FOUNDATION FOR DEFENSE OF DEMOCRACIES

Cognitive Combat

China, Russia, and Iran's Information War Against Americans

Edited by Bradley Bowman

June 2024

Cognitive Combat

China, Russia, and Iran's Information War Against Americans

Edited by
Bradley Bowman

June 2024

FDD PRESS

A division of the
FOUNDATION FOR DEFENSE OF DEMOCRACIES
Washington, DC

Table of Contents

Introduction

By Bradley Bowman

China, Russia, and Iran are waging an information war against the United States, yet many Americans do not realize they are under attack. Nor do they appreciate that developments on the battlefield of ideas and beliefs can have a decisive impact on the security and way of life Americans enjoy. This lack of awareness is ideal for Beijing, Moscow, and Tehran — predators like nothing better than hunting slumbering prey.

Americans may not realize they are already in an information war because adversaries attempt to conceal their activities. To make matters worse, Americans often think of international conflict consciously or subconsciously in the context of kinetic war — soldiers, ships, and aircraft battling one another on land, at sea, or in the air. So, when there is no overt conflict, Americans can be lulled into a false sense of security.

This propensity works to the advantage of China, Russia, and Iran, which view conflict with the United States more like a dial than a two-way switch.[1] These adversaries turn the dial's intensity up or down as needed, but hostile intentions toward the United States

1. This is related to the concept of the "gray zone" between peace and war where America's adversaries are active and the United States is often absent or inept.

and attacks in the information domain remain constant regardless of whether a 'shooting war' is underway.

So, what exactly does this information warfare look like?

In the United States, China pushes messages via a variety of means that seek to undermine Americans' trust in their leaders, their government, and each other. Simultaneously, Beijing is attempting to manipulate U.S. public opinion regarding Hong Kong, Taiwan, Tibet, and Xinjiang.[2] The Chinese Communist Party hopes these measures weaken and divide Americans and remove any U.S. obstacles to Beijing's control and oppression at home and "might makes right" foreign policy abroad.

Russia proliferates messages designed to exploit hot-button domestic issues, stoke division among Americans,[3] and undermine support for Ukraine.[4] In its Annual Threat Assessment, the U.S. Intelligence Community (IC) warned that Russia would attempt to use "influence operations" to affect the upcoming U.S. elections this year "in ways that best support [Moscow's] interests and goals."[5] In Africa, Russia partners with authoritarian regimes, providing them information warfare support.[6]

The Islamic Republic of Iran, for its part, uses information warfare to oppress the Iranian people,

Americans vote at a polling place on November 8, 2022, in Madison, Wisconsin. (Photo by Jim Vondruska/Getty Images)

threaten dissidents, magnify anti-American voices, manipulate Western opinions, threaten Israel, and enfeeble U.S. foreign policy.

Meanwhile, elsewhere in Asia, as well as in Africa and Latin America, Beijing and Moscow propagate stories of Western colonialism, decline, and unreliability to diminish American influence and competitiveness and enable Sino-Russian neo-imperialism and neo-colonialism.[7] The essential hallmarks of this strategy, which Chinese and Russian information warfare supports, are the abuse of local populations, seizure of resources, exploitation of the environment, imposition of debt traps, and procurement of ports ultimately for military purposes.[8]

2. U.S. Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," February 5, 2024. (https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf)
3. Mark Hosenball, "Russia stocking U.S. racial, social differences ahead of election: sources," *Reuters,* March 10, 2020. (https://www.reuters.com/article/us-usa-election-security/russia-stoking-u-s-racial-social-differences-ahead-of-election-sources-idUSKBN20X2O3); Bradley Bowman and Shane Praiswater, "Great Power Competition Comes Home to America," *Defense One*, November 3, 2020. (https://www.defenseone.com/ideas/2020/11/great-power-competition-comes-home-america/169760)
4. Julian E. Barnes and David E. Sanger, "Russia Amps Up Online Campaign Against Ukraine Before U.S. Elections," *The New York Times,* March 27, 2024. (https://www.nytimes.com/2024/03/27/us/politics/russian-ukraine-us-interference.html)
5. Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," February 5, 2024, page 12. (https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf)
6. Elizabeth Dwoskin, "How Russian disinformation toppled government after government in Africa," *The Washington Post,* October 30, 2023. (https://www.washingtonpost.com/technology/2023/10/21/percepto-africa-france-russia-disinformation)
7. U.S. Department of State, Office of the Spokesperson, "The Kremlin's Efforts to Spread Deadly Disinformation in Africa," February 12, 2024. (https://www.state.gov/the-kremlins-efforts-to-spread-deadly-disinformation-in-africa)
8. Craig Singleton, "China's Military Is Going Global," *The New York Times,* September 7, 2023. (https://www.nytimes.com/2023/09/07/opinion/china-military-strategy-global.html); "Latin America's China Challenge: A Conversation with SOUTHCOM Commander General Laura Richardson," *Foundation for Defense of Democracies,* October 11, 2023. (https://www.fdd.org/events/2023/10/11/latin-americas-china-challenge-a-conversation-with-southcom-commander-general-laura-richardson)

Despite these concerning dynamics, some might be tempted to dismiss information warfare as a harmless sideshow. But this misguided view plays into the hands of U.S. adversaries. "Foreign information manipulation and interference is a national security threat to the United States as well as to its allies and partners," asserts a 2024 Framework to Counter Foreign State Information Manipulation endorsed by the United States, the United Kingdom, and Canada.[9]

An enduring obstacle to understanding information warfare is the lack of consensus about what the phrase actually means.[10] Some definitions are too broad to be useful, and some have the opposite problem.

Department of Defense *Joint Publication 3-04, Information in Joint Operations* describes the information environment as "the aggregate of social, cultural, linguistic, psychological, technical, and physical factors that affect how humans and automated systems derive meaning from, act upon, and are impacted by information, including the individuals, organizations, and systems that collect, process, disseminate, or use information."[11] While that definition underscores the complexity of the information landscape, its breadth is so great that it may not aid comprehension or planning.

"The term "information warfare" refers to the messages — and means to convey those messages — that nation-states use to advance political, economic, and security objectives and to strengthen the government's foundations of power, reinforce those of allies and partners, and undermine those of adversaries."

Others sometimes conceptualize information warfare too narrowly, focusing only on the role of information as part of military operations,[12] with an emphasis on cyber security.[13] To be sure, combatants must protect their data and command-and-control systems while attacking the data and systems of the adversary.[14]

9. U.S Department of State, "The Framework to Counter Foreign State Information Manipulation," January 18, 2024. (https://www.state.gov/the-framework-to-counter-foreign-state-information-manipulation); U.S. Department of State, "Joint Statement from the United States, United Kingdom, and Canada on Countering Foreign Information Manipulation," February 16, 2024. (https://www.state.gov/joint-statement-from-the-united-states-united-kingdom-and-canada-on-countering-foreign-information-manipulation)

10. Questions regarding the definition of information warfare are not new. See: William E. Rohde, "What is Info Warfare?" *U.S. Naval Institute*, February 1996. (https://www.usni.org/magazines/proceedings/1996/february/what-info-warfare)

11. U.S. Joint Chiefs of Staff, "Joint Publication 3-04: Information in Joint Operations," September 14, 2022. (https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series)

12. U.S. Joint Chiefs of Staff, "Joint Publication 3-13: Information Operations," November 27, 2012. (https://irp.fas.org/doddir/dod/jp3_13.pdf). Information operations is defined in Joint Publication 3-13 as "The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own." This definition is too narrow for the purposes of this monograph. The concept of information warfare employed in this monograph transcends military operations and is more of a whole-of-government endeavor. Moreover, the joint publication also focuses on decision-making only rather than the broader objectives being pursued by the government. Outside of military operations, information warfare can refer to the denial and/or manipulation of information, often referred to as disinformation or propaganda. This is part of the reason why this monograph uses the term "information warfare" instead of the term "information operations."

13. U.S. Joint Chiefs of Staff, "Joint Publication 3-13: Information Operations," November 27, 2012. (https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/12102012_io1.pdf)

14. NATO has put forward a definition broadly aligned with this way of thinking. See: NATO, Defense Education Enhancement Programme, "Media – (Dis)Information – Security," accessed May 29, 2024. (https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf)

But that definition is too narrow for the purposes of this monograph.[15]

Warfare is the preserve of the Department of Defense, but much of the information war being waged against Americans occurs beyond the Pentagon's reach.[16] Accordingly, an American approach to information warfare that relies excessively on the Pentagon to respond will not be effective.

This monograph endeavors to take a grand strategic approach to the concept that transcends the military, encompassing the major tools of national power. Accordingly, for the purposes of this monograph, the term "information warfare" refers to *the messages — and means to convey those messages — that nation-states use to advance political, economic, and security objectives and to strengthen the government's foundations of power, reinforce those of allies and partners, and undermine those of adversaries.*[17]

Consistent with that definition, each chapter in this monograph begins by assessing the adversary's approach to information warfare. That includes the adversary's objectives, the core messages it seeks to convey, and how it disseminates those messages. Each chapter then assesses the U.S. government's response to the adversary's campaign and offers specific and actionable recommendations to better defend and advance American interests.

In the chapter on China, **FDD Senior Fellow and Director of its China Program Craig Singleton** notes that "Washington has awoken to the threat posed by China's growing military might and predatory, non-market practices." He warns, however, that "far less attention, and even fewer resources, have been devoted to neutralizing nefarious Chinese narrative-shaping efforts." Singleton assesses that "Chinese Communist Party (CCP) General Secretary Xi Jinping is attempting to transform China into a discourse superpower to advance its hegemonic ambitions."

While the people of China are the "principal target" of the CCP's information warfare campaign, Singleton warns that "the United States is a major focus." Specifically, the CCP spends billions annually to produce, broadcast, and amplify propaganda and other disinformation globally with the goal of "undermining faith in public institutions, introducing conflicting social narratives, and radicalizing groups within a population." Many of those efforts are focused on the United States. Indeed, the IC warned this year that "the PRC aims to sow doubts about U.S. leadership, undermine democracy, and extend Beijing's influence," among other goals.[18]

To strengthen its information warfare efforts, the IC assesses that People's Republic of China (PRC) actors have "increased their capabilities to conduct covert influence operations and disseminate disinformation."

---

15. *Army Doctrine Publication 3-13: Information* defines information warfare as "a threat's orchestrated use of information activities (such as cyberspace operations, electromagnetic warfare, psychological warfare, and influence operations) to achieve objectives from the strategic to the tactical levels of warfare." That definition is helpful in that it delineates some of the components of information warfare and explicitly notes that it can be waged at different levels, but the definition lacks some other key elements and largely neglects the non-military elements of the enterprise. It is also noteworthy that the Army's definition only has room for the adversary and does not contemplate the United States engaging in information warfare. See: U.S. Army, Headquarters, Department of the Army, "Army Doctrine Publication 3-13: Information," November 27, 2023. (https://irp.fas.org/doddir/army/adp3-13.pdf)

16. The Department of Defense's *Strategy for Operations in the Information Environment* published in July 2023 notes in passing, "All military operations and activities affect the information environment." That is certainly true, but a one-dimensional, military-dominated approach to information warfare will miss many vital informational battles not involving military forces and will fail to effectively employ, coordinate, and synchronize the various tools of national power. U.S. Department of Defense, "Strategy for Operations in the Information Environment," July 5, 2023. (https://media.defense.gov/2023/Nov/17/2003342901/-1/-1/1/2023-DEPARTMENT-OF-DEFENSE-STRATEGY-FOR-OPERATIONS-IN-THE-INFORMATION-ENVIRONMENT.PDF)

17. A more complete definition of information warfare would not focus exclusively on nation states alone and would include non-state actors such as Hamas and Hezbollah. But the focus for this monograph is three nation states: China, Russia, and Iran.

18. U.S. Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," February 5, 2024, page 12. (https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf)

That includes efforts "demonstrating a higher degree of sophistication in its influence activity, including experimenting with generative AI."[19]

Meanwhile, Beijing is pursuing the "great rejuvenation of the Chinese nation" by 2049.[20] As part of this effort, Beijing is undertaking the world's largest military armament and modernization campaign since World War II.[21] Those efforts are focused on building the capabilities to defeat the U.S. military in East Asia, if necessary.[22] But it is safe to assume that the CCP would rather accomplish its objectives in Taiwan at the lowest cost possible, including without (or with less) military conflict.

The CCP likely believes its information warfare campaign offers a potential means to accomplish its objective of subduing Taiwan without war with the United States.[23] The IC assessed in February that "Beijing is intensifying efforts to mold U.S. public discourse," including on issues such as Taiwan.[24]

If the CCP can encourage isolationist tendencies among Americans, persuade them the United States has no real interests worth fighting for in Asia, and motivate them to oppose the use of military force to defend core American interests, then the CCP could sideline the U.S. military without firing a single shot.

If the CCP fails to accomplish its objectives in Taiwan via non-kinetic means and decides to engage in armed aggression, CCP information warfare tools could be used to erode popular and political American support for a U.S. military intervention to help Taiwan.[25]

As it has before, the PRC could use social media platforms such as TikTok to influence American politics. The IC noted earlier this year that "TikTok accounts run by a PRC propaganda arm reportedly targeted candidates from both political parties during the U.S. midterm election cycle in 2022."[26]

"If the CCP can sow discord and self-doubt among Americans — weakening, dividing, and distracting them — that can undermine U.S. influence and power, and further erode Washington's ability to defend core U.S. interests."

More broadly, if the CCP can sow discord and self-doubt among Americans — weakening, dividing, and distracting them — that can undermine U.S. influence and power, and further erode Washington's ability to defend core U.S. interests. That, in turn, could facilitate Beijing's efforts to coerce its neighbors and

19. U.S. Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," February 5, 2024. (https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf)
20. Craig Singleton, "China's Military Aims," *Defending Forward,* Ed. Bradley Bowman, December 2020. (https://www.fdd.org/wp-content/uploads/2020/12/fdd-monograph-defending-forward.pdf)
21. John C. Aquilino, "Statement of Admiral John C. Aquilino, U.S. Nacy Commander, U.S. Indo-Pacific Command, U.S. Indo-Pacific Command Posture," Testimony before the House Armed Services Committee, March 18, 2024. (https://armedservices.house.gov/sites/republicans.armedservices.house.gov/files/INDOPACOM%20Posture%20Testimony%20ADM%20Aquilino%20HASC.pdf)
22. U.S. Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," February 5, 2024, page 10. (https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf).
23. The general concepts undergirding the CCP's approach are hardly new, particularly in China. "For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill," Sun Tzu, the Chinese general and strategist, wrote more than 2,000 years ago. Sun Tzu, *The Art of War,* Trans. Samuel B. Griffith (New York: Oxford University Press, 1963), page 77.
24. U.S. Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," February 5, 2024, page 10. (https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf)
25. Sean Lyngaas, "TikTok could be a valuable tool for China if it invades Taiwan, FBI director says," *CNN,* March 8, 2023. (https://www.cnn.com/2023/03/08/tech/tiktok-china-taiwan-fbi/index.html); U.S. Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," February 5, 2024, page 11. (https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf)
26. Ibid.

refashion international norms and institutions in the CCP's authoritarian image.

Unfortunately, Singleton concludes, the United States "lacks a comprehensive strategy" to combat China's information warfare. However, this monograph provides policy recommendations that can begin to address the unacceptable status quo.

In the chapter on Russia, **FDD Research Fellow Ivana Stradner** and **Russia Program Deputy Director John Hardie** detail Moscow's approach to information warfare as well as the U.S. response and necessary reforms. The Kremlin's approach resembles Beijing's strategy in several ways. Both the Kremlin and the CCP focus first on maintaining power at home by controlling and manipulating the information available to domestic populations. And like the CCP, the Kremlin views its information warfare efforts "as central to its broader struggle with the United States." Beijing and Moscow both believe it serves their interests to stoke discord and disunity among Americans as well as distrust in American elections and institutions.[27]

The Kremlin's information warfare operations "draw on the Soviet 'active measures' playbook, updated for the 21st century," according to Stradner and Hardie. They discuss Moscow's concept of "reflexive control," which seeks to lure "an enemy to voluntarily make a desired decision." To explain this concept, Stradner and Hardie analyze Russia's "bad-faith diplomatic negotiations prior to its 2022 invasion of Ukraine." They also note that the "advent of social media has enabled information-psychological operations to achieve greater and more targeted reach," pointing to Moscow's efforts to influence U.S. elections.

Stradner and Hardie acknowledge that the U.S. government has taken several steps since 2016 "to protect the U.S. information space and counter Russian disinformation" but believe more action is needed to "take the fight to Moscow in the information domain." They identify two primary weaknesses in the U.S. government's current information warfare efforts related to Russia that require urgent attention from decision-makers. First, they argue America often is "failing to reach ordinary Russians." And even when Washington succeeds in reaching average Russians, the communications are often "clumsy and pedestrian." Second, despite some ongoing efforts,[28] the authors sound the alarm that Moscow seems to be outpacing Washington "in the battle for hearts and minds in the Global South."

Finally, **FDD Chief Executive Officer Mark Dubowitz** and **FDD Senior Iran Advisor Saeed Ghasseminejad** argue that "Washington needs to step up its game" when it comes to information warfare with the Islamic Republic of Iran. Initial drafts of the three country chapters in this monograph were completed before October 7, 2023, when Iran-backed Hamas carried out a mass slaughter in Israel, spurring a regional war that continues to this day. After that attack, FDD spent several months focusing on how the United States and Israel could better work together to confront the Islamic Republic of Iran and its proxies more effectively.

Since October, there has been an escalation in Iranian and Iranian-backed military attacks across the Middle East. From October 17 to February 4, Iran-backed terrorist groups and militias attacked U.S. military forces in Iraq, Syria, and Jordan approximately 165 times.[29] A January 28 attack on a base in Jordan resulted in the deaths of three U.S. servicemembers and more

27. Bradley Bowman and Shane Praiswater, "Great Power Competition Comes Home to America," *Defense One*, November 3, 2020. (https://www.defenseone.com/ideas/2020/11/great-power-competition-comes-home-america/169760)
28. U.S. Department of State, Office of the Spokesperson, "The Kremlin's Efforts to Spread Deadly Disinformation in Africa," February 12, 2024. (https://www.state.gov/the-kremlins-efforts-to-spread-deadly-disinformation-in-africa)
29. Mike Daum and Bradley Bowman, "American Forces Under Attack by Iran and its Proxies," *Foundation for Defense of Democracies*, April 22, 2024. (https://www.fdd.org/iranattacksusforces)

than 40 injured.[30] Meanwhile, since November 2023, the Houthis in Yemen, who are armed, trained, and funded by Iran, have assaulted international shipping and freedom of navigation in and near the Red Sea.[31] And on April 13-14, the Islamic Republic of Iran conducted its first direct military attack on Israel from Iranian soil, launching more than 300 missiles and drones at the Jewish state.[32]

With all this military activity, some may overlook the information domain. "The regime's information warfare strategy seeks to secure the regime's survival by discrediting its domestic and foreign enemies, pacifying the Iranian people, strengthening the loyalty of followers, and recruiting new supporters," Dubowitz and Ghasseminejad write. "Tehran also seeks to use information warfare to influence and confuse foreign decision-makers and create chaos in target countries such as the United States, United Kingdom, Germany, Canada, Iraq, and Lebanon." Unfortunately, as with Beijing's and Moscow's information warfare campaigns, the authors conclude that "the U.S. government has thus far failed to fully grasp the scope of the Islamic Republic's information warfare activities, much less develop a unified and executable strategy that effectively counters Iran's global campaign."

Given the stakes in this war of ideas and beliefs with China, Russia, and Iran, an exhaustive multidisciplinary study of information warfare is needed. But the goals for this monograph are more modest. *Cognitive Combat: China, Russia, and Iran's Information War Against Americans* simply seeks to achieve four objectives: 1) sound the alarm for Americans that the three adversaries are waging information war against Americans whether they realize it or not; 2) survey the broad outlines of this war; 3) propose initial steps that can help the United States better defend itself in the information domain and begin to go on the offensive; and 4) serve as a foundation for additional research.

If Americans awaken to the information war that China, Russia, and Iran are waging, the United States can take concerted action and prevail. If Americans continue to slumber, the consequences could be dire.

30. Phil Stewart, Steve Holland, and Idrees Ali, "Three US Troops Killed in Jordan Drone Strike Linked to Iran," *Reuters*, January 29, 2024. (https://www.reuters.com/world/biden-says-three-us-service-members-killed-drone-attack-us-forces-jordan-2024-01-28)

31. Jonathan Lehrfeld, Diana Stacey, and Geoff Ziezulewicz, "All the Houthi-US Navy incidents in the Middle East (that we know of)," *Military Times*, February 12, 2024. (https://www.militarytimes.com/news/your-military/2024/02/12/all-the-houthi-us-navy-incidents-in-the-middle-east-that-we-know-of)

32. "Iran Launched More than 300 Drones and Missiles at Israel; Biden Condemns Attack," *The Washington Post*, April 13, 2024. (https://www.washingtonpost.com/world/2024/04/13/iran-israel-hamas-war-news-gaza-palestine)

China

By Craig Singleton

Introduction

Chinese Communist Party (CCP) General Secretary Xi Jinping is attempting to transform China into a discourse superpower to advance its hegemonic ambitions. Distinct from soft power, "discourse power" (话语权) seeks to set and shape global narratives to bolster China's composite national strength and international influence.[33] In countering ideas perceived as threatening to China's interests and legitimizing the CCP's policies, discourse power advances Xi's goal of fostering an international order that reflects Beijing's values and interests. To achieve discourse victory, Xi has restructured China's party-state to support the "integrated employment," across peacetime and wartime, of public opinion, legal, and psychological

33. "网传习近平8•19讲话全文：言论方面要敢抓敢管敢于亮剑 [The full text of Xi Jinping's speech on August 19 was circulated online: Dare to catch, dare to regulate, and dare to show the sword when it comes to speech]," *China Digital Times*, November 4, 2013. (https://chinadigitaltimes.net/chinese/321001.html)

warfare (三种战法).[34] While the principal target of these efforts is the Chinese people, the United States is a major focus of China's international cognitive warfare.

Washington has awoken to the threat posed by China's growing military might and predatory, non-market practices. However, far less attention, and even fewer resources, have been devoted to neutralizing nefarious Chinese narrative-shaping efforts aimed at influencing the perceptions and actions of key actors, both foreign and domestic, to undercut American interests. A concerted policy response is required to reverse this troubling trend.

China's Approach to Information Warfare

Chinese leaders believe the United States' success in exerting and maintaining international influence hinges on its capacity to shape global governance narratives, values, and norms. China's so-called "discourse power" thus consists of two mutually reinforcing elements. The first relates to the content of Beijing's cognitive warfare and involves the "right to speak," or the ability to "tell China's story well" (讲好中国故事) by championing CCP accomplishments, real or imagined.[35] The second relates to the means of making "China's voice heard" by constructing a "discourse system for external communication" (构建对外传播话语体系) to propagate CCP messaging.[36]

On a basic level, Beijing's discourse strategy seeks to alter global perceptions about Chinese autocracy and Western democracy, namely by comparing, contrasting, and consistently misrepresenting these competing visions in ways that are advantageous to China. In its most extreme form, called "cognitive domain warfare" (认知域作战) by China's People's Liberation Army, the CCP uses discourse power to influence individual and/or group behaviors to favor Beijing's tactical or strategic objectives.[37] This can be achieved by sowing social division, undermining faith in public institutions, introducing conflicting social narratives, and radicalizing groups within a population.

Discourse power reinforces the CCP's credibility while neutralizing criticism of its malign behavior. For instance, following reports regarding Beijing's persecution of Uyghurs in Xinjiang, Beijing pushed positive news stories about Xinjiang's culture and the CCP's economic stewardship over the region.[38] Beijing similarly leveraged state-backed and social media, including X, to undermine claims about Uyghur

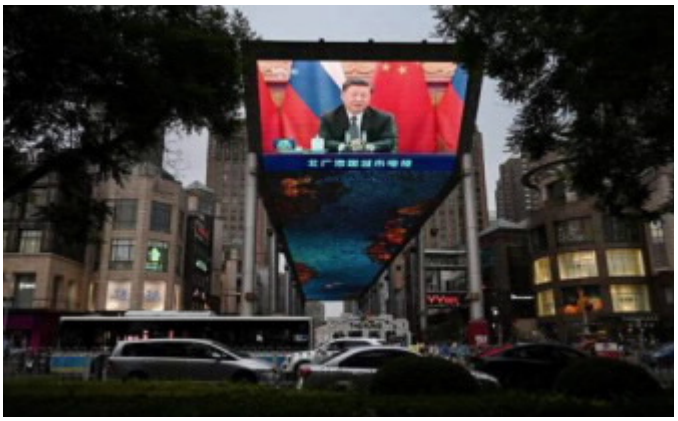
34. "In Their Own Words: Foreign Military Thought," *China Aerospace Studies Institute*, February 8, 2021. (https://www.airuniversity.af.edu/CASI/Display/Article/2485204/plas-science-of-military-strategy-2013); Mark Stokes, "The People's Liberation Army General Political Department: Political Warfare with Chinese Characteristics," *Project 2049 Institute*, October 14, 2013. (https://project2049.net/2013/10/14/the-peoples-liberation-army-general-political-department-political-warfare-with-chinese-characteristics)

35. Wen-Hsuan Tsai, "Enabling China's Voice to Be Heard by the World: Ideas and Operations of the Chinese Communist Party's External Propaganda System," *Problems of Post-Communism*, October 24, 2016, pages 203-213. (https://www.tandfonline.com/doi/abs/10.1080/10758216.2016.1236667)

36. "习近平在中共中央政治局第三十次集体学习时强调 加强和改进国际传播工作 展示真实立体全面的中国 [During the 30th collective study session of the Political Bureau of the CPC Central Committee, Xi Jinping emphasized strengthening and improving international communication work to present a true, three-dimensional and comprehensive China]," *Xinhua News Agency* (China), June 1, 2021. (http://www.xinhuanet.com/politics/2021-06/01/c_1127517461.htm)

37. Wu Jiaxi, "混合战争视野下的认知域作战 [Cognitive Domain Operations From the Perspective of Hybrid Warfare]," *People's Liberation Army Daily* (China), June 7, 2022. (http://www.81.cn/jfjbmap/content/2022-06/07/content_317171.htm)

38. James Griffiths, "From cover-up to propaganda blitz: China's attempts to control the narrative on Xinjiang," *CNN* April 17, 2021. (https://www.cnn.com/2021/04/16/china/beijing-xinjiang-uyghurs-propaganda-intl-hnk-dst/index.html); John Power, "Foreign influencers used to whitewash Xinjiang abuses: Report," *Al-Jazeera* (Qatar), December 15, 2021. (https://www.aljazeera.com/economy/2021/12/15/foreign-influencers-used-to-whitewash-xinjiang-abuses-report); Newley Purnell, "Facebook Staff Fret Over China's Ads Portraying Happy Muslims in Xinjiang," *The Wall Street Journal*, April 2, 2021. (https://www.wsj.com/articles/facebook-staff-fret-over-chinas-ads-portraying-happy-muslims-in-xinjiang-11617366096); "Inside a Chinese Propaganda Campaign," *The New York Times*, June 22, 2021. (https://www.nytimes.com/interactive/2021/06/22/technology/xinjiang-uyghurs-china-propaganda.html)



A large screen shows a news report about Chinese President Xi Jinping, outside a shopping mall in Beijing on May 19, 2021. (Photo by Greg Baker/AFP via Getty Images)

"concentration camps," referring to them as mere "vocational education training centers."[39]

Discourse power likewise aims to undercut America's reputation as a responsible global stakeholder, namely by touting authoritarianism's ostensible benefits and democracy's perceived dysfunction. For example, Beijing consistently framed Washington's pandemic response as "chaotic," while claiming mass lockdowns enabled China to achieve "strategic victory" over COVID-19.[40]

Consistent with Xi's Marxist-Leninist outlook, discourse power also aims to propagate new terminology and redefine existing vocabulary in ways that have a normative impact. The CCP has, for instance, speciously claimed that China's authoritarian one-party system represents a "whole-process people's democracy," thus implying the CCP represents the Chinese people's will.[41]

China spends billions annually to support its discourse ecosystem, one primarily overseen by the CCP's powerful Central Committee via its Propaganda and United Front Work departments.[42] These entities control China's publishing, film, and news media organizations, such as *People's Daily*, *The Global Times*, *Xinhua, and* China Global Television Network (CGTN). These outlets also produce paid content disseminated by other international media platforms

39. Adrian Zenz, "Brainwashing, Police Guards and Coercive Internment: Evidence from Chinese Government Documents about the Nature and Extent of Xinjiang's 'Vocational Training Internment Camps,'" *The Journal of Political Risk*, July 1, 2019. (https://www.uyghurcongress.org/en/38522-2); "Report: Fake Twitter accounts spread Chinese propaganda," *Associated Press*, April 25, 2022. (https://apnews.com/article/technology-business-china-beijing-race-and-ethnicity-14fec4421be0291e5f0ea580ecbd4b6d); Sigal Samuel, "China paid Facebook and Twitter to help spread anti-Muslim propaganda," *Vox*, August 22, 2019. (https://www.vox.com/future-perfect/2019/8/22/20826971/facebook-twitter-china-misinformation-ughiur-muslim-internment-camps)

40. "The State of Democracy in the United States," *Ministry of Foreign Affairs of the People's Republic of China*, December 5, 2021. (https://www.mfa.gov.cn/mfa_eng/zxxx_662805/202112/t20211205_10462535.html); "China achieves major, decisive victory in COVID response: CPC leadership," *Xinhua News Agency* (China), February 17, 2023. (http://english.scio.gov.cn/m/topnews/2023-02/17/content_85111534.htm); Jesusemen Oni, Adrianna Zhang, Milan Nesic, and Jonathan Muriithi, "How China Used Foreign Media to Reset Image During Pandemic," *Voice of America*, May 13, 2021. (https://www.voanews.com/a/east-asia-pacific_how-china-used-foreign-media-reset-image-during-pandemic/6205763.html). Beijing broadcasted these themes abroad, leading to a marked improvement in foreign perceptions about China's governance model.

41. Wang Xining, "Whole-process People's Democracy Is A High Quality Democracy," *Ministry of Foreign Affairs of the People's Republic of China*, December 11, 2021. (https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zwjg_665342/zwbd_665378/202112/t20211213_10467431.html#:~:text=Whole%2Dprocess%20people's%20democracy%20includes,making%2C%20management%2C%20and%20oversight); "Full text: China: Democracy That Works," *Embassy of the People's Republic of China in the United States of America*, December 4, 2021. (http://us.china-embassy.gov.cn/eng/zgyw/202112/t20211204_10462468.htm); Nectar Gan and Steve George, "China claims its authoritarian one-party system is a democracy – and one that works better than the US," *CNN*, December 8, 2021. (https://www.cnn.com/2021/12/08/china/china-us-democracy-summit-mic-intl-hnk/index.html)

42. "Beijing's Global Media Influence 2022," *Freedom House*, accessed May 22, 2024. (https://freedomhouse.org/report/beijing-global-media-influence/2022/authoritarian-expansion-power-democratic-resilience); "Beijing in 45b yuan global media drive," *South China Morning Post* (China), January 13, 2009. (https://www.scmp.com/article/666847/beijing-45b-yuan-global-media-drive); David Shambaugh, "China's Soft-Power Push," *Foreign Affairs*, June 16, 2015. (https://www.foreignaffairs.com/articles/china/2015-06-16/chinas-soft-power-push)

via reciprocal news-exchange agreements.[43] Such stories are often not identified as being authored by Beijing-backed sources.

The CCP has tasked these party organs with cultivating a "circle of international media influencers" to validate and amplify CCP narratives. These include, according to the CCP's Central Propaganda Department, "foreign politicians, parliamentary political parties, business elites, celebrities from all walks of life, and non-governmental organizations."[44] Other influencer targets include academics, industry associations, and think tanks.[45]

Besides generating traditional media abroad, the CCP also focuses on occupying emerging public opinion spaces, such as the internet and social media platforms, to influence global sentiments as well as to track and silence critics abroad. TikTok, owned by the Chinese company ByteDance, exemplifies China's strategic utilization of digital spaces to mold international perceptions and extend its discourse power.[46] By curating and promoting content that aligns with CCP narratives, TikTok has become a pivotal instrument in Beijing's efforts to shape global opinion and suppress dissenting voices.

China also maintains a 20 million-strong army of Chinese netizens, known as "network civilization volunteers," to support its digital disinformation efforts. These individuals wage the CCP's "online ideological struggle" (落实网络意识形态斗争) by amplifying online voices complimentary of China and suppressing those deemed "negative."[47]

The U.S. Response

The United States lacks a comprehensive strategy to combat China's cognitive warfare. The State Department's Global Engagement Center (GEC) leads Washington's efforts to expose and counter Chinese and other foreign state propaganda and disinformation

43. Chinese state-controlled outlets, such as Xinhua, have maintained paid content business relationships with outlets like Microsoft News (MSN), Reuters, and the British Broadcasting Channel (BBC). In other cases, Chinese state media, embassies, and China-based companies also sometimes pay media outlets or journalists to publish Chinese-approved content to promote Chinese state narratives. "Beijing's Global Media Influence 2022," *Freedom House*, accessed May 22, 2024. (https://freedomhouse.org/report/beijing-global-media-influence/2022/authoritarian-expansion-power-democratic-resilience#footnote3_12fce9a); John Dotson, "Xinhua Infiltrates Western Electronic Media, Part 2: Relationships with News Agencies and Distribution Services," *The Jamestown Foundation*, August 17, 2021. (https://jamestown.org/program/xinhua-infiltrates-western-electronic-media-part-2-relationships-with-news-agencies-and-distribution-services)

44. "《新时代宣传思想工作》第十章 对外宣传工作 'Propaganda and Ideological Work in the New Era' Chapter 10 External Propaganda Work]," *Central Party School Publishing*, April 6, 2021. (https://archive.ph/B8SIE)

45. "政党携手，共铸人类命运共同体 [Political Parties Join Hands to Build a Community with a Shared Future for Mankind], *Sohu*, February 13, 2018. (https://archive.ph/c00W0)

46. "5 Things to Know About ByteDance, TikTok's Parent Company," *Foundation for Defense of Democracies*, March 12, 2024. (https://www.fdd.org/analysis/2024/03/12/5-things-to-know-about-bytedance-tiktoks-parent-company)

47. The Chinese government, for instance, organizes "public opinion actual combat drills" (舆情实战演练; *yuqing shijian yanlian*), which simulate public relations crises and train netizens in online public opinion management, press relations, and "credibility restoration." "中国共产主义青年团湖州市委员会2019年部门预算一上申报情况 [The Huzhou Municipal Committee of the Communist Youth League of China's 2019 Department Budget First Declaration]," *Huzhou Municipal Committee of the Communist Youth League*, November 23, 2018. (https://perma.cc/5AP3-D8E8); "检察新闻官'论剑' [Prosecutor's Press Officer 'Discussing Swords']," *China Youth Network News* (China), July 26, 2015. (https://perma.cc/G4N4-VNCC); "网络舆论引导培训 [Online public opinion guidance training]," *People's Daily Online* (China), May 19, 2017. (https://perma.cc/L57M-9QPV); Ryan Fedasiuk, "A Different Kind of Army: The Militarization of China's Internet Trolls," *The Jamestown Foundation*, April 12, 2021. (https://jamestown.org/program/a-different-kind-of-army-the-militarization-of-chinas-internet-trolls); "团中央办公厅关于建立高校共青团网络宣传员队伍的通知 [Notice from the General Office of the Youth League Central Committee on the establishment of a team of online propagandists for the Communist Youth League of Colleges and Universities]," *China Digital Times* (China), January 19, 2015. (https://chinadigitaltimes.net/chinese/378737.html); "中国共产党、中国共产主义青年团简史纲要 [A Brief History of the Communist Party of China and the Communist Youth League of China]," *Communist Youth League Jiangxi Provincial*, April 16, 2019. (https://web.archive.org/web/20201205202348/https://tw.jxcfs.com/_mediafile/tw/files/20190416120254543.pdf)

aimed at influencing the policies, security, and stability of the United States, its allies, and its partners.[48] Of the GEC's fiscal year (FY) 2021 $60 million budget, only $11.3 million was dedicated to countering China's $10 billion discourse apparatus.[49] GEC's funding decreased in FYs 2022 and 2023 to $10.6 million and $9.9 million, respectively, even as China ramped up its disinformation activities.[50]

A 2022 State Department Inspector General (IG) report uncovered several still-unresolved operational, budgetary, and personnel challenges facing the center.[51] GEC, for instance, lacks an evaluation coordinator with decision-making authority to monitor its effectiveness. Furthermore, the IG recommended a complete operational assessment to align GEC's structure with its operational needs and changes to its grant-funding process to ensure GEC's budget could be better utilized.

The private sector is equally lacking. Social media platforms' attempts to label accounts belonging to the Chinese government or Chinese state-backed media have also proven woefully inadequate, even when those accounts are overtly state-affiliated.[52] For instance, in 2023, X removed its "Chinese state-affiliated media" label from the accounts of *Xinhua* and other Chinese journalists associated with other Chinese government-backed publications.[53]

Nonetheless, some progress has been made. In 2018, for example, the U.S. Department of Justice ordered *Xinhua* and *CGTN* to register under the Foreign Agents Registration Act (FARA).[54] Today, both outlets must publicly reveal information about their U.S.-based staffing, operations, and budgets.

Recommendations

A whole-of-American-society counter-offensive is necessary to combat China's cognitive warfare strategy. To be successful, this approach should include hardening America's democratic defenses; exposing China's malign activities and countering them when appropriate; and penetrating China's domestic information environment to undermine false narratives about the CCP's legitimacy.

Recommendations include:

- **Strengthen statutory framework.** Congress should modernize campaign finance, counter-interference, and espionage laws to enhance transparency and

48. U.S. Department of State, "About Us – Global Engagement Center," accessed May 22, 2024. (https://www.state.gov/about-us-global-engagement-center-2)
49. U.S. Department of State, "Congressional Budget Justification: Appendix 1: Department of State Diplomatic Engagement," 2022. (https://www.usaid.gov/sites/default/files/2022-10/FY-2023-CBJ-Appendix-1-Full-Document-Final.pdf)
50. U.S. Department of State, "Congressional Budget Justification: Appendix 1: Department of State Diplomatic Engagement," 2022. (https://www.usaid.gov/sites/default/files/2022-10/FY-2023-CBJ-Appendix-1-Full-Document-Final.pdf); U.S. Department of State, Advisory Commission on Public Diplomacy, "Comprehensive Annual Report on Public Diplomacy & International Broadcasting," March 2021. (https://www.state.gov/wp-content/uploads/2022/03/2021-ACPD-Annual-Report-508-WEB.pdf)
51. U.S. Department of State, Office of Inspector General, "Inspection of the Global Engagement Center," September 2022. (https://www.stateoig.gov/report/isp-i-22-15)
52. "Twitter drops 'government-funded' label on media accounts, including in China," *Reuters*, April 21, 2023. (https://www.reuters.com/technology/twitter-removes-state-affiliated-media-tags-some-accounts-2023-04-21); Erika Kinetz, "Army of fake fans boosts China's messaging on Twitter," *Associated Press*, May 28, 2021. (https://apnews.com/article/asia-pacific-china-europe-middle-east-government-and-politics-62b13895aa6665ae4d887dcc8d196dfc); Marcel Schliebs, Hannah Bailey, Jonathan Bright, and Philip N. Howard, "China's Inauthentic UK Twitter Diplomacy," *Oxford Internet Institute*, May 11, 2021. (https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/05/Chinas-Inauthentic-UK-Twitter-Diplomacy-Dem.Tech-Working-Paper-2021.2-2.pdf)
53. "Twitter drops 'government-funded' label on media accounts, including in China," *Reuters*, April 21, 2023. (https://www.reuters.com/technology/twitter-removes-state-affiliated-media-tags-some-accounts-2023-04-21)
54. Kate O'Keeffe and Aruna Viswanatha, "Justice Department Has Ordered Key Chinese State Media Firms to Register as Foreign Agents," *The Wall Street Journal*, September 18, 2018. (https://www.wsj.com/articles/justice-department-has-ordered-key-chinese-state-media-firms-to-register-as-foreign-agents-1537296756)

disclosure requirements for individuals/entities acting on Beijing's behalf. [55] This should include toughening existing sanctions and enforcement provisions to deter violators from interfering in the U.S. political system. FARA should be updated and revised to include mandated retroactive disclosure requirements for all individuals who have worked on China's behalf to influence our policymaking process. Building on the recent legislative actions requiring TikTok's divestiture, Congress should mandate a comprehensive risk assessment for all Chinese-owned applications operating in the United States.[56] This assessment must evaluate potential risks to national security and personal data privacy, aiming to identify other applications that may require similar regulations.

- **Increase cognitive warfare capacity**. As Beijing invests billions in strengthening its discourse power, Washington has failed to marshal the resources necessary to respond. Washington must significantly enhance its capacity to analyze, expose, and counter Chinese influence within its political and economic systems, to include potentially establishing a new U.S. government agency or department to marshal such work. For its part, GEC should expedite plans to replace its now-shuttered disinformation cloud website to identify new technologies to counter adversarial propaganda.[57] The GEC should be designated an official State Department bureau or bureau equivalent, and Congress should closely monitor the department's compliance with the 2022 IG report.
- **Increase language skills**. The United States needs more skilled professionals with Mandarin-language abilities to serve in U.S. departments and agencies responsible for identifying and countering Chinese disinformation and propaganda. Congress should require a report from the executive branch providing an update on personnel with Mandarin skills in relevant offices, an assessment of how many personnel with these skills are necessary in the respective offices, and an actionable plan to address any shortfalls. Congress should consider whether additional funding for language scholarships and other programs for U.S. citizens could help. Congress could ask the comptroller general to independently assess Mandarin language proficiency in the government and scrutinize the administration's response to the congressional reporting requirement.
- **Build domestic resiliency**. Congress should support the creation or expansion of public-private partnerships to enhance appropriate coordination in the civic technology space, including identifying and responding to China's discourse provocations in a manner consistent with First Amendment protections. Additional funding should be considered to pilot and deploy tools to blunt China's efforts to exert control over contested digital domains as well as to research the PLA and United Front's roles in supporting Chinese disinformation. To increase awareness, U.S. government leaders should call out false CCP narratives by frequently exposing them and providing credible U.S. perspectives.
- **Go on the offensive**. President Biden should direct the President's Intelligence Advisory Board to evaluate the potential risks and benefits associated with developing new intelligence authorities and capabilities to penetrate China's domestic information environment, with the goal of exposing and undermining false narratives about the CCP's legitimacy.

55. In the wake of several high-level counterintelligence investigations in 2018 and 2019, Australia undertook a similar initiative to reform its counter-interference and counter-espionage laws. "Australian Government legislation and codes," *Australian Government: Department of Education*, accessed May 24, 2024. (https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/templates-and-tools/australian-government-legislation-and-codes)

56. Craig Singleton, "It's not just a theory. TikTok's ties to Chinese government are dangerous." *USA Today*, March 18, 2024. (https://www.usatoday.com/story/opinion/2024/03/18/tiktok-sale-ban-chinese-government-us-security/72988111007)

57. "Defeat Disinfo," *U.S. Department of State*, accessed May 22, 2024. (https://www.state.gov/defeat-disinfo)

Russia

By Ivana Stradner and John Hardie

Introduction

As Russia's invasion of Ukraine continues, Moscow is also waging another war — in the information domain. The Kremlin views this so-called "information confrontation"[58] as central to its broader struggle with the United States. Moscow seeks to replace the U.S.-led international order with one more conducive to its imperialistic ambitions and authoritarian interests.

To prevail in this information confrontation, Washington will need to revamp its approach. To be sure, the United States has taken some important steps to protect its information space since Russia sought to meddle in the 2016 U.S. presidential election.[59] However, America and its allies are falling short on other important information battlefields, including in Russia itself and in the "Global South." To defeat

58. Lesley Kucharski, Mike Alberston, Marimar Calisto, and Brian Radzinsky, "Countering the 'Information Confrontation' Strategies of Russia and China," *Center for Global Security Research*, September 27-28, 2022. (https://cgsr.llnl.gov/content/assets/docs/CGSR-Disinformation-Workshop-Summary.pdf)

59. Federal Bureau of Investigation, "Russian Interference In 2016 U.S. Elections," accessed May 23, 2024. (https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections)

Moscow's information war, the United States cannot just play defense. Washington must also take the fight to the Kremlin within Russia and beyond.

Russia's Approach to Information Warfare

Moscow uses a broad definition of "information security," comprising "information-technical" (i.e., cyber and electronic warfare) and "information-psychological" components.[60] While the latter bears the closest resemblance to Western conceptions of "information warfare," these components are interrelated. Russia often uses technical means, including its formidable cyber capabilities, to facilitate information-psychological operations.

Moscow's aims in the information-psychological domain are two-fold: First, it strives to ensure regime security by controlling Russia's domestic information space and shielding it from perceived Western subversion.[61] Since Putin assumed office, the Kremlin has increasingly dominated Russia's information space.[62] Moscow uses technical means, intimidation, and legal persecution to silence undesirable voices[63] while promoting "patriotic" content and pursuing "digital sovereignty."[64] This clamp-down has accelerated following Russia's February 2022 invasion of Ukraine. In an attempt to legitimize and advance its information control, Moscow partners with like-minded regimes to promote authoritarian-friendly norms at the United Nations and other international fora.

Second, Russia seeks to use information-psychological operations to advance its influence and interests abroad. These operations draw on the Soviet "active measures" playbook, updated for the 21st century.[65] The advent of social media has enabled information-psychological operations to achieve greater and more targeted reach. Likewise, cyber operations can both sow discord through disruptive attacks and obtain embarrassing or divisive information for subsequent release. That said, Russia also still uses old-fashioned techniques such as creating media fronts;[66] funding

60. David Shedd and Ivana Stradner, "The Curious Omission in Russia's New Security Strategy," *Defense One*, August 25, 2021. (https://www.defenseone.com/ideas/2021/08/curious-omission-russias-new-security-strategy/184854)
61. Russian Federation Official Publication of Legal Acts, "О Стратегии национальной безопасности Российской Федерации [On the National Security Strategy of the Russian Federation]," July 2, 2021. (http://publication.pravo.gov.ru/Document/View/0001202107030001)
62. Ivana Stradner, "Russian hackers are sowing havoc. So why are we letting Moscow write the U.N.'s rules on cyberspace?" *The Washington Post*, July 13, 2021. (https://www.washingtonpost.com/opinions/2021/07/13/biden-letting-moscow-use-un-to-write-new-cyber-rules)
63. Andrei Soldatov and Irina Borogan, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries* (New York: PublicAffairs, 2015); Paul Mozur, Adam Satariano, Aaron Krolik, and Aliza Aufrichtig, "'They Are Watching': Inside Russia's Vast Surveillance State," *The New York Times*, September 22, 2022. (https://www.nytimes.com/interactive/2022/09/22/technology/russia-putin-surveillance-spying.html)
64. See, for example: Benoit Faucon, "Putin's Propaganda Chief Urges 'War Over People's Minds,'" *The Wall Street Journal*, December 10, 2022. (https://www.wsj.com/articles/putins-propaganda-chief-urges-war-over-peoples-minds-11670630966); Alena Epifanova, "Russia's Quest for Digital Sovereignty: Ambitions, Realities, and Its Place in the World," *German Council on Foreign Relations*, February 2022. (https://dgap.org/sites/default/files/article_pdfs/DGAP-Analyse-2022-01-EN_0.pdf); Sarah E. Needleman and Evan Gershkovich, "From YouTube to Rutube. Inside Russia's Influence Campaign." *The Wall Street Journal*, April 20, 2022. (https://www.wsj.com/articles/from-youtube-to-rutube-inside-russias-influence-campaign-11650447002)
65. The term "active measures," which originated during the Cold War, describes covert or deniable operations designed to subvert or otherwise influence foreign states. These operations range from spreading disinformation to conducting assassinations or orchestrating coups.
66. See, for example: Inga Springe and Sanita Jemberga, "Sputnik's Unknown Brother," *Re:Baltica*, April 6, 2017. (https://en.rebaltica.lv/2017/04/sputniks-unknown-brother); Bradley Hanlon and Thomas Morley, "Russia's Network of Millennial Media," *Alliance for Securing Democracy at the German Marshall Fund of the United States*, February 15, 2019. (https://securingdemocracy.gmfus.org/russias-network-of-millennial-media)

friendly journalists, officials, and political parties;[67] and orchestrating protests.[68]

Russia adapts its tactics as circumstances evolve. For example, whereas Moscow sought to influence the 2016 U.S. presidential election in part by releasing hacked information,[69] in 2020, Russia mainly laundered narratives through prominent Americans and U.S. media organizations.[70] When Western governments and companies cracked down on Russian propaganda outlets following Moscow's 2022 invasion of Ukraine, Russian diplomats stepped up to spread messages on social media.[71] Moscow has also adopted harder-to-detect disinformation techniques, such as creating fake versions of legitimate Western news sites.[72]

A key concept is *reflexive control*, defined in Soviet military literature as the process of conveying information that leads an enemy to voluntarily make a desired decision.[73] Russia's bad-faith diplomatic negotiations prior to its 2022 invasion of Ukraine provide an example. The Kremlin probably intended to distract the West from aggressively arming Ukraine and to create a pretext for Russia's eventual invasion once its maximalist demands were rejected. During the lead-up to the war, Paris and Berlin reportedly remained convinced that Russia was massing forces on Ukraine's borders merely to gain diplomatic leverage.[74] And the White House reportedly delayed military aid for Kyiv, hoping to buy time for a diplomatic resolution.[75]

Moscow describes the information domain as vital to modern warfare and seeks to integrate information-psychological (and information-technical) effects into its military operations.[76] Before and during its 2014 invasion of Ukraine, for example, Russia sought to use information-psychological operations to "soften the ground" and legitimize its actions domestically and

67. See, for example: Aubrey Belford, Saska Cvetkovska, Biljana Sekulovska, and Stevan Dojcinovic, "Leaked Documents Show Russian, Serbian Attempts to Meddle in Macedonia," *OCCRP*, June 4, 2017. (https://www.occrp.org/en/spooksandspin/leaked-documents-show-russian-serbian-attempts-to-meddle-in-macedonia); Pieter Haeck, "Belgium opens probe into pro-Russia network accused of paying MEPs," *Politico*, April 12, 2024. (https://www.politico.eu/article/belgiam-prosecutor-open-probe-pro-russia-network-accused-pay-mep)

68. See, for example: "Russian businessman funds opponents of Macedonia's name change," *Alliance for Securing Democracy at the German Marshall Fund of the United States*, accessed May 23, 2024. (https://securingdemocracy.gmfus.org/incident/russian-businessman-funds-opponents-of-macedonias-name-change); Polina Nikolskaya, Mari Saito, Maria Tsvetkova, and Anton Zverev, "Pro-Putin operatives in Germany work to turn Berlin against Ukraine," *Reuters*, January 3, 2023. (https://www.reuters.com/investigates/special-report/ukraine-crisis-germany-influencers)

69. U.S. Office of the Director of National Intelligence, "Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution," January 6, 2017. (https://www.dni.gov/files/documents/ICA_2017_01.pdf)

70. U.S. National Intelligence Council, "Foreign Threats to the 2020 US Federal Elections," March 10, 2021. (https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf)

71. David Klepper, "For Russian diplomats, disinformation is part of the job," *Associated Press*, April 19, 2022. (https://apnews.com/article/russia-ukraine-covid-technology-health-business-628cf047adf9fde93c0d7f820e46f8e4)

72. Julian E. Barnes and David E. Sanger, "Russia Amps Up Online Campaign Against Ukraine Before U.S. Elections," *The New York Times*, March 27, 2024. (https://www.nytimes.com/2024/03/27/us/politics/russian-ukraine-us-interference.html); U.S. Department of the Treasury, Press Release, "Treasury Sanctions Actors Supporting Kremlin-Directed Malign Influence Efforts," March 20, 2024. (https://home.treasury.gov/news/press-releases/jy2195)

73. Timothy Thomas, "Russia's 21st Century Information War: Working to Undermine And Destabilize Populations," *NATO Strategic Communications Centre of Excellence*, accessed May 23, 2024. (https://stratcomcoe.org/cuploads/pfiles/timothy_thomas.pdf)

74. Shane Harris, Karen DeYoung, Ysabelle Khurshudyan, Ashley Parker, and Liz Sly, "Road to war: U.S. struggled to convince allies, and Zelensky, of risk of invasion," *The Washington Post*, August 16, 2022. (https://www.washingtonpost.com/national-security/interactive/2022/ukraine-road-to-war)

75. Courtney Kube and Dan De Luce, "Despite appeals from Ukraine, Biden admin holds back additional military aid to Kyiv amid diplomatic push," *NBC News*, December 10, 2021. (https://www.nbcnews.com/politics/national-security/appeals-ukraine-biden-admin-holds-back-additional-military-aid-kyiv-di-rcna8421)

76. Joe Cheravitch, "The Role of Russia's Military in Information Confrontation," *Center for Naval Analyses*, June 2021. (https://www.cna.org/reports/2021/06/The-Role-of-Russia%27s-Military-in-Information-Confrontation.pdf)

internationally while employing *maskirovka* (deception) to generate a degree of plausible deniability.[77] In 2022, seeking to facilitate information control and sap Ukrainian will to fight, Russian hackers conducted destructive cyberattacks against Ukrainian media companies and critical infrastructure, complementing kinetic strikes against such targets.[78]

Meanwhile, Moscow continually seeks to subvert the United States and other "unfriendly" countries by exploiting divisions and interfering in domestic politics.[79] In the United States, Russian information operations have seized on wedge issues such as "gun control, ethnic group rivalries, tensions between police and local communities, and abortion."[80] Heading into the 2024 U.S. elections, Russian information operations have sought to undermine American support for Ukraine.[81] Stoking opposition to Ukraine aid is currently Moscow's main objective in Europe, too. In Slovakia, for example, local analysts say pro-Russia propaganda surged ahead of an April 2024 presidential contest that swung in favor of Ukraine skeptic Peter Pellegrini.[82]

Moscow also strives to promote Russian influence and narratives in the "Global South" and in battleground

---

77. See, for example: Raphael Satter and Dmytro Vlasov, "Ukraine soldiers bombarded by 'pinpoint propaganda' texts," *Associated Press*, May 11, 2017. (https://apnews.com/article/technology-europe-ukraine-only-on-ap-9a564a5f64e847d1a50938035ea64b8f); Ellen Nakashima, "Inside a Russian disinformation campaign in Ukraine in 2014," *The Washington Post*, December 25, 2017. (https://www.washingtonpost.com/world/national-security/inside-a-russian-disinformation-campaign-in-ukraine-in-2014/2017/12/25/f55b0408-e71d-11e7-ab50-621fe0588340_story.html); Margarita Jaitner and Peter A. Mattsson, "Russian Information Warfare of 2014," *NATO Cooperative Cyber Defence Centre of Excellence*, 2015. (https://www.ccdcoe.org/uploads/2018/10/Art-03-Russian-Information-Warfare-of-2014.pdf)

78. "An overview of Russia's cyberattack activity in Ukraine," *Microsoft*, April 27, 2022. (https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd). According to Microsoft, these attacks picked up in October 2022, when Russia launched a missile and drone campaign against Ukraine's power grid and other critical infrastructure. Clint Watts, "Preparing for a Russian cyber offensive against Ukraine this winter," *Microsoft*, December 3, 2022. (https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/#_ednref4). But Russian hackers also launched similar attacks earlier in the war. See: Joe Tidy, "Ukrainian power grid 'lucky' to withstand Russian cyber-attack," *BBC* (UK), April 12, 2022. (https://www.bbc.com/news/technology-61085480)

79. "Authoritarian Interference Tracker," *Alliance for Securing Democracy at the German Marshall Fund of the United States*, accessed May 23, 2024. (https://securingdemocracy.gmfus.org/toolbox/authoritarian-interference-tracker/?fwp_threat_actor=russia); Kylie Atwood, Michael Conte, and Devan Cole, "Russia has spent over $300 million on influencing foreign elections since 2014, US officials say," *CNN*, September 13, 2022. (https://www.cnn.com/2022/09/13/politics/russia-foreign-elections-influence/index.html)

80. Mark Hosenball, "Russia stoking U.S. racial, social differences ahead of election: sources," *Reuters*, March 10, 2020. (https://www.reuters.com/article/us-usa-election-security/russia-stoking-u-s-racial-social-differences-ahead-of-election-sources-idUSKBN20X2O3)

81. Clint Watts, "Russian US election interference targets support for Ukraine after slow start," *Microsoft*, April 17, 2024. (https://blogs.microsoft.com/on-the-issues/2024/04/17/russia-us-election-interference-deepfakes-ai); Julian E. Barnes and David E. Sanger, "Russia Amps Up Online Campaign Against Ukraine Before U.S. Elections," *The New York Times*, March 27, 2024. (https://www.nytimes.com/2024/03/27/us/politics/russian-ukraine-us-interference.html). For another recent example, see: U.S. Department of the Treasury, Press Release, "Treasury Targets the Kremlin's Continued Malign Political Influence Operations in the U.S. and Globally," July 29, 2022. (https://home.treasury.gov/news/press-releases/jy0899)

82. Paul Hockenos, "Russia Just Helped Swing a European Election," *Foreign Policy*, April 17, 2024. (https://foreignpolicy.com/2024/04/17/slovakia-president-pellegrini-russia-election-interference-disinformation). For other examples, see: "Czechs Bust Major Russian Propaganda Network," *Agence France-Presse* (France), March 27, 2024. (https://www.barrons.com/news/czechs-bust-major-russian-propaganda-network-1ee4d2df); Florian Reynaud and Philippe Ricard, "France uncovers vast network of Russian disinformation sites," *Le Monde* (France), February 12, 2024. (https://www.lemonde.fr/en/pixels/article/2024/02/12/france-uncovers-vast-network-of-russian-disinformation-sites_6518362_13.html)

countries elsewhere. Russian propaganda outlets are often popular in these nations.[83] Moscow's messaging often exploits colonial grievances to villainize the West. In November 2023, the State Department warned that Moscow "is currently financing an on-going, well-funded disinformation campaign across Latin America," aiming "to leverage developed media contacts in" over a dozen Latin American countries.[84] The Russians have established similar schemes in Africa.[85] They have also lent their information warfare services (and private military contractors) to a host of Russia-friendly regimes in exchange for influence and access to natural resources.[86]

The U.S. Response

Since 2016, Washington has taken some notable steps to protect the U.S. information space and counter Russian disinformation. Notably, U.S. Cyber Command has pre-emptively targeted Russian trolls and hackers to protect recent U.S. elections — a key foundation of American stability, power, and democratic credibility.[87] U.S. Cyber Command has also worked with allies and partners to hunt Russian hackers.[88] Washington has wielded declassified intelligence to counter Russian disinformation, including by revealing that Moscow planned to stage a false-flag attack to justify its 2022 invasion of

83. Yaroslav Trofimov, "Why Many in the Developing World Have Sided With Russia," *The Wall Street Journal*, October 27, 2022. (https://www.wsj.com/articles/why-many-in-the-developing-world-have-sided-with-russia-11666900508); David Klepper and Amanda Seitz, "Russia aims Ukraine disinformation at Spanish speakers," *Associated Press*, April 2, 2022. (https://apnews.com/article/russia-ukraine-ap-top-news-facebook-europe-media-fb3758a9a11182558976a3a4f3b121dd); Vedant Patel, "Yevgeniy Prigozhin's Africa-Wide Disinformation Campaign," *U.S. Department of State*, November 4, 2022. (https://www.state.gov/disarming-disinformation/yevgeniy-prigozhins-africa-wide-disinformation-campaign)

84. U.S. Department of State, "The Kremlin's Efforts to Covertly Spread Disinformation in Latin America," November 7, 2023. (https://www.state.gov/the-kremlins-efforts-to-covertly-spread-disinformation-in-latin-america)

85. U.S. Department of State, "The Kremlin's Efforts to Covertly Spread Disinformation in Latin America," November 7, 2023. (https://www.state.gov/the-kremlins-efforts-to-covertly-spread-disinformation-in-latin-america); Elizabeth Dwoskin, "How Russian disinformation toppled government after government in Africa," *The Washington Post,* October 30, 2023. (https://www.washingtonpost.com/technology/2023/10/21/percepto-africa-france-russia-disinformation)

86. Roman Badanin, "Шеф и повар. Часть третья. Расследование о том, как Россия вмешивается в выборы в двадцати странах [Chef and Cook Part III: Investigation Into How Russia Interferes in Elections in 20 Countries]," *Proekt* (Russia), April 11, 2019. (https://www.proekt.media/investigation/prigozhin-polittekhnologi). For a broader, more recent overview, see: Jack Watling, Oleksandr V Danylyuk, and Nick Reynolds, "The Threat from Russia's Unconventional Warfare Beyond Ukraine, 2022–24," *Royal United Services Institute*, February 2024. (https://static.rusi.org/SR-Russian-Unconventional-Weapons-final-web.pdf)

87. Ellen Nakashima, "U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms," *The Washington Post*, February 27, 2019. (https://www.washingtonpost.com/world/national-security/us-cybercommand-operation-disrupted-internet-access-of-russian-trollfactory-on-day-of-2018-midterms/2019/02/26/1827fc9e36d6-11e9-af5b-b51b7ff322e9_story.html); Ellen Nakashima, "U.S. cyber force credited with helping stop Russia from undermining midterms," *The Washington Post*, February 14, 2019. (https://www.washingtonpost.com/world/nationalsecurity/us-cyber-force-credited-with-helping-stop-russia-fromundermining-midterms/2019/02/14/ceef46ae-3086-11e9-813a0ab2f17e305b_story.html); David E. Sanger and Julian E. Barnes, "U.S. Tried a More Aggressive Cyberstrategy, and the Feared Attacks Never Came," *The New York Times*, November 9, 2020. (https://www.nytimes.com/2020/11/09/us/politics/cyberattacks-2020-election.html); David E. Sanger and Nicole Perlroth, "Microsoft Takes Down a Risk to the Election, and Finds the U.S. Doing the Same," *The New York Times*, October 12, 2020. (https://www.nytimes.com/2020/10/12/us/politics/election-hacking-microsoft.html); Ellen Nakashima, "Cybercom disrupted Russian and Iranian hackers throughout the midterms," *The Washington Post*, December 22, 2022. (https://www.washingtonpost.com/national-security/2022/12/22/cybercom-russia-iran-attacks)

88. See, for example: Sean Lyngaas, "Cyber Command's midterm election work included trips to Ukraine, Montenegro, and North Macedonia," *CyberScoop*, March 14, 2019. (https://www.cyberscoop.com/cyber-command-midterm-elections-ukraine-montenegro-andnorth-macedonia); Julian E. Barnes, "U.S. Cyber Command Expands Operations to Hunt Hackers From Russia, Iran and China," *The New York Times*, November 2, 2020. (https://www.nytimes.com/2020/11/02/us/politics/cyber-commandhackers-russia.html)

Ukraine.[89] Washington has also exposed some Russian media fronts.[90] Since 2017, the Justice Department has required various Russian propaganda arms, including RT (formerly known as Russia Today), to register as foreign agents.[91] Following Russia's 2022 invasion of Ukraine, RT America ceased operations after U.S. companies refused to work with it,[92] although former RT America employees reportedly launched a similar media venture shortly thereafter.[93]

However, important weaknesses remain. First, America is generally failing to reach ordinary Russians. Although Moscow insists it faces a U.S.-directed "hybrid war,"[94] Washington struggles to penetrate Russia's information space, particularly now that many Western outlets have been forced to leave Russia.[95] Overt U.S. government messaging is often clumsy and pedestrian. For example, the State Department's Russian-language Telegram channel, belatedly launched days after Moscow's full-scale invasion, simply reposts department press releases. As of this writing, it has only around 7,100 subscribers.[96]

Washington is also struggling in the battle for hearts and minds in the "Global South," where Russian propaganda outlets are often more popular than Western media. For instance, RT en Español has over 17 million followers on Facebook, Latin America's most popular social media platform. CNN en Español has 14 million.[97] In July 2023, Putin announced that various Russian state media outlets, including RT and Sputnik's parent company, would open new offices in Africa.[98]

Meanwhile, the Pentagon's already middling clandestine information warfare efforts have faced setbacks. In August 2022, researchers indicated that U.S. military information support operations, or MISO, had apparently used fake social media accounts to promote pro-U.S. content, including anti-Kremlin messaging targeting Central Asian audiences. Some of the accounts posted fictitious content. White House concerns led the Pentagon to launch a review of MISO. The accounts apparently achieved little reach and were easily detected by Facebook and Twitter.[99] Moreover, the Pentagon is reportedly considering cutting MISO

89. Ellen Nakashima, Shane Harris, Ashley Parker, John Hudson, and Paul Sonne, "U.S. accuses Russia of planning to film false attack as pretext for Ukraine invasion," *The Washington Post,* February 3, 2022. (https://www.washingtonpost.com/national-security/2022/02/03/russia-ukraine-staged-attack)
90. U.S. Department of the Treasury, Office of Foreign Assets Control, Press Release, "Treasury Escalates Sanctions Against the Russian Government's Attempts to Influence U.S. Elections," April 15, 2021. (https://home.treasury.gov/news/press-releases/jy0126); U.S. Department of the Treasury, Office of Foreign Assets Control, Press Release, "Treasury Russians Bankrolling Putin and Russia–Backed Influence Actors," March 3, 2022. (https://home.treasury.gov/news/press-releases/jy0628)
91. U.S. Department of Justice, "Foreign Agents Registration Act -- Browse Filings," accessed May 21, 2024. (https://efile.fara.gov/ords/fara/f?p=1381:1:26779218968177)
92. Jeremy Barr, "RT America goes off the air amid backlash to Kremlin-funded media," *The Washington Post,* March 4, 2022. (https://www.washingtonpost.com/media/2022/03/03/rt-america-production-company-closes)
93. Lachlan Markay, "Scoop: Russia state propaganda alums launch new D.C. media venture," *Axios,* January 26, 2023. (https://www.axios.com/2023/01/26/russia-rt-america-globaltek)
94. See, for example: "Lavrov slams all-out sanctions spree, says West's values 'aren't worth a red cent,'" *Tass* (Russia), March 25, 2022. (https://tass.com/politics/1427557)
95. "RFE/RL Suspends Operations In Russia Following Kremlin Attacks," *Radio Free Europe/Radio Liberty,* March 6, 2022. (https://www.rferl.org/a/rferl-suspends-russia-operations/31738541.html)
96. США по-русски, *Telegram*, accessed May 21, 2024. (https://t.me/USApoRusski)
97. "RT en Español," *Facebook*, accessed May 21, 2024. (https://www.facebook.com/ActualidadRT); "CNN en Español," *Facebook*, accessed May 21, 2024. (https://www.facebook.com/CNNee)
98. "RT, Sputnik and other Russian media to open offices in Africa – Putin," *Russia Today* (Russia), July 27, 2023. (https://www.rt.com/africa/580391-putin-africa-information-space)
99. Ellen Nakashima, "Pentagon opens sweeping review of clandestine psychological operations," *The Washington Post*, September 19, 2022. (https://www.washingtonpost.com/national-security/2022/09/19/pentagon-psychological-operations-facebook-twitter); "Unheard Voice: Evaluating five years of pro-Western covert influence operations," *Graphika and Stanford Internet Observatory*, August 24, 2022. (https://public-assets.graphika.com/reports/graphika_stanford_internet_observatory_report_unheard_voice.pdf)

billets as a cost-saving measure,[100] which would exacerbate existing MISO staffing challenges.[101]

Recommendations

It is time to take the fight to Moscow in the information domain. That will require countering both Russia's information-technical and information-psychological efforts. The following recommendations can help Washington proactively counter Russian disinformation and reach key audiences within Russia and elsewhere:

- **Revamp U.S. efforts to reach ordinary Russians and Russian speakers in neighboring countries.** The U.S. Government — including the U.S. Agency for Global Media, State Department (including the Global Engagement Center (GEC), Defense Department, and Intelligence Community — should offer or facilitate engaging content on platforms frequented by Russians and Russian speakers, crafting messaging tailored to Russia's culture and political reality rather than attempting to sell the American dream, which does not resonate with most Russians. Programming inside Russia should focus on revealing Putin's lies and the costs of his unprovoked invasion for average Russians. Congress should require a classified report on any existing efforts to counter disinformation inside Russia and how those efforts can be better measured and strengthened.
- **Strengthen U.S. efforts to fight Russian information warfare in the "Global South."** The interagency should prioritize efforts to counter Russian narratives and disinformation tactics in Latin America, Africa, and Asia. The armed services committees should request information from the Department of Defense about the composition, resourcing, and geographic distribution of Military Information Support Teams operating out of U.S. embassies and whether the current posture is appropriate. Congress should also require that the administration submit an assessment of any statutory limitations on efforts to address Russian disinformation.
- **Facilitate offensive information operations by non-governmental actors.** The administration and Congress should review grantmaking practices to facilitate offensive information operations within the private sector. For example, the GEC currently produces reports to spotlight Russian disinformation. It also funds journalists and civil society groups with the hope that they will counter Russian disinformation and influence. However, the GEC does not give these groups direction regarding their content. Washington should consider empowering the GEC to contract third-party organizations for specific tasks, e.g. creating short, engaging films about Kremlin corruption or the Russian-instigated food crisis. Washington could also harmonize the GEC's grantmaking operations with the U.S. Agency for Global Media's (USAGM's) Open Technology Fund (OTF), which funds internet freedom technologies at every stage of the development cycle. By creating a combined, better-resourced grant-making body, Washington could create a more nimble and creative organization that is also aggressive.[102]

---

100. Patrick Tucker, "US may cut info-warfare assets as China, Russia expand influence ops," *Defense One,* February 8, 2024. (https://www.defenseone.com/policy/2024/02/exclusive-us-may-cut-info-warfare-assets-china-russia-expand-influence-ops/394050)

101. U.S. Department of Defense, Office of Inspector General, Press Release, "Evaluation of the DoD's Military Information Support Operations Workforce (Report No. DODIG-2024-068)," March 27, 2004. (https://www.dodig.mil/In-the-Spotlight/Article/3719783/press-release-evaluation-of-the-dods-military-information-support-operations-wo); U.S. Department of Defense, Office of Inspector General, "Evaluation of U.S. Special Operations Command's Joint Military Information Support Operations Web Operations Center (DODIG-2023-080)," June 8, 2008. (https://www.dodig.mil/reports.html/Article/3421329/evaluation-of-us-special-operations-commands-joint-military-information-support)

102. The grantmaking efforts of the GEC and OTF should be harmonized, which can enhance the effectiveness of countering disinformation. By aligning their strategies, these entities can avoid duplication of efforts and ensure a more streamlined and cohesive approach to addressing information warfare. Harmonization can leverage the relative strengths of both organizations and promote efficient resource allocation within the U.S. government, leading to a more comprehensive and impactful response to global challenges related to information manipulation.

Iran

By Mark Dubowitz and Saeed Ghasseminejad

Introduction

In August 1978, the Islamist followers of Ayatollah Ruhollah Khomeini set Cinema Rex in Abadan on fire and burned almost 500 Iranians alive. Khomeini's operatives blamed the attack on Savak, the intelligence and security service for the Mohammad Reza Shah Pahlavi government.[103] The Cinema Rex incident helped ignite the Islamic Revolution of 1979, which led to the fall of the Pahlavi dynasty. In retrospect, however, the Islamist clergy had won the information war against the Shah long before the revolution succeeded.[104]

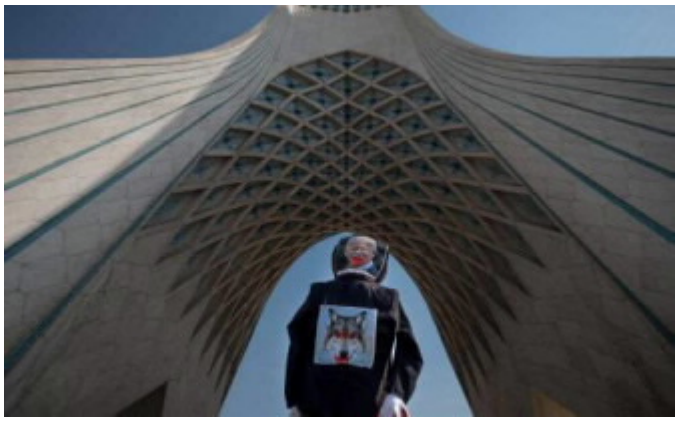
Since 1979, the Islamic Republic has heavily invested in information warfare that features both defensive and offensive elements, focusing on Iranians, Americans, and

103. Ali Sajjadi, "آتش سوزی سینما رکس: آغازوحشت بزرگ چهل ساله [The Arson at the Rex Cinema: How Iran's Forty-Year Terror Began]," July 22, 2018. (https://www.amazon.com/Cinema-Atash-soozi-Aghaz-vahshat-bozorg/dp/1723585068)
104. Alireza Kermani, "بازخوانی پرونده سینما رکس پس از ۳۰ سال [Reviewing the Cinema Rex Case after 30 years]," *Radio Farda*, August 20, 2008. (https://www.radiofarda.com/a/f6_Iran_Abadan_Rex_Cinema/461554.html)

other key audiences around the world.[105] Washington needs to step up its game. This requires interagency investment in better understanding and countering the Islamic Republic's information warfare; implementing a persistent campaign focused on sanctioning the regime's disinformation networks; expanding U.S. information warfare efforts; and improving offensive information operations inside Iran that support the Iranian people and target the Islamic Republic.

Tehran's Approach to Information Warfare

Developing an effective information warfare campaign against the Islamic Republic requires the U.S. government to clearly understand the regime's information warfare goals, messages, and means. The regime's information warfare strategy seeks to secure the regime's survival by discrediting its domestic and foreign enemies, pacifying the Iranian people, strengthening the loyalty of followers, and recruiting new supporters. Tehran also seeks to use information warfare to influence and confuse foreign decision-makers and create chaos in target countries such as the United States, United Kingdom, Germany, Canada, Iraq, and Lebanon.[106]



A pro-regime supporter carries an effigy of U.S. President Joe Biden during a rally at Azadi (Freedom) Square in Tehran, Iran, on February 11, 2024. (Photo by Morteza Nikoubazl/ NurPhoto via Getty Images)

Within Iran, the regime's key information goal is to destroy the reputation of any alternatives that might replace it, portraying opponents as traitors and challenging their competence. The regime seeks to stoke fear that the collapse of the Islamic Republic would be the end of the Iranian nation and the beginning of an endless civil war.[107]

Internationally, the regime uses information warfare to weaken adversaries in target countries by deepening existing political and societal fissures, creating new

105. Mark Dubowitz and Saeed Ghasseminejad, "Iran's COVID-19 Disinformation Campaign," *Combating Terrorism Center At West Point, CTC Sentinel*, June 2020. (https://ctc.westpoint.edu/irans-covid-19-disinformation-campaign); Seth G. Jones and Danika Newlee, "The United States' Soft War with Iran," *Center for Strategic and International Studies*, June 11, 2019. (https://www.csis.org/analysis/united-states-soft-war-iran); Saeed Ghasseminejad and Alireza Nader, "Who runs Iran's Propaganda abroad?" *Radio Farda*, April 17, 2020. (https://en.radiofarda.com/a/who-runs-iran-s-propaganda-machine-abroad/30561872.html); Emerson T. Brooking and Suzanne Kianpour, "Iranian digital influence efforts: Guerrilla broadcasting for the twenty-first century," *Atlantic Council*, February 11, 2020. (https://www.atlanticcouncil.org/in-depth-research-reports/report/iranian-digital-influence-efforts-guerrilla-broadcasting-for-the-twenty-first-century); Toby Dershowitz and Talia Katz, "Torture TV: The Case for Sanctions on the Islamic Republic of Iran's State-Run Media," *Foundation for Defense of Democracies*, February 27, 2020. (https://www.fdd.org/wp-content/uploads/2020/02/fdd-report-torture-tv-the-case-for-sanctions-on-the-islamic-republic-of-irans-state-run-media.pdf)

106. Facebook, Press Release, "April 2020 Coordinated Inauthentic Behavior Report," May 5, 2020. (https://about.fb.com/news/2020/05/april-cib-report); Ben Nimmo, C. Shawn Eib, Lea Ronzaud, Rodrigo Ferreira, Thomas Lederer, and Melanie Smith, "Iran's Broadcaster: Inauthentic Behavior," *Graphika*, May 2020. (https://public-assets.graphika.com/reports/graphika_report_irib_takedown.pdf). For a good example, see the Iran International and Semafor stories about Tehran's efforts to create a network of Iran experts in the West to disseminate pro-Tehran points of view among American and European media and officials. Jay Solomon, "Inside Iran's influence operation," *Semafor*, September 29, 2023. (https://www.semafor.com/article/09/25/2023/inside-irans-influence-operation); Bozorgmehr Sharafeddin, "Inside Tehran's Soft War, How Iran Gained Influence In US Policy Centers," *Iran International*, September 29, 2023. (https://content.iranintl.com/en/investigates/inside-tehran-softwar/index.html)

107. "براندازی جمهوری اسلامی مساوی با تجزیه ایران است" [Malayer's Friday Prayer Imam: the fall of the Islamic Republic is equal to partition of Iran]," *Iranian Student News Agency* (Iran), October 7, 2022. (https://www.isna.ir/news/1401071507121/براندازی-جمهوری-اسلامی-مساوی-با-تجزیه-ایران-است)

ones, and intensifying distrust among citizens and between citizens and their governments. The regime focuses on radical anti-American and anti-Israel left-wing and right-wing groups, marginalized minorities, the Iranian diaspora, and Muslim communities.[108]

To convey its messages and achieve its goals, the Islamic Republic employs a multi-layered information warfare apparatus with branches across the globe.

The state-controlled Islamic Republic of Iran Broadcasting (IRIB) plays a prominent role in this campaign.[109] To influence non-Iranian audiences, IRIB operates TV channels in foreign languages, including English (Press TV), Spanish (Hispan TV), and Arabic (Al-Alam). In a notable win for Tehran, IRIB managed to convince prominent political figures such as the British Labor Party's Jeremy Corbyn and Pablo Iglesias of Spain's Podemos political party to appear on, or consult for, IRIB channels.[110]

Further, the Islamic Revolutionary Guard Corps (IRGC)-controlled Fars News and Tasnim News seek to magnify the voices of anti-American figures through their English language operations.[111] Fars and Tasnim identify Western pundits and analysts who agree with the regime's point of view to echo Tehran's propaganda through interviews.

In the West, the regime uses hacktivist groups to gather information and influence policy and politics.[112] For example, the regime worked to influence perceptions of the American public during the 2020 U.S. election.[113] The regime uses agents to undermine opposition groups and discredit or assassinate dissidents. Mohammad Reza Madhi, for example, appeared in the opposition political sphere in 2010 and presented himself as a former high-ranking intelligence officer who was forced to flee the country after he had uncovered corruption by top regime officials. Madhi insinuated himself into opposition groups and got involved in efforts to create a government in exile. A year later, he appeared in a documentary broadcast by the IRIB, called "A Diamond to Deceive," in which he described his activities. The regime used the Madhi saga to gather information and sow mistrust and fear among opposition figures. Madhi

108. "The Second International 'New Horizon' Conference in Tehran Draws Leading Holocaust Deniers, Conspiracy Theorists, And BDS Activists From Around The World – And Is Backed And Supported By Iranian Regime," *MEMRI*, October 15, 2014. (https://www.memri.org/reports/second-international-new-horizon-conference-tehran-draws-leading-holocaust-deniers); Muhammad Fraser-Rahim, "Iran and #BlackLivesMatter," *LobeLog*, April 29, 2016. (https://lobelog.com/iran-and-blacklivesmatter)

109. For a detailed overview of IRIB, see: Toby Dershowitz and Talia Katz, "Torture TV, The Case for Sanctions on the Islamic Republic of Iran's State-Run Media," *Foundation for Defense of Democracies*, February 2020. (https://www.fdd.org/wp-content/uploads/2020/02/fdd-report-torture-tv-the-case-for-sanctions-on-the-islamic-republic-of-irans-state-run-media.pdf)

110. Adam Payne, "Jeremy Corbyn was paid by an Iranian state TV station that was complicit in the forced confession of a tortured journalist," *Business Insider*, July 2, 2016. (https://www.businessinsider.com/jeremy-corbyn-paid-iran-press-tv-tortured-journalist-2016-6); Adam Payne, "Jeremy Corbyn finally talked about the money he received from Iran's Press TV," *Business Insider*, September 1, 2016. (https://www.businessinsider.in/jeremy-corbyn-finally-talked-about-the-money-he-received-from-irans-press-tv/articleshow/53961694.cms); Giles Tremlett, "The Podemos revolution: how a small group of radical academics changed European politics," *The Guardian* (UK), March 31, 2015. (https://www.theguardian.com/world/2015/mar/31/podemos-revolution-radical-academics-changed-european-politics)

111. Saeed Ghasseminejad, "The Men Who Built Fars News," *Iran Disinformation Project*, accessed March 21, 2024. (https://irandisinfo.org/ghasseminejad-farsnews-deception-part-one)

112. Sean Lyngaas, "Hackers actively supporting Iran's domestic and foreign spying efforts, researchers warn," *CNN*, September 7, 2022. (https://www.cnn.com/2022/09/07/politics/iran-irgc-hackers-mandiant/index.html)

113. Two Iranian nationals gained access to U.S. voter information through at least one state election website and sent disinformation and threatening messages to prospective voters while posing as an American group. U.S. Department of Justice, Press Release, "Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election," November 18, 2021. (https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-enabled-disinformation-and-threat-campaign-designed). In many cases, hacktivist groups or hackers working for front companies run these operations. But the operations are mostly likely directed by the IRGC and/or Ministry of Intelligence and Security cyber division.

described how he infiltrated an opposition group and portrayed them as foolish and corrupt.[114]

In September 2023, Iran International and Semafor revealed a sophisticated influence operation, devised and run by a former IRGC officer and close confidant of Iran's former foreign minister, Javad Zarif. The goal was to influence Western public opinion and policymakers on behalf of the Islamic Republic of Iran by creating close personal and professional connections with a group of dual-national Iranians in policy and media circles who had access to Western policymakers.[115]

The regime also furthers its information warfare objectives by sometimes cloaking its efforts behind a benign disguise.[116] Missionaries, for example, are trained in Qom, especially at Al-Mustafa International University, and then sent to countries around the world to run Islamic centers and mosques.[117] Al-Mustafa, with branches in some 50 countries,[118] has trained more than 60,000 students from more than 130 nations,[119] including many in Latin America. Meanwhile, Al-Mustafa not only teaches how to proselytize but also recruits foreign fighters and intelligence operatives and sends them into the fray. The United States recognized this problem in December 2020 when it designated the university[120] for supporting the Quds Force, the IRGC's overseas operations arm.[121]

---

114. Iran's Ministry of Intelligence and Security play a critical role in such operations. Federal Research Division, Library of Congress, "Iran's Ministry of Intelligence and Security: A Profile," December 2012. (https://irp.fas.org/world/iran/mois-loc.pdf); Golnaz Esfandiari, "Alleged Iranian Agent Who Infiltrated Opposition Claims He Met With Hillary Clinton," *Radio Free Europe/Radio Liberty*, June 10, 2011. (https://www.rferl.org/a/iran_agent_opposition_clinton_intelligence_ministry/24231353.html). They seek to influence global public opinion with a focus on millions of Iranian expatriates, the majority of whom reside in Western Europe and North America. Regime officials regularly meet with Iranian ex-pats around the world, inviting them to travel to Iran and invest there. "دکتر رئیسی در دیدار با ایرانیان مقیم آمریکا [Iranians living in the United States meet with Dr. Raisi]," *The High Council of Expatriate Iranian at the Ministry of Foreign Affairs*, September 25, 2023. (https://iranian.mfa.ir/portal/newsview/730150/دکتر-رییسی-در-دیدار-با-ایرانیان-مقیم-آمریکا)

115. Jay Solomon, "Inside Iran's influence operation," *Semafor*, September 29, 2023. (https://www.semafor.com/article/09/25/2023/inside-irans-influence-operation); Bozorgmehr Sharafeddin, "Inside Tehran's Soft War, How Iran Gained Influence In US Policy Centers," *Iran International*, September 29, 2023. (https://content.iranintl.com/en/investigates/inside-tehran-softwar/index.html)

116. The German government expelled the deputy head of the Islamic Center of Hamburg, Seyyed Soleiman Musavifar, in June 2022 for his support of extremist organizations and his connections to Iran-backed Hezbollah. "Germany Expels Iranian Cleric Over Support For Shiite Extremists," *Iran International*, June 19, 2022. (https://www.iranintl.com/en/202206199642). Unsurprisingly, the regime attempts to deflect scrutiny of its information warfare efforts by hiding some of them within its global network of Islamic Centers and leveling false charges of Islamophobia.

117. Seth G. Jones and Danika Newlee, "The United States' Soft War with Iran," *Center for Strategic and International Studies*, June 11, 2019. (https://www.csis.org/analysis/united-states-soft-war-iran); Hassan Dai, "Tehran's soft-power reach extends all the way to Africa," *Jewish News Syndicate*, November 12, 2018. (https://www.jns.org/tehrans-extensive-soft-power-reach-in-africa); Frud Bezhan, "Charges Against Cleric Put Iran's Balkan Activities Under Spotlight," *Radio Free Europe/Radio Liberty*, June 28, 2016. (https://www.rferl.org/a/kosovo-iran-cleric-arrest/27886917.html)

118. Frud Bezhan, "U.S. Sanctions Put Spotlight On Iran's International Network Of Religious Seminaries," *Radio Free Europe/Radio Liberty*, December 20, 2020. (https://www.rferl.org/a/iran-u-s-sanctions-religious-seminaries-network-al-mustafa/31014153.html)

119. "طلاب ۱۳۰ ملیت در جامعة المصطفی تحصیل می‌کنند [Students from 130 nations study at Al-Mustafa University]," *The Islamic Republic News Agency* (Iran), May 3, 2023. (https://www.irna.ir/news/85100795/طلاب-۱۳۰-ملیت-در-جامعة-المصطفی-تحصیل-می-کنند); "جامعه المصطفی بیش از ۶۰ هزار نفر از ۱۳۰ کشور جهان فارغ التحصیل دارد [Al-Mustafa University has more than 60,000 alumni from more than 130 countries]," *Javan* (Iran), February 9, 2018. (https://www.javanonline.ir/003kjI)

120. U.S. Department of the Treasury, Press Release, "Treasury Sanctions Iran's Envoy in Yemen and University Facilitating Recruitment for Qods Force," December 8, 2020. (https://home.treasury.gov/news/press-releases/sm1205)

121. Emanuele Ottolenghi, "Emerging External Influences in the Western Hemisphere," *Testimony before the Senate Committee on Foreign Relations Subcommittee on Western Hemisphere, Transnational Crime, Civilian Security, Democracy, Human Rights, and Global Women's Issues*, May 10, 2017. (https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/documents/51017_EO_Testimony.pdf); Anwar Luz, "How Two Months at an Iranian Seminary Changed My Life," *New Lines Magazine*, February 28, 2023. (https://newlinesmag.com/first-person/how-two-months-at-an-iranian-seminary-changed-my-life); Emanuele Ottolenghi, "Soleimani U," *Tablet Magazine*, February 23, 2022. (https://www.tabletmag.com/sections/news/articles/soleimani-u). In addition, Iranian organizations such as the Islamic Development Organization and the Islamic Propaganda Office of Qom Seminary are involved in such operations to varying degrees.

The U.S. Response

The U.S. government has focused primarily on outreach to the Iranian people via the USAGM's Persian-language news services, Radio Farda and Voice of America's Persian News Network (PNN).[122] These efforts aim to counter the regime's disinformation campaigns against its own citizens by empowering civil society and explaining American ideas and policy. However, for years PNN has been beset with reported problems related to internal mismanagement and questions about the quality of its content.[123] Indeed, the market share of these American efforts is eclipsed by other outlets, including UK-owned Iran International, BBC Persian, and Manoto.[124]

Measuring the success of such U.S. efforts inside Iran is difficult, but it seems clear that there is room for improvement.[125] PNN could learn from its more successful rivals, such as Manoto and Iran International.

More broadly, the U.S. government has thus far failed to fully grasp the scope of the Islamic Republic's information warfare activities, much less develop a unified and executable strategy that effectively counters Iran's global campaign.

The most substantive U.S. wins have come through sanctioning Tehran's information warfare machine. Over the last few years, the U.S. Department of the Treasury designated hacktivist groups, Al-Mustafa International University, the New Horizon Conference, the IRGC-connected Fars News and Tasnim News, and elements of the IRIB for their roles in the regime's information warfare campaign.[126]

These designations can create obstacles to the regime's operations, especially in the United States and allied countries. Sanctions provide Washington with authorities to freeze assets, expel or block operatives, and unravel the complex networks that support these operations. Nonetheless, enforcement of these designations still needs to improve. For example, the IRGC-connected Tasnim News still operates on the U.S.-based social media network X despite being sanctioned. Furthermore, personnel associated with

122. In addition to the USAGM, the U.S. government has been using the social media accounts of the president of the United States, secretary of state, and State Department's Persian outreach, USA Beh Farsi, to address Iranians. The Trump administration used these channels effectively to communicate with the Iranian people. But under President Biden, these channels have lost their prominence in the Persian-language sphere due to missteps and misguided policy. For more information, see: Saeed Ghasseminejad and Behnam Taleblu, "Biden's tone-deaf Iran policy ignores what the Iranian people want: freedom, not terrorism," *New York Post*, April 7, 2024. (https://nypost.com/2024/04/07/opinion/bidens-tone-deaf-iran-policy-ignores-what-the-iranian-people-want-freedom-not-terrorism)

123. Helle Dale, "Reaching Iran: Problems with U.S. Media Messaging," *Jewish Policy Center*, Summer 2012. (https://www.jewishpolicycenter.org/2012/05/31/iran-us-media); U.S. House Foreign Affairs Committee, Press Release, "McCaul Pushes For Oversight of Repeated Stonewalling at USAGM Ahead of Next Congress," December 20, 2022. (https://foreignaffairs.house.gov/press-release/mccaul-pushes-for-oversight-of-repeated-stonewalling-at-usagm-ahead-of-next-congress); Ilan Berman, "Reforming U.S. Persian Language Media - A preliminary Assessment," *American Foreign Policy Council*, April 22, 2019. (https://afpc.org/publications/policy-papers/iran-strategy-brief-no.-13-reforming-u.s.-persian-language-media-a-preliminary-assessment); "U.S. Persian Media Study Final Synthesis Report," *American Foreign Policy Council*, October 6, 2017. (https://www.usagm.gov/wp-content/media/2011/11/AFPC_Persian-Language-Broadcasting-Study_synthesis-report.pdf)

124. Ilan Berman, "Reforming U.S. Persian Language Media - A preliminary Assessment," *American Foreign Policy Council*, April 22, 2019. (https://www.afpc.org/publications/policy-papers/iran-strategy-brief-no.-13-reforming-u.s.-persian-language-media-a-preliminary-assessment)

125. It is worth noting that a leading goal for Tehran in the March 2023 Beijing-brokered Iran-Saudi Arabia agreement was apparently an end to Iran International's broadcasts.

126. U.S. Department of the Treasury, Press Release, "Treasury Sanctions Iran's Envoy in Yemen and University Facilitating Recruitment for Qods Force," December 8, 2020. (https://home.treasury.gov/news/press-releases/sm1205); U.S. Department of Justice, Press Release, "Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election," November 18, 2021. (https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-enabled-disinformation-and-threat-campaign-designed); U.S. Department of the Treasury, Press Release, "Treasury Sanctions Iranian Organizations and Individuals Supporting Intelligence and Cyber Targeting of U.S. Persons," February 13, 2019. (https://home.treasury.gov/news/press-releases/sm611)

Al-Mustafa continue to operate freely in numerous countries, including some allied with the United States.

Recommendations

To more effectively counter Tehran in the information warfare sphere, it is essential to have a comprehensive and detailed understanding of its objectives, key messages, and methods. Such an understanding should be the foundation of a U.S. plan to wage a more effective defensive and offensive information warfare campaign targeting the regime in Tehran. The following recommendations should also be considered:

- **Establish an interagency task force.** The Biden administration should establish an interagency task force to conduct a comprehensive review of Tehran's information warfare campaign. The task force should recommend improvements to ongoing U.S. offensive and defensive information warfare measures focused on dismantling Tehran's information network in the United States.[127] If the administration fails to promptly establish the task force, Congress should require it.[128]
- **Implement a persistent campaign to designate and expose individuals and entities supporting the regime's information warfare efforts.** Washington's effort to designate entities associated with the Islamic Republic's information warfare campaign requires ongoing vigilance and maintenance as Tehran finds new ways to advance its objectives. The administration should ramp up efforts to designate persons and entities involved in Tehran's information warfare operations, especially those connected to the IRGC, using appropriate designation criteria. Congress should require an annual report from the U.S. Treasury on designations related to Iran's information warfare activities. It is essential that the designations be fully enforced. For example, satellite companies, web hosting services, and social media firms should not offer service to designated entities.[129]
- **Widen the effort.** The U.S. government should more effectively leverage the expertise and outreach of American private sector and nonprofit organizations to better inform policy and augment it with private action. Specifically, the U.S. government should establish better connections with the large number of Iranian-Americans who deplore the Islamic Republic and maintain ongoing connections within Iran.
- **Improve USAGM's broadcasts.** USAGM, including its PNN and Radio Farda services, is a primary component of the American response to Iran's information warfare efforts, but it is in dire need of additional congressional oversight and reform. Congress should press PNN and Radio Farda to regularly report the metrics by which they assess performance and impact. Congress should push PNN and Radio Farda to create more focused programming that better explains U.S. policy, scrutinizes the Islamist regime, and accurately covers actual conditions within Iran. U.S.-funded programming should include investigative journalism on topics such as regime corruption and human rights abuses as well as rapid responses to the regime's disinformation. Congress should require a report from USAGM assessing current levels of message penetration and proposed improvements. Lastly, Congress should designate an independent ombudsman fluent in Farsi to review coverage and investigate questions about impact, lack of context, and biased reporting.

127. At a minimum, experts and officials from the Department of State, Department of Defense, Department of Justice, Federal Bureau of Investigation, Central Intelligence Agency, and Department of the Treasury should participate.
128. Congress should mandate the administration provide a written and unclassified report with a classified annex that details Tehran's information warfare operations, assesses America's response, and proposes recommendations to strengthen U.S. information warfare efforts targeting the Islamic Republic. Congress may want to require the comptroller general to conduct an independent assessment as well.
129. This includes entities such as Press TV, IRIB, Tasnim News, Fars News, and Al-Mustafa University.

Conclusion

By Bradley Bowman

The governments of China, Russia, and Iran, despite their differences, understand that ideas and beliefs play a decisive role in shaping what individuals and nations support or oppose and ultimately determining which actions are taken or avoided. Armed with this understanding, Beijing, Moscow, and Tehran are waging a methodical information war campaign targeting three groups. The first and most important target audience for each regime is its own domestic population. The second target audience is Americans, the U.S. government, and its allies and partners. And the third is populations and governments in other countries where these regimes seek to obtain valuable strategic resources or concessions.

It might seem odd that the primary information warfare focus of Xi Jinping, Vladimir Putin, and Ali Khamenei is their own people. But when one considers the autocratic, authoritarian, and/or totalitarian natures of these regimes, it makes sense. Xi, Putin, and Khamenei must manipulate the flow of information to their people to maintain a monopoly on power. If a government does not enjoy the consent of the governed, the regime must attempt the Orwellian management of information to their oppressed peoples so that they submit to their subjugated state.

China, Russia, and Iran also focus their information warfare campaigns on Americans because they believe

the United States possesses a unique ability to challenge the regimes' oppression at home and aggression abroad[130] — more specifically, the *existence*, *potential*, and *power* of the United States directly challenge the regimes in Beijing, Moscow, and Tehran.

The mere *existence* of the United States (and its democratic allies) conveys to the people of China, Russia, and Iran that there is an appealing alternative to authoritarianism and autocracy. The regimes and their proxies sometimes respond by suggesting that democracy is inferior or that it cannot work in their respective regions. The former argument is rather predictable for authoritarians eager to retain their grip on power. The latter argument is decisively refuted by the existence of free peoples and democratic governments in Taiwan, Ukraine, and Israel. That explains some of the vitriol we see toward Taipei, Kyiv, and Jerusalem, respectively.

With these unflattering contrasts between tyranny at home and freedom nearby, the leaders of these three regimes should be concerned about the *potential* for the United States to adopt offensive information warfare operations in their countries. Such a campaign could systematically expose each regime's corruption and oppression and help the Chinese, Russian, and Iranian people advocate for their own rights, including more representative governance.[131] Much to the detriment of U.S. interests and the satisfaction of Xi, Putin, and Khamenei, successive U.S. administrations have resisted offensive information warfare efforts inside China, Russia, and Iran for fear of "provoking" them.

As made clear in this volume, Beijing, Moscow, and Tehran suffer from no such reluctance when it comes to aggressively waging information warfare inside the United States. These authoritarian regimes appear unconcerned about "provoking" the United States. The result is that the United States has failed to put up a fight, even as all three regimes wage aggressive information war in America. This is the equivalent of a kinetic war in which one combatant is relentlessly firing mortars, rockets, and missiles and the recipient of the strikes assiduously refuses to respond for fear of provoking an aggressor already launching salvos.

Skeptics of such arguments will no doubt express concern that aggressive U.S. offensive information warfare operations inside China, Russia, and Iran could spark a dangerous escalatory cycle. Curiously, such concerns often seem to emerge only when Americans awake to aggression against them and begin contemplating how to respond.[132]

Admittedly, such concerns about escalation are not entirely ridiculous. But these concerns must be weighed against the dangers associated with accepting the status quo in which China, Russia, and Iran are targeting with increasing ferocity and AI-empowered effectiveness[133] the socio-political foundations upon which American unity, stability, liberty, and security stand.

For too long, America has tried a strategy of inaction, at worst, and restraint, at best, when it comes to responding to information warfare aggression by China, Russia, and Iran. The results from this head-in-the-sand strategy are not good, and they will only get worse without change.

As a result of the ineffective U.S. information warfare defense and an arguably almost non-existent offense, Washington has failed to deter adversary offensive information warfare operations against Americans. That

130. Matt Pottinger, "Remarks by Matthew Pottinger at Parliamentary Intelligence-Security Forum in London," August 31, 2023. (https://www.fdd.org/analysis/2023/08/31/remarks-by-matthew-pottinger-at-parliamentary-intelligence-security-forum-in-london)
131. Mark Dubowitz, "Mapping Protests in Iran," *Foundation for Defense of Democracies,* May 29, 2024. (https://www.fdd.org/analysis/2023/01/27/mapping-the-protests-in-iran-2)
132. Fareed Zakaria, "On GPS: Does the US need a more confrontational China strategy?" *CNN,* April 28, 2024. (https://www.cnn.com/videos/world/2024/04/28/gps-0428-former-trump-aide-on-china-policy.cnn)
133. Russell Hanson, Adam R. Grissom, and Christopher A. Mouton, "The Future of Indo-Pacific Information Warfare: Challenges and Prospects from the Rise of AI," *RAND Corporation,* March 14, 2024. (https://www.rand.org/pubs/research_reports/RRA2205-1.html)

has left China, Russia, and Iran with the impression that they can wage war openly on Americans, our security, and our democracy with few consequences.

A call for aggressive offensive information warfare operations against China, Russia, and Iran is not a call for Washington to proactively use the U.S. military to conduct regime change. The U.S. experiences in Afghanistan and Iraq serve as a cautionary tale for those contemplating the preemptive use of U.S. military forces to topple any regime, not to mention a nuclear-armed great power adversary.

An American offensive information warfare campaign in China, Russia, and Iran focused on exposing corruption, lies, and oppression[134] and ensuring the respective populations know the truth regarding their regime's foreign and domestic policies is different. More importantly, if Beijing, Moscow, and Tehran don't like having to fend off offensive information warfare operations in their respective countries, perhaps that could prompt them to assess whether it is in their interest to continue information warfare operations against the United States.

Of course, these regimes also realize that American military *power* presents a serious impediment to their regional ambitions. Xi seeks to conquer Taiwan, Putin seeks to subjugate Ukraine, and Khamenei seeks to exterminate the State of Israel.[135] In each case, the United States is a leading obstacle to their expansionist aims. That is why each regime is focused on an information warfare strategy in the United States. They have two key objectives: 1) dividing Americans against one another or exacerbating existing tensions so that they are too distracted and weak[136] to project U.S. power abroad to defend their core interests[137]; and 2) deceiving Americans into believing that the United States has no interests in the outcomes in Taiwan, Ukraine, and Israel.[138]

"The United States can win this information war if it has the will to do so. The stakes could not be higher and there is no time to waste."

If unchallenged, these information warfare campaigns present a fundamental threat to the United States. These three regimes want to sideline American power as they target three of our most vital and vulnerable partners: Taiwan, Ukraine, and Israel.[139]

Of course, the problems and divisions in the United States cannot be blamed on America's adversaries. Unfortunately, Americans are quite adept at creating their own problems. But it would be dangerous to not recognize that Beijing, Moscow, and Tehran seek to exacerbate and magnify existing social-political fault lines to help pave the way for their wider ambitions.[140]

The final group targeted for information warfare is populations and governments in countries that are not necessarily allied with the United States, where the three regimes seek to obtain valuable strategic

134. "Executions Surge in Iran and Protests Persist," *Foundation for Defense of Democracies,* May 3, 2024. (https://www.fdd.org/analysis/2024/05/03/executions-surge-in-iran-as-protests-persist)
135. Bradley Bowman and Mira Resnick, "Reviving the Arsenal of Democracy," *Foreign Podicy,* May 17, 2024. (https://www.fdd.org/podcasts/2024/05/17/reviving-the-arsenal-of-democracy)
136. Ivana Stradner, "Russia Wants Texas to Secede," *Kyiv Post* (Ukraine), February 14, 2024. (https://www.fdd.org/analysis/2024/02/14/russia-wants-texas-to-secede)
137. Ivana Stradner, "Washington Needs to Fight Russia's Information War Using This Tactic," *Kyiv Post* (Ukraine), May 3, 2023. (https://www.fdd.org/analysis/2023/05/03/washington-needs-to-fight-russias-information-war-tactic)
138. Bradley Bowman and RADM (Ret.) Mark Montogomery, "Supporting America's Allies Puts America First," *National Review,* February 23, 2024. (https://www.fdd.org/analysis/op_eds/2024/02/23/supporting-americas-allies-puts-america-first)
139. Col. Hsu Min-Cheng, "Inoculating Society against Authoritarian Influence in the Digital Age: Fortifying the Barracks against Authoritarian Cognitive Warfare," *Air University, Journal of Indo-Pacific Affairs*, May 8, 2024. (https://www.airuniversity.af.edu/JIPA/Display/Article/3768526/inoculating-society-against-authoritarian-influence-in-the-digital-age-fortifyi)
140. Bradley Bowman and Maj. Shane Praiswater, "Great Power Competition Comes Home to America," *Defense One,* November 3, 2020. (https://www.defenseone.com/ideas/2020/11/great-power-competition-comes-home-america/169760)

resources or concessions.[141] Their focus is on parts of Asia as well as Africa and Latin America.[142] If the United States and its allies cede ground in these strategic countries due to a failure to counter adversary information warfare, the results will be serious. U.S. diplomatic, economic, and military interests will suffer, while Beijing, Moscow, and Tehran cultivate corrupt leaders who prey on the local population, destroy the environment, and slowly but surely undermine the U.S.-led world order.

Seen in this light, the information warfare waged by China, Russia, and Iran can seem overwhelming. To make matters worse, this axis of aggressors is more aligned than it has been in decades.[143]

But there are at least two reasons why Americans can be cautiously optimistic. First, the United States has an unparalleled network of capable allies that have capabilities in the information domain and coordinate with Washington to secure common interests.[144] In the July 11, 2023, Vilnius Summit Communique, all NATO members expressed concern regarding China and Russia's "disinformation" campaigns.[145] While a declaration is not a strategy, there exists a solid foundation on which to build.

A second reason for optimism is that America's constitutional system, the foundation of the U.S. government's power and a vital source of stability for Americans, is stronger and more resilient than the regimes of our authoritarian adversaries that rule through coercion and fear. Their inferior governance model is replete with weaknesses and vulnerabilities that can be exploited.

In this information war, Americans must become more agile. But in the rush to respond, however, Americans should not become like their adversaries. Rather than propagating lies and engaging in disinformation — the hallmarks of the regimes in Beijing, Moscow, and Tehran — U.S. information warfare operations should be grounded in truth. That will make U.S. efforts credible and effective. Tethering U.S. information warfare operations to the truth will also highlight the differences between autocrats willing to say anything to cling selfishly to power versus a democracy highlighting facts on behalf of the free people they represent and those suffering under the regimes they disdain.

But before better policies can be adopted, Americans must first wake up. A dangerous information war is already underway. The United States must adopt policies to better defend itself and begin to go on the offensive.

The United States can win this information war if it has the will to do so. The stakes could not be higher, and there is no time to waste.

---

141. Craig Singleton, "Mapping the Expansion of China's Global Military Footprint," *Foundation for Defense of Democracies,* April 30, 2024. (https://www.fdd.org/plaexpansion)

142. "Latin America's China Challenge: A Conversation with SOUTHCOM Commander General Laura Richardson," *Foundation for Defense of Democracies,* October 11, 2023. (https://www.fdd.org/events/2023/10/11/latin-americas-china-challenge-a-conversation-with-southcom-commander-general-laura-richardson)

143. Bradley Bowman and H.R. McMaster, "Supporting Ukraine and Israel will Help Deter Aggression Around the World," *Newsweek*, February 21, 2024. (https://www.newsweek.com/supporting-ukraine-israel-will-deter-aggression-around-world-opinion-1870864)

144. North Atlantic Treaty Organization, "Countering Hybrid Threats," March 7, 2024. (https://www.nato.int/cps/en/natohq/topics_156338.htm)

145. North Atlantic Treaty Organization "Vilnius Summit Communique: Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Vilnius 11 July 2023," July 11, 2023. (https://www.nato.int/cps/en/natohq/official_texts_217320.htm)

Acknowledgments

I want to thank Craig, Ivana, John, Mark, and Saeed for their excellent chapters. Their knowledge, experience, and professionalism made my job easier, and I genuinely appreciate their patience with me throughout this process. Their insights will help Americans better understand the information war that China, Russia, and Iran are waging against us. If some of these recommendations are adopted, the United States can begin to punch back more effectively in the information domain.

Thanks to Matt Armstrong for helping me refine my definition of information warfare and understand some of the relevant history and context. Students of strategy will recognize the ends-ways-means infrastructure undergirding the definition. Much of my thinking related to strategy was shaped by Cold War historian and Yale Professor John Lewis Gaddis as well as the late and great professor of ancient Greece and the Peloponnesian War Donald Kagan, under whom I studied in graduate school.

John Gray provided much-appreciated research support in the early stages of the project. Elizabeth Robbins provided useful feedback as well. I also want to thank the peer reviewers who took the time to scrutinize chapter drafts and offer constructive input.

Special thanks to Jonathan Schanzer and David Adesnik for their valuable suggestions that made the monograph more succinct and readable. Thanks also to David May for his diligence and support.

Allie Shisgal helped keep the project coordinated and moving forward, and Erin Blumenthal played an indispensable leadership role as always. Daniel Ackerman's creative genius is evident once again in the monograph's cover design.

Cover Illustration by Daniel Ackerman/FDD

About the Authors

Bradley Bowman

Monograph Editor

Bradley Bowman is senior director of FDD's Center on Military and Political Power. He has almost nine years of experience in the U.S. Senate, where he was a national security advisor to members of the Senate Armed Services and Foreign Relations Committees. He also served as an active-duty U.S. Army officer, Black Hawk pilot, staff officer in Afghanistan, Council on Foreign Relations international affairs fellow, and assistant professor at West Point, where he taught courses in grand strategy, American foreign policy, and American politics.

Mark Dubowitz

Mark Dubowitz is FDD's chief executive. Sanctioned by Iran in 2019 and Russia in 2022, he is widely recognized as a key influencer in shaping policies to counter the threats from the regime in Iran. According to *The New York Times*, "Mark Dubowitz's campaign to draw attention to what he saw as the flaws in the Iran nuclear deal has taken its place among the most consequential ever undertaken by a Washington think tank leader."

Saeed Ghasseminejad

Saeed Ghasseminejad is a senior Iran and financial economics advisor at FDD, where he specializes in Iran's economic and financial markets, sanctions, and illicit finance.

John Hardie

John Hardie serves as deputy director of FDD's Russia Program. His research focuses on Russian foreign and security policy, U.S. policy toward Russia and the post-Soviet space, and transatlantic relations.

Craig Singleton

Craig Singleton is a senior fellow at FDD, where he also serves as senior director of FDD's China program. He previously spent more than a decade as a senior U.S. diplomat, completing multiple overseas assignments in the Middle East, Latin America, and East Asia. While stationed in Washington, DC, Craig focused on developing policies aimed at confronting China's malign influence activities and North Korea's nuclear weapons program.

Ivana Stradner

Dr. Ivana Stradner serves as a research fellow with FDD's Barish Center for Media Integrity. She studies Russia's security strategies and military doctrines to understand how Russia uses information operations for strategic communication. Her work examines both the psychological and technical aspects of Russian information security.

About the Foundation for Defense of Democracies

The Foundation for Defense of Democracies (FDD) is a Washington, DC-based, nonpartisan policy institute focusing on foreign policy and national security. For more information, please visit www.fdd.org.

FDD's Barish Center for Media Integrity

FDD's Barish Center for Media Integrity addresses the national security threats posed by misinformation, disinformation campaigns, and influence operations waged by foreign adversaries against the United States and allied democracies.

FDD's Center on Military and Political Power

FDD's Center on Military and Political Power promotes understanding of the defense strategies, policies, and capabilities necessary to deter and defeat threats to the freedom, security, and prosperity of Americans and our allies, by providing rigorous, timely, and relevant research and analysis.

FDD's Center on Cyber and Technology Innovation

FDD's Center on Cyber and Technology Innovation (CCTI) seeks to advance U.S. prosperity and security through technology innovation while countering cyber threats that seek to diminish it. CCTI promotes a greater understanding within the U.S. government, private sector, and allied countries of the threats to and opportunities for national security presented by the rapidly expanding technological environment.

FDD
FOUNDATION FOR
DEFENSE OF DEMOCRACIES

P.O. Box 33249
Washington, DC 20033-3249
(202) 207-0190
www.fdd.org