operations.[20]

2. Coordination: All Sectors, At All Times

The breadth of activity related to hostile state information operations, whether Russian campaigns or China's "three warfares" approach, spans the remit of multiple government agencies. The Department of Defense and wider USG 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

[15] Kristofer Goldsmith, "An Investigation into Foreign Entities Who Are Targeting Troops and Veterans Online," Vietnam Veterans of America, September 17, 2019.

[16] Tom Dreisbach and Meg Anderson, "Nearly 1 In 5 Defendants In Capitol Riot Cases Served In The Military," NPR, January 21, 2021.

[17] National Security Commission on Artificial Intelligence, "Final Report," NSCAI, 2020, 127.

[18] UK Government Communications Service, "RESIST Counter Disinformation Toolkit," Government Communications Service, 2020.

[19] *Ibid.*

[20] Matthew Gault, "Read the Pentagon's 20-Page Report on Its Own Meme," *VICE News*, March 23, 2021.

situated at the forefront of foreign interference, hostile states have the potential to exploit the government's difficulty 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.[21]

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 must be integrated to advance a shared view of what adversaries are doing, whom they are targeting, and whether these activities are effective.

In its report, the NSCAI recommends the creation of a Joint Interagency Task Force bringing together the Departments of "State, Defense, Justice, and Homeland Security, and the [Office of the] Director of National Intelligence to stand-up an operations center to counter foreign-sourced malign information...survey the landscape of relevant public and private actors, coordinate among them, and act in real time to counter foreign information campaigns."[22]

While I agree with the NSCAI's conclusion that the Federal Government requires a central node for the monitoring and coordination of intelligence and policymaking around disinformation, ideally in the White House, my research across Central and Eastern Europe suggests it is necessary to involve nontraditional security departments via leads with the necessary security clearances in such efforts as well. Building this situational awareness across the government will enable the prioritized coordination of effective responses in the short term and beyond. Policy and operational levers for ameliorating vulnerabilities and building resilience against information threats in the long term lie with departments of education, health, and at local levels; 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.[23]

3. **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, and tools, 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. Building cross-border resilience and reducing vulnerability to deny benefit, however, requires enduring cooperation and demonstrations of shared capability and resolve.

The NSCAI suggests that one way to build this resolve is through an international task force to counter and compete against disinformation, led by the Global Engagement Center (GEC) at the

[21] European Center of Excellence for Countering Hybrid Threats, "Tackling the Bureaucratic Vulnerability: An A to Z for Practitioners," European Center for Countering Hybrid Threats, 2020.
[22] National Security Commission on Artificial Intelligence, 274.
[23] Nina Jankowicz, "The Disinformation Vaccination," *Wilson Quarterly*, Winter 2018.

Department of State.[24] In principle, this is an operable suggestion, though I would add some nuance to its implementation. To begin with, the GEC's remit is too large, budget too small, and reputation within the interagency and international community too uncertain to add such a task force to its portfolio. Currently, the GEC conducts open source intelligence analysis in addition to its coordination, policymaking, and programmatic work. I recommend that intelligence gathering and analysis be left to the Intelligence Community and shared within the interagency. While the GEC should benefit from such analysis, its limited resources are better allocated in coordinating with embassies and other agencies in establishing and implementing policy and program priorities.

Finally, while the idea of a task force for international coordination is a noble one, the United States must be careful not to reinvent the wheel in its desire to engage on issues related to information operations. We are arriving late to this party and should seek to use American convening power to augment, not upstage, existing task forces and coordination efforts, particularly those spearheaded by close allies, such as the International Partnership for Countering State-Sponsored Disinformation (led by the United Kingdom in cooperation with the GEC) and the G7 Rapid Response Mechanism (led by Canada).[25]

Enduring Information Vigilance cannot be built overnight; it requires a long-term commitment that will likely outlast the political class initiating it. 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.

It bears repeating that our democratic values are at the core of Enduring Information Vigilance. Adversaries use information operations to exploit open societies and undermine these shared values; therefore, they must remain the center of gravity for any approach to countering hostile interference. Preserving our transparency, openness, and commitments to freedom of expression and human rights will ensure the United States continues to provide an alternative to authoritarian regimes. **We must act not only as the staunchest defender and guarantor of these values among our allies abroad, but lead by example, underlining that disinformation knows no political party and that the United States is committed to reversing its normalization in our own political discourse.**

Once again, Chairman Langevin, Ranking Member Stefanik, and Members of the Subcommittee, it has been an honor to share my thoughts with you today, and I look forward to answering your questions.

[24] National Security Commission on Artificial Intelligence, 278.

[25] Global Affairs Canada, "Rapid Response Mechanism Canada - Protecting Democracy," GAC, June 9, 2019.