Atlantic Council DFRLab

Effective US government strategies to address China's information influence

By Kenton Thibaut
Edited by Iain Robertson and Zoë Aikman

Atlantic Council

Driven by the mission of "shaping the global future together," the Atlantic Council is a nonpartisan, global organization that galvanizes US leadership and engagement in the world, in partnership with allies and partners, to shape solutions to global challenges. Incubated at the Atlantic Council in 2016, the Digital Forensic Research Lab (DFRLab) is a field-builder, studying, defining, and informing approaches to the global information ecosystem and the technology that underpins it. The DFRLab uses open-source methodologies to uncover the origin of disinformation narratives and inauthentic activity, identify the content in use, measure spread within and across platforms, and evaluate engagement and audience reach. This approach is centered in the human expertise of a team of individuals based on-the-ground across five continents who apply language and local contextual expertise to produce a comprehensive and transparent assessment of any given investigation.

Atlantic Council
1030 15th Street NW, 12th Floor
Washington, DC 20005

For more information, please visit www.AtlanticCouncil.org.

July 2024

The mission of the Digital Forensic Research Lab (DFRLab) is to identify, expose, and explain disinformation where and when it occurs using open-source research; to promote objective truth as a foundation of government for and by people; to protect democratic institutions and norms from those who would seek to undermine them in the digital engagement space; to create a new model of expertise adapted for impact and real-world results; and to forge digital resilience at a time when humans are more interconnected than at any point in history, by building the world's leading hub of digital forensic analysts tracking events in governance, technology, and security.

Kenton Thibaut is a senior resident China fellow at the Atlantic Council's Digital Forensic Research Lab (DFRLab), where she leads China-related research and engagements in the Democracy + Tech Initiative.

The author would like to thank the following reviewers for their thoughtful feedback and recommendations:

- Emerson Brooking
- Graham Brookie
- Rose Jackson

Effective US government strategies to address China's information influence

By Kenton Thibaut
Edited by Iain Robertson and Zoë Aikman

Table of Contents

Executive Summary

China's global influence operations have received increasing attention in the national security community. Numerous congressional hearings, media reports, and academic and industry findings have underscored China's increased use and resourcing of foreign information manipulation and interference (FIMI) tactics in its covert operations both in the United States and abroad.

In response, US government offices the Foreign Malign Influence Center (FMIC), the Global Engagement Center (GEC), and the Cybersecurity and Infrastructure Security Agency (CISA), among others, have made strides in raising awareness of the issue and charting pathways to increase the resilience of the US information ecosystem to foreign influence. To date, however, the efforts to counter the influence of the People's Republic of China (PRC) have been fragmented. That fragmentation is indicative of a lack of cohesion around the concept of influence operations itself.

Across the government and nongovernment sectors alike, there is considerable variation regarding the definition and scope of information manipulation. For example, the Department of State's (DOS's) GEC has an expansive definition, which includes "leveraging propaganda and censorship, promoting digital authoritarianism, exploiting international organizations and bilateral partnerships, pairing cooptation and pressure, and exercising control of Chinese-language media."[1] Others define it more narrowly as disinformation and propaganda spread by a foreign threat actor in a coordinated, inauthentic manner, and largely occurring on social media platforms.[2]

This variation is a reflection of the holistic and multifaceted nature of Chinese influence. Coercive tactics and influence operations have long been a central part of China's strategic tool kit and core to how it engages with the outside world. Because China conceives of the information domain as a space that must be controlled and dominated to ensure regime survival, information operations are part of a much bigger umbrella of influence that spans the economic, political, and social domains.[3] It may be more useful to think of information manipulation as existing within the broader conceptual framework of China's weaponization of the information domain in service of its goal to gain global influence.

As previous work by the Digital Forensic Lab (DFRLab) has shown, China's approach to the information domain is coordinated and proactive, taking into account the mutually constitutive relationships between the economic, industrial, and geopolitical strategies of the Chinese Communist Party (CCP). The aim of its efforts is to gain influence—or "discourse power"—with the ultimate goal of decentering US power and leadership on the global stage.[4] One of the main mechanisms through which the CCP seeks to achieve this objective is by focusing on the dominance of information ecosystems. This ecosystem encompasses not only narratives and content that appear in traditional and social media but also the digital infrastructure on which communication systems rely, the policies that govern those systems at the international level, and the diplomatic strategy deployed by Beijing's operatives abroad to gain buy-in for the CCP's vision of the global order.[5]

The DFRLab's previous two reports, which explored China's strategy and the impacts of its operations abroad, found that the United States will not be successful in addressing the challenges of Chinese influence if it sees that influence as separate from the interconnected economic, political, and technical domains in which its strategy is embedded.

To this end, the DFRLab hosted a series of one-on-one expert interviews, conducted research and workshops, and held a virtual roundtable discussion with scholars and practitioners with expertise on or experience in addressing authoritarian influence and information operations, US government processes and policies around these issues, and Chinese foreign policy. This issue brief is part of a larger body of work that examines the Chinese government's interests and capabilities and the impacts of party's efforts to shape the global information ecosystem.[6] The focus of this report is on how the US government can best respond to those challenges, including the architecture, tools, and strategies that exist for addressing PRC influence and information manipulation, as well as any potential gaps in the government tool kit.

This report finds that, to mount the most effective response to Chinese influence and the threat it poses to democratic interests at home and on the international stage, the United States should develop a global information strategy, one that reflects the interconnected nature of regulatory, industrial, and diplomatic policies with regard to the information domain. A core

1 "How the People's Republic of China Seeks to Reshape the Global Information Network," US Department of State, September 28, 2023, https://www.state.gov/gec-special-report-how-the-peoples-republic-of-china-seeks-to-reshape-the-global-information-environment/.

2 Monica Murero, "Coordinated Inauthentic Behavior: An Innovative Manipulation Tactic to Amplify COVID-19 Anti-Vaccine Communication Outreach via Social Media," *Frontiers in Sociology* 8 (2023), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10060790/#:~:text=Coordinated%20inauthentic%20behavior%20(CIB)%20is,across%20multiple%20social%20media%20platforms.

3 See *U.S. Response to China's Foreign Influence Operations*, US House Committee on Foreign Affairs, Subcommittee on Asia and the Pacific (2018) (statement of Peter Mattis, Jamestown Foundation fellow), https://www.congress.gov/115/meeting/house/108056/witnesses/HHRG-115-FA05-Wstate-MattisP-20180321.pdf; Dr. Mareike Ohlberg et al., *Countering China's Information Manipulation in the Indo-Pacific and Kazakhstan: A Framework for Understanding and Action*, International Republican Institute, 2023, https://www.iri.org/resources/countering-chinas-information-manipulation-in-the-indo-pacific-and-kazakhstan/; Matt Schrader, *Friends and Enemies: A Framework for Understanding Chinese Political Interference in Democratic Countries,* Alliance for Securing Democracy, April 22, 2020, https://securingdemocracy.gmfus.org/wp-content/uploads/2020/04/Friends-and-Enemies-A-Framework-for-Understanding-Chinese-Political-Interference-in-Democratic-Countries.pdf.

4 Kenton Thibaut, *Chinese Discourse Power: Ambitions and Reality in the Digital Domain*, DFRLab, August 2022, https://www.atlanticcouncil.org/wp-content/uploads/2022/11/Chinese-Discourse-Power-Ambitions-and-Reality-in-the-Digital-Domain.pdf; Kenton Thibaut, *Chinese Discourse Power: Capabilities and Impact,* DFRLab, August 2023, https://www.atlanticcouncil.org/wp-content/uploads/2023/08/Chinese-Discourse-Power-Capabilities-and-Impact-1.pdf.

5 Ibid; Ibid.

6 Ibid.

assumption undergirding this concept is that US policymaking space tends to over-index on the threat of information manipulation in particular while under-indexing on the core national interest of fostering a secure, interoperable information environment on a larger scale.

The limits of understanding Chinese influence as systemic and part of a broader strategy has sometimes led US response to be pigeonholed as an issue of strategic communications, rather than touching on the information and technology ecosystems, among others, where China focuses its information and influence efforts. Responding to Chinese influence with government messaging is not sufficient to address the complex nature of the challenge and places the United States in a position of reactivity.

In short, understanding that the CCP (1) integrates its tech industrial strategy, governance policy, and engagement strategy and (2) connects its approach at home to how it engages abroad, the United States needs to do the same, commensurate with its values. It should not respond tit-for-tat but rather have a collective strategy for a global competition for information that connects its tech strategy to its governance approach to its engagement around the world.[7]

That is not to say that a US strategy on information resilience should mirror China's, or that such a strategy should be developed in response to the PRC's actions in the information domain. Nor is it to say that the United States should adopt a similar whole-of-government approach to the information domain. There are silos by design in the US system and important legal and normative foundations for the clear delineation of mission between them. What this issue brief argues for is a strategic breaking down of silos to facilitate proactive action versus a dangerous breaking down of legally required silos.

This report emphasizes that the United States should articulate how major initiatives like the CHIPS and Science Act, regulatory approaches like the recent executive orders on AI and data security, and the DOS's recent cyberspace and digital policy strategy are part of a cohesive whole and should be understood and operationalized as such.

The strategy should outline what the United States stands for as much as what it is against. This requires that the United States frame its assessment of threat within a broader strategy of what its values are and how those values should be articulated in its regulatory, strategic, and diplomatic initiatives to promote open information environments and shore up information resilience. This includes working with allies and partners to ensure that a free, open, and interoperable internet is a global priority as well as a domestic one; developing common standards for understanding and thresholding foreign influence; and promoting connectivity at home and abroad. One finding of this report is that the United States is already leaning into its strengths and values, including championing policies that support openness and continuing support for civil society. This, along with the awareness of influence operations as the weaponization of the information domain, is a powerful response to authoritarian attacks on the integrity of both the domestic US and global information spaces.

The United States has a core national security interest in the existence of a rules-based, orderly, and open information environment. Such an environment facilitates the essential day-to-day tasks related to public diplomacy, the basic expression of rights, and investment in industries of strategic and economic value. Absent a coherent strategy on these core issues related to the integrity of the United States' information environment that is grounded in an understanding of the interconnected nature of their constitutive parts, the challenges of foreign influence and interference will only continue to grow.

This issue brief contains three sections. For sections one and two, experts in different aspects of the PRC's information strategy addressed two to three main questions; during the course of research, further points were raised that are included in the findings. Each section represents a synthesis of the views expressed in response to these questions. The third section comprises recommendations for the US government based on the findings from the first two sections.

Section 1: Baselining the PRC's weaponization of the information domain

What is China's information strategy and how has it evolved? Where is it going? What areas of the policy conversation are understudied?

China's information strategy has undergone a significant transformation in the past five years, moving beyond mere digital influence to a comprehensive exercise of political power on a global scale. While digital operations are a notable aspect, they represent only a fraction of China's broader strategy aimed at shaping international discourse and perceptions in its favor. Thus, over-indexing on the digital side of influence in the form of "information operations" misses the bigger picture: China's efforts in the information domain are about exercising political power abroad.

Over the past few years, a series of trends have emerged, revealing the CCP's concerted effort to wield influence abroad through a web of covert operations. At the heart of these operations lies a coordinated strategy, orchestrated by different branches of the CCP. Explicit indications of directed actions toward signals intelligence and proprietary platform information have demonstrated a coordinated effort to align and array the entire CCP apparatus, including the People's Liberation Army, the United Front Work Department (UFWD), the Public Security Bureaus, and the Ministry of State Security. As indus-

7 For more on the challenges of fighting disinformation and the strengths and weaknesses of countermessaging campaigns, see Jon Bateman and Dean Jackson, *Countering Disinformation Effectively: An Evidence-Based Policy Guide,* Carnegie Endowment for International Peace, January 31, 2024, https://carnegieendowment.org/research/2024/01/countering-disinformation-effectively-an-evidence-based-policy-guide?lang=en.

try, government, and counterespionage experts observed, this overarching command and control structure suggests a meticulous alignment of resources toward shaping narratives and influencing political spaces beyond China's borders.

Increased coordinated efforts complement further emerging trends of the PRC, from the involvement of domestic law enforcement offices in clandestine operations abroad and the convergence of covert disinformation with traditional tradecraft to the rise of transnational repression targeting diaspora communities. In the past couple of years, Chinese state-linked information operations have shifted from almost exclusive clandestine targeting of traditional dissidents, China's neighbors in the Asia-Pacific, and countries in Africa to targeting the political space in the United States and Europe. Recognizing the limitations of overt messaging in the United States, the CCP has turned to covert tactics, utilizing proxies (sometimes unwitting[8]) and targeting subnational or state government offices less familiar with their tactics, including UFWD affiliations.

As part of the increasing overlap between covert tactics and traditional intelligence, new threat actors in China have also begun to participate in influence operations. While operations were traditionally led by foreign-focused entities like the Ministry of Foreign Affairs and the Ministry of State Security, there has been a notable increase in involvement by domestic law enforcement offices undertaking clandestine influence operations overseas. This diversification of actors underscores the wide spectrum of resources at the CCP's disposal, further enhancing its ability to project influence beyond China's borders. Moreover, surveillance and targeting of dissident communities offline now extend seamlessly into online clandestine information campaigns. Private Chinese companies have even begun developing spyware specifically tailored to target these communities, blurring the lines between state-sponsored surveillance and private enterprise.

Equally concerning is the rise of transnational repression tactics employed by the Chinese government to target members of the diaspora community. Public criticism of diaspora members serves as a signal for online operators to harass them, while encrypted apps are used to organize attacks and monitor dissidents.[9] Platforms like WeChat that are used as tools for communication within the diaspora have become instruments of surveillance and propaganda dissemination to mobilize support for China's interests overseas. According to experts on Chinese government messaging on WeChat to overseas Chinese, government accounts use wedge narratives to amplify themes of social and political alienation, with these accounts more likely to discuss anti-Asian hate crimes and political dysfunction in target Western countries.

Despite lacking the sophistication of Russia's information warfare capabilities, China compensates with persistence and the sheer scale of and intent behind its operations. A significant challenge for the United States in effectively dealing with the evolution in China's tactics lies in the lack of information sharing between governments, platforms, and civil society compared to years past. This gap in collaboration exposes vulnerabilities, particularly in the context of upcoming elections where foreign influence could sway outcomes. Therefore, overlooked components of China's information strategy must be worked into robust response strategies that provide the backdrop to proactive action by the United States.

Of particular interest is the underexplored phenomenon of China's targeting of foreign political elites, deploying state-linked disinformation campaigns to influence diaspora communities and shape policy trajectories in host countries. This strategy extends beyond the digital realm, encompassing a spectrum of directed relationships, offline initiatives, and United Front Work organizations' activities, all coordinated to exert political leverage abroad.[10] Recent studies have highlighted how state-affiliated disinformation campaigns towards Canada's Chinese diaspora population target candidates whom Beijing opposes while also trying to sway Liberal Party policies by rallying these communities.[11] These tactics, notably, are not new; China has been undertaking such efforts for years and is remarkably effective in some areas.

China's sophisticated, multilayered approach to shaping global perceptions and policies complicates isolating digital influence from other aspects related to business and trade. A comprehensive understanding of information manipulation thus necessitates contextualization within a larger context to formulate effective countermeasures. Central to this endeavor is identifying and mitigating vectors through which political elites and decision-making processes are influenced, recognizing that these vectors span digital, economic, and geopolitical domains, all of which emanate from China's overarching strategic orientation.

Compounding this challenge is the pervasive misunderstanding of influence operations among affected audiences, necessitating a more nuanced approach to communication and awareness-raising efforts. In particular, bridging this gap is crucial for global majority countries, for whom concepts like "information manipulation" or "media influence" may resonate more than the abstract notion of influence operations. By con-

8 Donie O'Sullivan, Isabelle Chapman, Allison Gordon, and Yahya Abou-Ghazala, "Exclusive: A Baltimore Musician Was Hired to Organize a Protest. He Says He Never Knew His Client Had Links to Pro-China Operatives," CNN, July 26, 2023, https://www.cnn.com/2023/07/26/us/pro-china-information-campaign-invs/index.html.

9 For an example, see Kelly Ng, "Hong Kong Offers HK$1M Bounties on Five Overseas Activists," BBC News, December 14, 2023, https://www.bbc.com/news/world-asia-china-67724230.

10 For more on the United Front, see *China's Global Influence and Interference Activities*, U.S.-China Economic and Security Review Commission (2023) (statement of Peter Mattis), https://www.uscc.gov/sites/default/files/2023-03/Peter_Mattis_Testimony.pdf; Ray Wang and Gerry Groot, "Who Represents? Xi Jinping's Grand United Front Work, Legitimation, Participation and Consultative Democracy," *Journal of Contemporary China* 27, no. 112 (2018): 569–83, https://www.tandfonline.com/doi/abs/10.1080/10670564.2018.1433573.

11 Kenton Thibaut, "China-Linked WeChat Accounts Spread Disinformation in Advance of 2021 Canadian Election," Medium, November 4, 2021, https://medium.com/dfrlab/china-linked-wechat-accounts-spread-disinformation-in-advance-of- 2021-canadian-election-cb5a8389049.

textualizing these issues within familiar frameworks, broader awareness can be cultivated, facilitating more-informed responses to the intricate web of influence woven by the PRC.

Section 2: US Government responses to, and equities concerning, the PRC's weaponization of the information domain

What are the tools and tactics that different parts of the US government are using to address this issue? From your vantage point, do you see gaps of coverage or collaboration? What have you seen work well?

One of the biggest hurdles the United States faces is its treatment of the PRC's influence as an information problem rather than as a strategic question that demands cohesive interagency collaboration and leveraging US strengths and values. In addressing the multifaceted challenge posed by PRC influence, different arms of the US government have employed a range of tools and tactics. At a tactical level, specific strategies are proving effective in countering disinformation and misleading content generated by foreign actors online. Substantial research has supported fact-checking and labeling government-produced content as effective techniques to combat the spread of certain narratives.[12] Moreover, as the potential utilization of generative AI in amplifying foreign influence gains prominence in policy circles,[13] researchers are actively devising innovative techniques to identify and address this type of material.[14]

Focusing government efforts on specific aspects of online influence campaigns, however, could risk compartmentalizing efforts and neglecting the larger strategic picture. In the US government, much of the efforts are siloed, with little interaction between teams whose interests and portfolios align with the issues PRC influence touches upon. Narrowly defining influence as solely in the digital domain (a problem discussed in Section 1) confines the issue to specific agencies like the Federal Bureau of Investigation (FBI), the Office of the Director of National Intelligence (ODNI), and GEC and overlooks its multidimensional aspects that encompass security, democracy, economics, and intelligence.

To illustrate, the US system as structured is largely resourced to identify, attribute, and take down information operations that are concentrated online. This structure, though, may hinder a more holistic response to influence activities, which often encompass much more than coordinated inauthentic behavior online. For example, a combination of US government entities has successfully disrupted operations like "Spamouflage Dragon"—also known as Dragonbridge—which comprised a vast network of accounts linked to Chinese assets that had minimal reach. For operations such as these, within the US government, ODNI is responsible for identifying influence operations, GEC helps with attribution, and the Department of Defense (DoD) helps with disruption. This fragmented approach impedes the development of a holistic strategy to confront the systemic nature of PRC influence. A more strategic, coordinated, and proactive approach to shoring up resilience to PRC influence efforts in the United States and globally is needed.

It is important to note, however, that such a division is intentional and appropriate, as it draws a clear line between foreign activities and constitutionally protected domestic discussions, which is essential for maintaining crucial legal silos between certain departments and agencies handling issues related to information integrity and disinformation. Focusing foreign influence mitigation efforts on online activities, though, may not be the most effective allocation of resources, as illustrated by the minimal reach of online networks like Spamouflage Dragon. A lack of understanding of impact and risk prioritization is evident in the US government's response to foreign information manipulation. At the same time, it is hard to demonstrate value per dollar and successes in stopping China's foothold in other countries, which in turn makes it difficult to figure out the right number of resources to allocate. What is clear is that China's wide-ranging and strategic influence tactics require the United States' responses to be diverse and comprehensive.

This requires a shift in strategic understanding and perspective of the information domain in which the United States operates. In doing so, the United States should not turn away from its values-based strategy, not just for democracy and human rights reasons, but precisely because such a strategy has served it well in advancing its interests globally. As referenced earlier, previous DFRLab research outlined how China's leadership came to view the success of the US model in the international system is largely based on the appeal of US values, including freedom of speech, freedom of the press, and a focus on human rights, and its "open" society. Referencing the success of the US model, the CCP has sought to emulate this strategy as a means to gain influence—or, as it terms it, "discourse power"—on the global stage.[15]

As an example, China has been successful in seeding the narrative that the global connectivity gap between Western and G-77 countries is a result of technological hegemonism, and that the United States (unlike China) will never stand up for the interests of this bloc. Such tactics are aimed at priming countries to be suspicious of the United States and other Western

12 Jon Bateman and Dean Jackson, *Countering Disinformation Effectively.*

13 Nathan Beauchamp-Mustafaga, *Exploring the Implications of Generative AI for Chinese Military Cyber-Enabled Influence Operations,* RAND, February 1, 2024, https://www.rand.org/pubs/testimonies/CTA3191-1.html.

14 "I Wasn't There: Applications of Blockchain to Privacy Preserving Reality Protection," Princeton DeCenter, December 4, 2023, https://decenter.princeton.edu/events/i-wasnt-there-applications-of-blockchain-to-privacy-preserving-reality-protection/

15 Thibaut, *Chinese Discourse Power: Ambitions and Reality in the Digital Domain*; Thibaut, *Chinese Discourse Power: Capabilities and Impact.*

countries, their companies, and their actions. China uses narratives like these to engage in coalition building among G-77 countries and to gain buy-in for its own policy proposals in the United Nations (UN) and other forums—for example, China's efforts to promote the concept of "development as the basic human right" appears with frequency in the most recent zero draft of the United Nation's Global Digital Compact.[16]

Internationally, empowering civil society actors to understand and respond to the multifaceted nature of Chinese influence is essential. China's influence is often underestimated in global majority countries, with limited awareness of its impact. Civil society voices hold significant sway in those regions, often surpassing government communications, particularly where there is historical distrust of the United States. However, funding for civil society initiatives aimed at democracy, human rights, and governance is insufficient. Many organizations are hesitant to accept funding from the DoD or the intelligence community due to inherent skepticism. Therefore, there is a pressing need for increased private and allied funding to address these systemic challenges effectively.

At the same time, there are structural limits to what the US government can—and should—do regarding the information domain. The PRC takes a whole-of-government approach to the information domain because it views it as an arena to be controlled, dominated, and shaped to reflect CCP prerogatives. The US government, by design, maintains legal and normative silos between departments and agencies in order to maintain clear structural limits on the ways government can interact with the domestic information environment.

There is still much the US government can do, however, to lead the way in shoring up information resilience to foreign threats. In the United States, much of the defensive work can be done by strengthening existing commitments and communicating resources and tools to civil society actors, who are increasingly targets of malign actors' efforts. For example, a significant portion of China's global expenditure on technological acquisitions is directed at private sector technology companies in the Bay Area; and Chinese diaspora communities face escalating levels of propaganda, surveillance, and harassment. In this environment, efforts to empower and educate communities serve as a frontline defense against undue PRC influence. Educating communities about the threat posed by state actors, providing access to available resources, and empowering civil society in alignment with US values and constitutional principles are crucial steps in enhancing its information resilience.

In a similar vein, strengthening the United States' own regulatory frameworks and policy spaces is imperative to safeguard against undue PRC influence. The United States presently lacks strategic clarity on protecting critical information infrastructure amid geopolitical competition. Similarly, there is a marked absence of domestic regulations governing core issues like platform transparency and countering foreign interference. Addressing these gaps, while enhancing alignment with partners and allies on its approach to the information environment, will significantly bolster information resilience.

A major finding of this report is that the US policymaking space over-indexes on the threat of foreign malign influence but under-indexes on the core national interest of fostering a resilient information environment. Indeed, a prevailing view among many of the experts interviewed for this series and who have written[17] on the topic was that leaning into core democratic values—including embracing an open information environment and policies that encourage the development of such—is perhaps the single most effective strategy for defending against PRC influence efforts. This, along with a broader awareness of the problem of foreign malign influence, can powerfully counteract authoritarian efforts to undermine the integrity of democratic information spaces, both in the United States and abroad.

Section 3: Recommendations for effective US Government responses to address PRC weaponization of the information domain

While tactical approaches are effective in countering online foreign influence, a notable challenge arises when assessing the larger landscape of PRC influence efforts. One major hurdle is the tendency to view PRC influence primarily as an information problem rather than a complex strategic issue. Addressing this challenge requires a comprehensive approach that involves pooling resources and investments across government departments and agencies. Additionally, crafting well-aligned messaging that integrates policy objectives with diplomatic support is essential.

Shoring up the US regulatory and policy space to better ensure information resilience is key. A commonsense approach to governing the information ecosystem—including regulations on funding, transparency and disclosure of influence-related events, and foreign influence in the US electoral system—can go a long way in protecting the US information ecosystem from PRC weaponization. In this respect, how the United States governs its own companies has a major impact on what it can find out about foreign influence. Congress could pass legislation to this effect to establish standards for transparency and disclosure when platforms are targeted by foreign actors for

16 For more on the GDC, see Konstantinos Komaitis, "The UN Wants More Say Over the Future of the Internet. That's Not Necessarily a Good Thing," Tech Policy Press, March 26, 2023, https://www.techpolicy.press/the-un-wants-more-say-over-the-future-of-the-internet-thats-not-necessarily-a-good-thing/.

17 See, for example, Gavin Wilde, "From Panic to Policy: The Limits of Foreign Propaganda and the Foundations of an Effective Response," *Texas National Security Review* 7, no. 2 (Spring 2024), https://tnsr.org/2024/03/from-panic-to-policy-the-limits-of-foreign-propaganda-and-the-foundations-of-an-effective-response/.

malign influence purposes, to mandate regular public threat reporting, and to encourage avenues for information sharing between platforms and independent researchers.

Outlined below are six categories of recommendations for the United States to best position itself to meet the challenges of governing and defending a free, open, and interoperable information space.

1. Strategy

- **Develop a strategy for the information environment.** To combat malign influence, the United States should contextualize its response to information manipulation by developing an information strategy that is commensurate with its values. This strategy should be referenced in other foreign policy documents in a way that recognizes the interconnectivity between the informational domain and national security strategy. These documents include, for example, DOS's annual Strategic Plan and Integrated Country Strategies, the US Agency for International Development (USAID) and DOS's Joint Strategic Plan, DoD's Strategy for Operations in the Information Environment, the Department of Commerce's and US Trade Representative's strategic plans, and initiatives from the Biden administration such as the CHIPS and Science Act. Central to the articulation of this strategy should be establishing an open information environment as a core national interest—that is, grounding its assessment of threats to the information domain from China or other threat actors in the context of what the United States aims to foster and develop at home and abroad.
- **Ensure this strategy is interlocking and self-referential.** An interlocking, self-referential approach based on US values will serve to advance US interests and increase information resilience and defense at home and abroad. For example, a diplomatic engagement strategy for the Global Digital Compact should be linked with ongoing efforts to address the connectivity gap through investment initiatives like the Partnership for Global Infrastructure and Investment (PGII) in both internal strategy documents and strategic communications. An example of an effective articulation of such an information approach in a strategy document can be found in the DOS's International Cyberspace and Digital Policy Strategy, released in May 2024. The strategy links the building of an open and resilient digital ecosystem to priorities like shoring up resilience against nefarious efforts by China, Russia, and other authoritarian regimes to weaponize the information environment to peddle influence and undermine their enemies. It also takes a stand on what the US government is for: ensuring the security of telecommunication networks, ensuring the effectiveness and transparency of global internet governance bodies like the International Telecommunication Union, and highlighting the centrality of a rights-respecting digital ecosystem that emphasizes multistakeholder processes and is aligned with the approach of its allies.
- **Align US information strategy with the approaches of partners and allies.** The United States should engage consistently with partner countries to align mutual goals of fostering a free, open, and interoperable information environment in multistakeholder and multilateral forums. For example, to bring more allies into the fold around common objectives in the information space, the United States should deploy the full tool kit of existing mechanisms like the Freedom Online Coalition[18] and the many national and international development finance institutions focused on investing in connectivity abroad. Internet governance is a prime example of how strategic articulation of US principles at home and abroad and coordination with partners in various forums has significant impact on US national interests. Indeed, at a policy and governance level, there is little meaningful difference between the domestic and global internet. As such, Chinese efforts to impose state-centric, authoritarian-friendly internet governance norms through processes such as the Global Digital Compact can have a direct impact on how the data and information produced by US citizens flows around the world. Articulating the United States' strong interest in a free, open, interoperable, and secure internet is also essential in this broader information strategy, and should be viewed as a national priority.

2. Legislation

- **Pass legislation on public reporting standards for platform companies.** Congress should pass and enact legislation creating standards for companies to complete quarterly threat reports that are open to the public and outline details of covert state actor activity on their platforms. Companies like Meta and Microsoft routinely release these reports; other social media companies have released them in the past but not at regular intervals. This type of reporting should be mandated as a condition of operation.
- **Pass legislation establishing disclosure standards for industry when foreign threat actors target platforms.** Platforms and communications companies should be required to disclose to the relevant government entities when their platforms are targeted by foreign actors. Currently, such disclosure is entirely up to the companies' discretion and subject to the individual policy of a particular platform. These disclosures should be required as part of routine reporting activities. Such reporting is essential to US government counterparts understanding from a systemic and longitudinal perspective how foreign threat actor activities targeting core communication platforms are evolving over time, allowing for more-effective and more-tailored responses.

18 For more on the Freedom Online Coalition, see Rose Jackson, Leah (Léa) Fiddler, and Jacqueline Malaret, "An Introduction to the Freedom Online Coalition," DFRLab, December 6, 2022, https://dfrlab.org/2022/12/06/introduction-freedom-online-coalition/.

- **Create standards for access to social media data for independent researchers.** Congress could do more to require increased and more-standardized access for independent researchers to relevant social media data related to foreign threats. This would ensure policymakers have visibility in the ways the global information environment is being both weaponized by adversarial countries and used as an early warning and monitoring system.
- **Enhance authority to authorize novel or blended forms of funding.** Congress should be granted the authority to ensure that funding across departments and agencies is allocated in a way that reflects a broader, interconnected information strategy. Given the interconnected nature of foreign influence, a more agile government response that touches on multiple department and agency mandates is needed. Certain departments or agencies will lead in dealing with certain aspects of foreign influence and should pool resources with other government entities that could play meaningful support roles when mutually beneficial to do so. Congress should have greater authority to authorize flexible funding, including pooled funding that can be shared across agencies.

3. Disclosure and transparency

- **Engage in rapid government disclosure of FIMI.** When instances of foreign malign influence threaten public understanding of quickly unfolding events, rapid public disclosure by the relevant US government entities can be extremely valuable. For example, in the lead-up to the Ukraine war, the US National Security Council, the US intelligence community, and other national security agencies worked with allies and partners to quickly declassify and release intelligence to expose Russian disinformation campaigns in almost real time,[19] undermining the effectiveness of Russia's "false flag" campaigns put forward in advance of the invasion as a means of justifying its invasion.
- **Establish declassification standards that support rapid government disclosure.** Hand in hand with the above is rapid declassification of otherwise classified information when the potential benefit to increasing accurate public knowledge deems it appropriate.
- **Enable data sharing and access for researchers to relevant social media data.** Social media platforms should reverse the trend of hollowing out trust and safety teams and shutting down avenues for researcher access to platform data, either by severely restricting what type of data is available (as Meta has down with the shutting down of its social media listening tool CrowdTangle) or by making application programming interface access prohibitively expensive and thus inaccessible to most research organizations (as is the case with the platform X).

4. Information sharing

- **Expand existing interagency mechanisms on elections to cover broader issues related to foreign influence.** The FMIC, the CISA, and the FBI have an existing interagency mechanism to develop public awareness around election-related foreign influence threats. The success of such efforts is exemplified by a recently released guide outlining the threat landscape in regard to foreign malign influence and US election infrastructure.[20] This interagency mechanism should be expanded and capacity built out to share information and intelligence on foreign influence efforts beyond elections.
- **Flag in-process Intelligence Community (IC) products related to foreign influence that may require quick action from authorities during election season.** The IC also has several interagency bodies focused on information sharing, building cross-agency expertise, and facilitating interagency cooperation. Within these existing cooperative mechanisms, the IC should consider a mechanism for flagging in-process products that are making a particular assessment relevant to elections and foreign interference. This would raise awareness in advance of potential cases of foreign malign influence that might require urgent action by the Department of Justice, CISA, or other agencies.
- **Commission a report from relevant departments and agencies on "lessons learned" from elections as a use case for best practices on responding to foreign influence threats more broadly.** The US government should task CISA, FMIC, and other relevant government offices to write a joint report on lessons learned from elections as a use case for understanding institutional structures' strengths, weaknesses, gaps, and capacity related to responding to foreign influence. Elections are relevant indicators for foreign influence because they are a consistent focal point for such activities—they occur at a known moment in time and are high-impact periods (e.g., they require a shared set of facts, citizens to consume information and engage with one another, and citizens to make collective decisions about the future of their societies). The processes and expertise surrounding elections could be useful in informing a more-expansive government approach to foreign influence.
- **Ensure foreign influence frameworks and strategies are aligned with partner approaches.** The GEC, the European External Action Service's (EEAS's) Information Integrity and Countering FIMI division, and other offices in allied and partner countries have existing frameworks on foreign malign influence. These should be contextualized, and relevant offices should develop a mechanism to

19 Katie Bo Lillis, Natasha Bertrand, and Kylie Atwood, "How the Biden Administration Is Aggressively Releasing Intelligence in an Attempt to Deter Russia," CNN, February 11, 2022, https://edition.cnn.com/2022/02/11/politics/biden-administration-russia-intelligence/index.html.

20 "Securing Election Infrastructure Against the Tactics of Foreign Malign Influence Operations," Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, and Office of the Director of National Intelligence, April 2024, https://www.dni.gov/files/FMIC/documents/products/Securing-Election-Infrastructure-Against-The-Tactics-Of-Foreign-Malign-Influence-Operations-Apr2024.pdf.

exchange information on activities undertaken by malign actors in the global information environment.

5. Resource sharing

- **Consider joint or pooled budgets for departments and agencies that engage in countering China's weaponization of the information domain.** Despite significant funding allocated to entities like the DoD, resources remain insufficient for agencies with less financial backing, such as USAID. Pooling resources through joint interagency budgets, as with the DoD- and DOS-funded Countering the PRC Malign Influence Fund (CPIF), could bolster information resilience efforts. Notably, a systemic approach to countering foreign influence alleviates the burden of engaging in tit-for-tat responses, allowing the US government to focus on leveraging its strengths and values. For example, USAID receives limited funding set aside solely to counter and compete with the PRC government, but demand far exceeds supply. In cases where USAID is best positioned—for example, in engaging with US partners abroad on the ground on development financing issues—a joint budget or account could be developed between USAID and DoD to support information resilience.
- **Make existing funding allocated for counter-PRC efforts more fungible.** The resources allocated under funds to counter malign PRC efforts should be made more fungible for organizations that are less resourced but that play a lead role in curbing PRC influence abroad. For example, arrangements between DOS and DoD in previous fiscal years included provisions for fund sharing within CPIF. The Biden administration's budget request for fiscal year 2025 includes a total of $400 million for the CPIF, which is designed to "block PRC inroads, compete with the PRC, and respond concretely to specific PRC challenges."[21] And it includes an additional $2.1 billion to enact the administration's Indo-Pacific Strategy, which also involves curbing PRC influence in the region.
- **Ensure that a broader information strategy is aligned with that of the United States' allies and push other partners to engage more deeply on these issues.** To develop a more proactive vision for ensuring the resilience of the global information environment, the United States should make sure its strategy on engagement around that environment is aligned with the strategies of its allies and partners and that its resourcing reflects this alignment. The EEAS, the British Foreign, Commonwealth, and Development Office, and Global Affairs Canada all have existing engagement mechanisms related to foreign malign influence and are investing in this space. Similarly, US partners such as Japan have recently begun to invest more resources in understanding and countering PRC influence efforts. The United States should push European countries, its Five Eyes partners, and other countries to become more engaged in countering PRC efforts. For example, there may be opportunity for coordination with the Baltic states and other Eastern European states that may be alarmed by China's deepening relationship with Russia post-Ukraine invasion. The Baltics and other Central European states, such as the Czech Republic, may be good partners to raise the issue inside the auspices of the European Union to get the larger body to engage more deeply and proactively.
- **Ensure US diplomatic strategy includes greater public diplomacy efforts to publicize the value of a free, open, and interoperable global information environment.** One promising avenue to provide a positive agenda for what democracies stand for, and an effective counter to Chinese efforts in this space, would be to focus on messaging and investment around connectivity and US and allied efforts to close the digital divide. For example, the CHIPS and Science Act and PGII provide a unique opportunity to foster the development of an open, interoperable, reliable, secure, and trusted internet, expand economic opportunity, position the United States as a leader, defend national security, and provide a credible alternative to Chinese money and influence. Coupled with this messaging should be a coordinated investment strategy that focuses on capacity building across the connectivity ecosystem, which includes community networks, municipal providers, small businesses, and community-focused internet service providers.
- **Support open-source research on China's weaponization of the information domain.** The US government should continue to invest in and increase funding for research into how China views the information environment as a whole that encompasses economic, diplomatic, political, and technical dimensions. While understanding China's digital footprint is important, more research is needed to better understand how, in what ways, and why China engages in the behavior it does and to best understand what its pain points and priorities may be. In parallel could be joint efforts with partners and allies to bolster open-source research globally, as it is essential to public awareness of how threat actors' tactics are evolving.

6. Multistakeholder engagement

- **Engage the multistakeholder community in broader technology policy.** While governments play a leading role in curbing PRC influence, there are limits to what they can (and should) involve themselves in regarding the monitoring and regulation of information spaces. To this end, nongovernmental actors—including from industry, academia, the technical community, and civil society—could be transformative in helping mount an effective defense against malign efforts to weaponize the information environment. In this respect, the United States could leverage the strengths of its multistakeholder approach to global governance to build resilience and defend against Chinese efforts. Opening up university exchange programs

21 See: https://www.state.gov/wp-content/uploads/2024/03/FY-2025-Congressional-Budget-Justification-Appendix-One-Department-of-State-Diplomatic-Engagement.pdf

on technology infrastructure and supporting industry to offer similar exchanges in support of US friendshoring and tech derisking strategies are examples of how to leverage the multistakeholder, nongovernment system to US advantage. One recent example of how this worked in favor of US interests is the April 2024 deal between Microsoft and G42, a United Arab Emirates' AI-focused company, which was arranged under the guidance of the Department of Commerce.[22] As part of the deal for G42 to use its AI models on Microsoft's platforms, the US government required that G42 stop using Huawei telecom equipment.

- **Maintain an active presence and engagement in multilateral forums and ensure civil society is well represented in multistakeholder forums on internet governance.** Authoritarian efforts to undo the multistakeholder model of an open internet are finding new life through the UN's Global Digital Compact. Democratic countries, industry, and civil society must organize a clear, resourced, and urgent strategy to ensure the result does not move the world toward a multilaterally governed (i.e., state-controlled) internet. To do so, they must demonstrate the value of and strong global support for the multistakeholder model and address the G-77 bloc's frustrations with the concentration of tech-related power in the United States and Europe. Focusing on connectivity, digital inclusion, and development in these forums could undercut the well-funded Chinese strategy of taking advantage of global frustrations to advance its interest in a less open and more authoritarian-friendly internet.
- **Expand opportunities for cooperation on science and technology issues, including people-to-people exchange.** As part of the strategy for articulating how to achieve the vision of a free and open global information environment, the United States should have a diplomatic engagement strategy that matches its goal. Similar efforts should be made to enhance the appeal of democratic countries to counter PRC efforts at wooing elites and young talent, especially from global majority countries. The United States and allies should consider opening up more exchange trips, fellowships, scholarships, and US centers abroad to compete with and counter the well-resourced PRC strategy on technology exchange. This creates opportunities for positive narratives, which would require any Chinese effort to spend more time dismantling. While difficult to measure, these types of efforts could cost relatively little compared to other investments and major initiatives the United States may be considering in different parts of the world.
- **Increase funding for civil society and nongovernmental organizations focused on capacity building and research on countering PRC weaponization of the information environment.** As part of a global strategy, the US government should support civil society organizations that focus on educating and training people to understand PRC influence efforts. Educating stakeholders on the UFWD and related influence efforts could be particularly effective in raising awareness. Empowering civil society groups to strengthen safeguards through investment screenings, transparency regulations, and information resilience—rather than putting it in terms of US-China competition—could be a fruitful avenue for getting civil society organizations onboard. For instance, education about the risks of Chinese investment, which often lacks transparency and accountability, could be beneficial. Encouraging collaboration between journalists and civil society organizations could also raise awareness about PRC influence, especially issues like anti-corruption, in local communities. As mentioned earlier, there is a need to bolster open-source research globally to understand how China's weaponization of the information domain plays out on the ground in specific contexts. An example of how this is supported in a constructive way can be found in USAID's most recent draft strategy on democracy, human rights, and governance. In it, USAID outlines emerging focal areas for research, including information manipulation, and highlights that such research "require[s] accompanying investment in learning so that USAID and our partners can more quickly discover which combinations of approaches are effective."

Conclusion

The United States has a fundamental national security interest in maintaining a rules-based, orderly, and open information environment. A coherent strategy must focus on shoring up resilience at home and abroad. A narrow focus on countering China, without taking into account the interdependent nature of information ecosystem and the requirement for a holistic approach, means challenges posed by countries like China weaponizing the information domain will only intensify.

22 Karen Kwok, "Microsoft's G4 Deal Puts UAE in America's AI Tent," Reuters, April 17, 2024, https://www.reuters.com/breakingviews/microsofts-g42-deal-puts-uae-americas-ai-tent-2024-04-16/.

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*Alexander V. Mirtchev

TREASURER
*George Lund

DIRECTORS
Stephen Achilles
Elliot Ackerman
*Gina F. Adams
Timothy D. Adams
*Michael Andersson
Alain Bejjani
Colleen Bell
Sarah E. Beshar
Karan Bhatia
Stephen Biegun
Linden P. Blue
Brad Bondi
John Bonsell
Philip M. Breedlove
David L. Caplan
Samantha A. Carl-Yoder
*Teresa Carlson
*James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
*Helima Croft
Ankit N. Desai
Dario Deste
*Lawrence Di Rita
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Richard Edelman
Stuart E. Eizenstat
Tara Engel
Mark T. Esper
Christopher W.K. Fetzer
*Michael Fisch
Alan H. Fleischmann
Jendayi E. Frazer
*Meg Gentle
Thomas H. Glocer
John B. Goodman
Sherri W. Goodman
Marcel Grisnigt
Jarosław Grzesiak
Murathan Günal
Michael V. Hayden
Tim Holt
*Karl V. Hopkins
Kay Bailey Hutchison
Ian Ihnatowycz
Wolfgang F. Ischinger
Deborah Lee James
*Joia M. Johnson
*Safi Kalo
Andre Kelleners
Brian L. Kelly
John E. Klein
*C. Jeffrey Knittel
Joseph Konzelmann
Keith J. Krach
Franklin D. Kramer
Laura Lane
Almar Latour
Yann Le Pallec
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Marco Margheri
Michael Margolis
Chris Marlin
William Marron
Roger R. Martella Jr.
Gerardo Mato
Erin McGrain
John M. McHugh
*Judith A. Miller
Dariusz Mioduski
*Richard Morningstar
Georgette Mosbacher
Majida Mourad
Virginia A. Mulberger
Mary Claire Murphy
Julia Nesheiwat
Edward J. Newberry
Franco Nuschese
Joseph S. Nye
*Ahmet M. Ören
Ana I. Palacio
*Kostas Pantazopoulos
Alan Pellegrini
David H. Petraeus
Elizabeth Frost Pierson
*Lisa Pollina
Daniel B. Poneman
Robert Portman
*Dina H. Powell McCormick
Michael Punke
Ashraf Qazi
Thomas J. Ridge
Gary Rieschel
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Ivan A. Schlager
Rajiv Shah
Wendy R. Sherman
Gregg Sherrill
Jeff Shockey
Kris Singh
Varun Sivaram
Walter Slocombe
Christopher Smith
Clifford M. Sobel
Michael S. Steele
Richard J.A. Steele
Mary Streett
Nader Tavakoli
*Gil Tenzer
*Frances F. Townsend
Clyde C. Tuggle
Francesco G. Valente
Melanne Verveer
Tyson Voelkel
Kemba Walden
Michael F. Walsh
Ronald Weiser
*Al Williams
Ben Wilson
Maciej Witucki
Neal S. Wolin
Tod D. Wolters
*Jenny Wood
Alan Yang
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Condoleezza Rice
Horst Teltschik
William H. Webster

**Executive Committee Members*

List as of April 24, 2024

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org