The Information Instrument of Power: More Than an Enabling Afterthought



Word Count: 3841

A paper submitted to the Faculty of the United States Naval War College, Newport, RI in partial satisfaction of the requirements of the Department of Joint Military Operations. DISTRIBUTION A. Approved for public release: distribution unlimited. The contents of this paper reflect the author's own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

REPORT DOCUMENTATION PAGE					Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD- 26-04-2021	MM-YYYY) 2	R. REPORT TYPE	INAL		DATES COVERED (From - To) N/A
4. TITLE AND SUBTITL	E		an Enabling Afterthought	-	a. CONTRACT NUMBER /A
The Informati	ion Instrument of Pa	wer• More Than a			D. GRANT NUMBER
				5	C. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)					d. PROJECT NUMBER /A
Rebecca F. Russo, Lt	Col, USAF				e. TASK NUMBER /A
				. WORK UNIT NUMBER /A	
7. PERFORMING ORG	D ADDRESS(ES)		8	PERFORMING ORGANIZATION REPORT NUMBER	
Writing & Tea Naval War Co	ter		N	/A	
686 Cushing F Newport, RI 0					
9. SPONSORING/MONI	TORING AGENCY NAMI	E(S) AND ADDRESS(ES)			D. SPONSOR/MONITOR'S ACRONYM(S) //A
					1. SPONSOR/MONITOR'S REPORT UMBER(S)
			N	/A	
12. DISTRIBUTION / AVAILABILITY STATEMENT Distribution Statement A: Approved for public release; Distribution is unlimited.					
13. SUPPLEMENTARY NOTES A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the curriculum. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.					
14. ABSTRACT Due to great power competition resurgence, the United States has worked to secure the country through a balanced approach of all instruments of national power (diplomatic, informational, military, economic (DIME)). However, because information and its environment are so complex, the United States has lagged in effectively using the information instrument of power (IOP) in a comprehensive, orchestrated manner. This ineffective usage of the information instrument is due to the lack of a holistic understanding of information and how it is wielded for power, the absence of a comprehensive national strategy, and inadequate orchestration with other instruments of power. Unless the United States develops a better shared understanding of the information dimension, it will continue to be outmaneuvered by its adversaries in the informational domain. Additionally, the United States requires a comprehensive and deliberate information strategy with actionable items at the national level covering connectivity, content, and cognition. Furthermore, it would greatly benefit from a single orchestrator of the information IOP that sits on the National Security Council or a better-empowered lead agency to provide a more whole-of-nation approach. In doing so, the United States will be more secure and better prepared to compete against its adversaries in this complicated and volatile space.					
15. SUBJECT TERMS (Key words) Information, Instrument of Power, Information Strategy, DIME, Cognition					
16. SECURITY CLASSI		· · ·	17. LIMITATION	18. NUMBER	19a. NAME OF RESPONSIBLE PERSON
a. REPORT UNCLASSIFIED	b. ABSTRACT UNCLASSIFIED	c. THIS PAGE UNCLASSIFIED	OF ABSTRACT	OF PAGES	Director, Writing Center 19b. TELEPHONE NUMBER (include area code) 401-841-6499

Standard Form 298 (Rev. 8-98)

INTRODUCTION

Due to great power competition resurgence, the United States has worked to secure the country through a balanced approach of all instruments of national power (diplomatic, informational, military, economic (DIME)). However, because information and its environment are so complex, the United States has lagged in effectively using the information instrument of power (IOP) in a comprehensive, orchestrated manner. This ineffective usage of the information instrument is due to the lack of a holistic understanding of information and how it is wielded for power, the absence of a comprehensive national strategy, and inadequate orchestration with other instruments of power.

The United States' security is at risk because it ineffectively utilizes the information IOP while adversaries such as Russia and China increasingly exploit this domain. This gives Russia and China a significant advantage by undermining the democratic values of a free and open society, which the United States tries to exemplify and project world-wide. To overcome this, the United States needs to reinvigorate its narrative and distribute it far and wide as part of a national information strategy.¹ The goal of this strategy would be to outline a proactive, whole-of-nation approach to actively protect against and counter its adversaries' subversive tactics in the information domain. By doing so, the United States lessens the likelihood of adversaries sowing distrust, confusion, and internal strife within the American public, institutions, and global audiences while protecting democracies, economies, and the Liberal International Order (LIO) writ large.

¹ John Arquilla and Douglas A. Borer, *Information Strategy and Warfare: A Guide to Theory and Practice* (New York: Routledge, 2009), 237-238.

POWER AND ITS INSTRUMENTS

A nation's use of power to compel or persuade others is often accepted as "the ability to influence the behavior of others to achieve a desired outcome."² International Relations (IR) expert Edward Carr offered three categories of political power: " (a) military power, (b) economic power, (c) power over opinion."³ Furthermore, IR practitioners and academics refined the categories to delineate and reduce the instruments' complexity.⁴ However, this simplification altered Carr's original premise and distilled the instruments into mechanisms and capabilities often aligned with agencies or departments, instead of the instruments themselves.⁵ The origins of monikers such as DIME and MIDLIFE (military, informational, diplomatic, law enforcement, intelligence, financial, and economic) represent accepted categorizations, but there is no single, agreed-upon list.⁶ In this analysis, DIME will be the categorization method in the interest of simplicity, its wide acceptance, and to stay closer to the historical context of an instrument versus a capability or mechanism of power.⁷

Much like the IOPs, there is no single, shared definition of information, information environment, or information warfare.⁸ This lack of definitions creates incredible complexity, open to misunderstanding and misuse. The Department of Defense (DoD) states, "the information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. This environment consists of three interrelated dimensions that continuously interact with individuals, organizations, and systems. These

² Edward Hallett Carr 1892-1982, *The Twenty Years' Crisis, 1919-1939: An Introduction to the Study of International Relations* (London: Macmillan & co. ltd, 1946), 1-21.

³ Carr, *The Twenty Years' Crisis*, 108.

⁴ D. Robert Worley, Orchestrating the Instruments of Power: A Critical Examination of the U.S. National Security System (Raleigh: Lulu Press, 2012), 275-276.

⁵ Worley, Orchestrating the Instruments of Power, 275-276.

⁶ Worley, Orchestrating the Instruments of Power, 275.

⁷ Worley, Orchestrating the Instruments of Power, 275-291.

⁸ Catherine A. Theohary, "Information Warfare: Issues for Congress," (Federation of American Scientists, 2018), 1.

dimensions are the physical, informational, and cognitive."⁹ Offered differently by subject matter experts Dennis Murphy and Daniel Kuehl, the information dimensions are termed "connectivity (the ability to exchange information), content (the actual information), and the cognitive effect (the impact of human beliefs)."¹⁰ Using Murphy and Kuehl's framework, one can reason that these three dimensions, in combination with the previous definition of power, yield a more comprehensive version of information power as "the use of informational content and the technologies and capabilities that enable the exchange of that content, used globally to influence the social, political, economic or military behavior of human beings, whether one or one billion in the support of national security objectives."¹¹ This definition drives an important distinction that information is not only a key enabler of the other instruments, but also an instrument itself. This distinction explains why adversaries are so effective in this space. They can target small audiences and influence human cognition, allow it to spread through social mediums, and ultimately influence political and economic environments to undermine the United States' security apparatus. Adversaries appear to know and manipulate the collective American psyche better than the United States knows how to, placing it at a strategic disadvantage.

LACK OF COMPREHENSIVE STRATEGY

The United States' lack of a comprehensive information strategy contributes to its continued underutilization of the information IOP. The strategy is both unbalanced and incomplete in terms of incorporating components of connectivity, content, and cognition at the national level. Russia and China's aggressive and effective maneuvering in the information

⁹ Joint Chiefs of Staff, Doctrine for the Armed Forces of the United States, JP 3-13 (Washington, DC: Joint Chiefs of Staff, 2014), I-1.

¹⁰ Dennis Murphy and Daniel Kuehl, "The Case for a National Information Strategy," *Military Review* 95, no. 5 (2015), 72-73. ¹¹ Murphy and Kuehl, "The Case for a National Information Strategy," 72.

space exacerbates the United States' underperformance and narrow focus on defensive and reactive measures and undermines the American value of a free and open digital society.

First, the current national strategy is unbalanced because it views information only as an enabler of the other instruments. The 2018 National Security Strategy (NSS) exhibits an increased focus on information and influence, but the default instrument is still military power.¹² This default is evident through the DoD's extensive budget, large mission set, and force size relative to State or Treasury departments. Because of this imbalance, it is common for government officials to automatically associate the information instrument of power with operational level military information operations or the Department of State's role in public diplomacy.¹³ However, this narrow view is flawed. United States' informational power is much more than that.¹⁴ Additionally, the DoD is not the only agency trying to defend against human cognition manipulation, making it ill-equipped to be the primary source of power at the strategic level of information warfare.

Second, the NSS is also incomplete within the information instrument of power. The NSS still favors the connectivity dimension of the information environment with an emphasis on cyberspace. The release of the 2018 National Cybersecurity Strategy signals deference to connectivity without adequate concern for content and cognition that would allow the United Stated to employ information intentionally.¹⁵ The title of Pillar IV of the 2018 NSS, Advance American Influence, might lead one to believe that information's cognitive dimension is at the forefront of the United States' strategy. Yet, the ways and means of influence primarily focus on

¹² William J. Burns, "The Lost Art of American Diplomacy: Can the State Department be Saved?" *Foreign Affairs* (*New York, N.Y.*) 98, no. 3 (2019), 98.

¹³ Theohary, "Information Warfare: Issues for Congress", 1-7.

¹⁴ Donald M. Bishop, "DIME, Not DiME: Time to Align the Instruments of U.S. Informational Power," The Strategy Bridge (The Strategy Bridge, June 22, 2018).

¹⁵ Kevin Truitte, "An American National Information Security Strategy," Georgetown Security Studies Review, July 29, 2019.

diplomatic, economic, and military capabilities except "protecting a free and open internet."¹⁶ The current strategy has historical underpinnings from the 1999 RAND study that suggested the American information strategy should revolve around "guarded openness."¹⁷ However, that foundational study failed to account fully for the manipulative cognitive aspect of the environment. Additionally, RAND identified a severe tendency to focus on securing the technological aspects of connection vice a comprehensive approach, including sharing ideas and influencing the psyche.¹⁸ This disparity exists based on the country's admission of tepid and fragmented attempts at countering information exploitation.¹⁹ Furthermore, the United States' priority actions (ways) are focused on "understanding how adversaries gain informational and psychological advantages across all policies," not necessarily how to counter them. A free and open society makes it incredibly difficult to use connectivity as the sole means of maintaining and gaining power over opinion. Vulnerabilities can always be exploited, so the best way to counter such a strategy is through a strong and widely distributed narrative that affects the human psyche. Until the United States develops a more comprehensive information strategy around content and cognition, including domestic needs, adversaries such as Russia and China will continue to sow distrust and confusion.

Russia created a distinct strategic advantage in the information domain at all levels. Its strategy focuses on offensive techniques targeting democratic populations' collective cognition while manipulating or creating false information.²⁰ Russia also looks for an adversary's whole-

¹⁶ U.S. President, *The National Security Strategy of the United States of America* (Washington, DC: White House, 2017), p 41.

¹⁷ John Arquilla et al., *The Emergence of Noopolitik*, Toward an American Information Strategy, 1st ed. (Santa Monica, CA: Rand, 1999), 5.

¹⁸ John Arquilla et al., *The Emergence of Noopolitik*, 2-3.

¹⁹ U.S. President, *The National Security Strategy of the United States of America* (Washington, DC: White House, 2017), p 35.

²⁰ Marcel H. van Herpen 1945, *Putin's Propaganda Machine: Soft Power and Russian Foreign Policy* (Lanham: Rowman & Littlefield, 2016), 1-19.

of-nation vulnerabilities to create confusion and public distrust, thereby undermining the very functions of democracy.²¹ This strategy and a pronounced understanding of free and open societies led to Russia's highly effective disinformation campaign against the United States during the 2016 presidential election. Conversely, the United States unbalanced and incomplete strategy failed to counter Russia's offensive propaganda effectively. It caused decision-makers to question their authorities and options because of impinging on Constitutional rights to free speech.²² The United States' strategy is heavily focused on keeping Russia out of the technical space versus out of American minds and is a losing proposition. There will always be technical vulnerabilities. Moreover, the best technical capabilities in an intangible domain cannot overcome strategic cognitive shortcomings.²³ A national strategy that combines technical defenses and aggressive truth campaigns with efforts to prevent adversaries from manipulating information will provide a more holistic approach to countering wide-spread disinformation.

China's information strategy is also outperforming the United States'. China is less aggressive in trying to influence specific events such as the United States' elections. However, China's strategy and focus on cultural and informational influence have involved more insidious and dishonest methods to pressure persons and organizations in an effort to cause confusion and deception.²⁴ China's efforts to target universities, think tanks, the Chinese American community, businesses, and media shows the breadth of their strategy to use information in the form of soft power to gain a regional and global advantage.²⁵ Alarmingly, China's efforts focus

²¹ James Andrew Lewis, "Can We Compete in Cyberspace?" Center for Strategic and International Studies, November 2, 2020.

 ²² Joseph Menn, "U.S. Government Loses to Russia's Disinformation Campaign: Advisers," *Reuters*-12-21, 2016.
²³ Lewis, "Can we Compete in Cyberspace?"

²⁴ Larry Jay Diamond and Orville Schell, *China's Influence & American Interests: Promoting Constructive Vigilance: Report of the Working Group on Chinese Influence Activities in the United States* (Stanford, CA: Hoover Institution Press, 2019), 2.

²⁵ Diamond and Schell, Chinese Influence & American Interests, 5.

on the technology education sector, where they use traditional theft and espionage to alter data or introduce cognitive errors to influence decision-makers.²⁶ This goes well beyond Russia's tactics of influence and is alarming, especially since the United States has been slow to counter China.²⁷ It is not to say that the United States should move to a strategy like China and harshly censor a free and open society.²⁸ Instead, it is necessary to find innovative ways to counter China's technological and cognitive, sympathy-seeking tactics that can slow the information differential gradually eroding values of American democracy. A more comprehensive strategy and better shared understanding in the information domain are just two of the necessary elements required to allow the United States to wield the information instrument more effectively. It also needs to focus on orchestrating information at the national level.

STRATEGIC ORCHESTRATION

The United States lacks a single person or entity that orchestrates the information instrument of power effectively at the national level. The National Security Council consists of the President, Vice President, Secretary of State, Secretary of the Treasury, Secretary of Defense, the Assistant to the President for National Security Affairs, the Chairman of the Joint Chiefs of Staff, and the Director of National Intelligence (DNI).²⁹ Based on that listing, the strategic level head or lead agency for each IOP except information is in attendance: State for diplomacy, Defense for military, and Treasury for economic. There is a significant interagency overlap with these entities and their instruments of power. For example, within the economic IOP, the Department of Treasury coordinates and enforces economic sanctions. The DoD provides

²⁶ Theohary, "Information Warfare: Issues for Congress", 11.

²⁷ Diamond and Schell, Chinese Influence & American Interests, 4-5.

²⁸ Lewis, "Can we Compete in Cyberspace?"

²⁹ "National Security Council," The White House (The United States Government, January 18, 2021), https://www.whitehouse.gov/nsc/.

foreign military assistance, and the United States Agency for International Development provides foreign aid, but all under the State Department's guidance. Still, the President has an advisor that closely aligns with each of the IOPs except information. Intelligence and information are not the same; therefore, one should not ascertain that the DNI is the lead for information. Intelligence is focused on collecting and analyzing information based on the prioritized needs of decision-makers.³⁰ Other entities generally perform actions based on that intelligence. Intelligence is an integral part of information but does not include the broader information connectivity and proactive content dimension.

This raises the question of who coordinates information at the national level? The answer is that no one is focused on it, and the interagency processes for coordination in this domain are broken.³¹ The United States also fails to effectively coordinate with the private sector and inform the American public to ensure a whole-of-nation approach to one of the most pressing threats facing its free and open society. Since companies and individuals can participate actively and passively in society's social, economic, and political aspects, they can be both targets and perpetrators in disinformation campaigns.³² It is crucial that the American narrative reaches its population to counter efforts to change the beliefs and behaviors from adversarial disinformation.³³ The recent addition of the Office of Public Engagement (OPE) is a step in the right direction.³⁴ Research shows that the best way to counter disinformation is through the

³⁰ Mark M. Lowenthal, Intelligence: From Secrets to Policy (Thousand Oaks, California: SAGE/CQ Press, 2020) 38-40.

³¹ Worley, Orchestrating the Instruments of Power, 434.

³² Gabriel Cederberg et al., *National Counter-Information Operations Strategy* (Belfer Center for Science and International Affairs: Harvard Kennedy School Belfer Center, 2019) 4-5.

³³ Arquilla and Borer, Information Strategy and Warfare, 57.

³⁴ "Office of Public Engagement," The White House (The United States Government, January 18, 2021), https://www.whitehouse.gov/ope/.

timely release of credible evidence to the contrary.³⁵ Therefore, the OPE will only be as effective as the proactive narrative it creates and distributes and is incorporated into the national security structure to release timely counter-evidence to disinformation campaigns.

Some might argue that the State Department is the lead for information after the dissolution of the United States Information Agency (USIA) in 1999, at the end of the Cold War.³⁶ However, the mission of the USIA focused on supporting "national interests abroad through information dissemination."³⁷ The State Department's Global Engagement Center (GEC) is home to many of the same missions today.³⁸ Yet, the GEC lacks a clear mission and authority of all the other information operations outside the Bureau of Public Diplomacy and Public Affairs.³⁹ Others might suggest that DoD is the lead for information since it has the bulk of capabilities and information operations resources. However, "Title 10 U.S.C 2241 prohibits DoD from domestic publicity or propaganda," so informing and educating the American public and private sector would be well outside its authority and scope.⁴⁰ These disparate missions and lack of authorities indicate that no person or entity is orchestrating the information IOP, creating a disjointed approach.

Some may also suggest that the government has taken tremendous steps to work with the private sector by developing the National Council for Information Sharing and Analysis Centers. Although these centers are improvements in open-source sharing, they primarily focus on physical and cyber threats to critical infrastructure and lack content and cognition considerations

³⁵ Linda Robinson et al., Modern Political Warfare: Current Practices and Possible Responses (Santa Monica, Calif: RAND Corporation, 2018) 229.

 ³⁶ Theohary, "Information Warfare: Issues for Congress", 7.
³⁷ Theohary, "Information Warfare: Issues for Congress", 7.

 ³⁸ Theohary, "Information Warfare: Issues for Congress", 7.
³⁹ Theohary, "Information Warfare: Issues for Congress", 7.

⁴⁰ Theohary, "Information Warfare: Issues for Congress", 7-8.

of the other dimensions of information.⁴¹ Lastly, one might consider the Department of Homeland Security as the lead for information, but it is equally under-resourced and lacks strategic oversight of the other agencies."42 The United States requires orchestration at the national level to employ the comprehensive dimensions of the information IOP, both domestically and internationally, or risk being further outperformed by its adversaries. The decision space will only grow more complicated as technologies advance and populations become more globalized.

RECOMMENDATIONS

America must forcefully reinject itself into the global information domain. Specifically, the United States must create a holistic understanding of information and its dimensions, develop a comprehensive national-level Information Strategy, and develop a position on the National Security Council that oversees and orchestrates the information IOP with a whole-of-nation approach.

Creating a shared understanding amongst domestic and international agencies and educating the American public on how to work securely and prevent manipulation in the information domain is the first step in becoming more effective in utilizing the instrument.⁴³ This is hard and controversial, but necessary. A set of recognized terms across agencies and a public campaign to inform the American people of the dangers of misinformation, disinformation, and propaganda would be a starting point. Americans must be able to authenticate information, and unless the government steps into this gap, disinformation campaigns will continue to be widely effective.⁴⁴ Educating the American public about these

 ⁴¹ "National Council of ISACs," accessed Jan 16, 2021, https://www.nationalisacs.org.
⁴² Truitte, "An American National Information Security Strategy,".

⁴³ Kimberly Underwood, "A New Front in Information Warfare," *SIGNAL Magazine*, 1 May 2018.

⁴⁴ Underwood, "A New Front in Information Warfare."

topics, as early as grade school, could model public health efforts to share facts, reporting measures, and standard methods to spot bad information.⁴⁵ With the welcome addition of the Office of Public engagement, the administration should also reinvigorate the U.S. Agency for Global Media (USAGM) with an initial focus on Radio Free Europe/Asia and Voice of America.⁴⁶ This structure already exists and would provide an easy way for the United States to reassert itself in the information domain.⁴⁷ Careful attention should be given to expanding USAGM tools to spread the American message rapidly and broadly. With this element of shared understanding underway, the United States can then focus on a deliberate strategy.

The United States needs a national information strategy. Up until this point, strategies have focused on the defense of the technical dimension. As outlined in the book, *Information Strategy and Warfare*, "Strategic influence must be offensive and not reactive...unless the enemy makes a strategic mistake, the best that can be hoped for in a defensive campaign is a tie."⁴⁸ Ties in the information domain do not guarantee a free and open society for the United States, democratic partners, and aspiring nations alike. Today's misinformation and disinformation environment will make it unlikely that any Russian or Chinese strategic information mistake will have a detrimental impact on themselves. Therefore, adversaries should be publicly admonished for their poor behavior and the strategy must include counter-information options while upholding American values of a free and open society.⁴⁹ This approach must include the American public, academia, the private sector, and government

⁴⁵ Gabriel Cederberg et al., *National Counter-Information Operations Strategy* 4-7, 11-12.; "Ensuring the Digital Way of Life in e-Estonia - e-Estonia," e, April 4, 2018, https://e-estonia.com/digital-way-life-e-estonia/.

⁴⁶ "United States Agency for Global Media," USAGM, accessed November 25, 2020, https://www.usagm.gov/whowe-are/mission/.

⁴⁷ Bishop, "DIME, Not DiME: Time to Align the Instruments of U.S. Informational Power."

⁴⁸ Arquilla and Borer, *Information Strategy and Warfare*, 60.

⁴⁹ Gabriel Cederberg et al., *National Counter-Information Operations Strategy* (Belfer Center for Science and International Affairs: Harvard Kennedy School Belfer Center, 2019), 4-5.

organizations at every level with a goal of speed and accuracy of validating and publicizing information. Specifically, a strategy should include: a focused narrative on the importance of democracy and the Liberal International Order (content/cognition), goals to distribute the narrative domestically and internationally while disrupting an adversary's message (connectivity/cognition), continued protection of the mediums through which messaging flows (connectivity), deceiving the adversary at the time and place of our choosing.⁵⁰

Finally, the United States would benefit from an NSC-level advisor and orchestrator of the information strategy or a designated lead agency with the authorities required to match ways and means to strategic ends. The country needs someone dedicated to thinking about connectivity, content, and cognition. It is likely a bridge too far to create an entire entity on par with the other departments due to cost. Thus far, research does not support a complete functional consolidation of the information IOP. If provisions exist for an entity focused on the information IOP, the mission set should not be limited to USIA of old concepts.⁵¹ The new agency should include all three dimensions and include both external and domestic strategies for countering its adversaries in the information domain. With these three improvements, the United States can gain ground against its adversaries and better prepare for the challenges of ever-changing and innovating technologies such as machine learning, artificial intelligence, and deep fakes that will further complicate the information domain.⁵²

CONCLUSION

The United States' standing as the sole superpower is waning. Its customary focus on the military, diplomatic, and economic instruments of power will further undermine its superpower

 ⁵⁰ Arquilla and Borer, Information Strategy and Warfare, 1.
⁵¹ Matthew Armstrong, "No, We Do Not Need to Revive the U.S. Information Agency," War on the Rocks, November 12, 2015.

⁵² Alina Polyakova Chris Meserole, "Disinformation Wars," Foreign Policy, May 25, 2018.

status unless its grand strategy utilizes the information instrument of power more effectively. Great Power adversaries such as Russia and China are using their nationally coordinated information strategy more effectively to wield informational power and take advantage of the western openness to advance their global status. Unless the United States develops a better shared understanding of the information dimension, it will continue to be outmaneuvered by its adversaries in the informational domain. Additionally, the United States requires a comprehensive and deliberate information strategy with actionable items at the national level covering connectivity, content, and cognition. Furthermore, it would greatly benefit from a single orchestrator of the information IOP that sits on the National Security Council or a betterempowered lead agency to provide a more whole-of-nation approach. In doing so, the United States will be more secure and better prepared to compete against its adversaries in this complicated and volatile space.

BIBLIOGRAPHY

- "Ensuring the Digital Way of Life in E-Estonia.", last modified -12-20T15:49:16+00:00. Accessed 25 November 2020, https://e-estonia.com/digital-way-life-e-estonia/.
- "Joint Publication 3-13: Information Operations." *Cyber Warfare : A Documentary and Reference Guide*, 2020. https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/12102012_io1.pdf

"National Council of ISACs." Accessed Jan 16, 2021, https://www.nationalisacs.org.

- "National Security Council." The White House. The United States Government, January 18, 2021. Accessed Jan 16, 2021, https://www.whitehouse.gov/nsc/.
- "Office of Public Engagement." The White House. The United States Government, January 18, 2021. Accessed January 20, 2021. https://www.whitehouse.gov/ope/.
- "United States Agency for Global Media." USAGM. Accessed November 25, 2020. https://www.usagm.gov/who-we-are/mission/.
- Armstrong, Matthew. "No, We Do Not Need to Revive the U.S. Information Agency." War on the Rocks, 2015, Accessed 25 November 2020, https://warontherocks.com/2015/11/no-we-do-not-need-to-revive-the-u-s-information-agency/.
- Arquilla, John and Douglas A. Borer 1962. 2007. *Information Strategy and Warfare: A Guide to Theory and Practice*. New York: Routledge.
- Arquilla, Ronfeldt. The Emergence of Noopolitik: Toward An American Information Strategy. The Emergence of Noopolitik. 1st ed. Santa Monica: RAND Corporation, 1999. doi:10.7249/mr1033osd.
- Bishop, Donald. "DIME, Not DiME: Time to Align the Instruments of U.S. Informational Power.", last modified June 20, Accessed 25 November 2020, https://thestrategybridge.org/the-bridge/2018/6/20/dime-not-dime-time-to-align-theinstruments-of-us-informational-power.
- Blank, Stephen. "Russian Information Warfare as Domestic Counterinsurgency," American foreign policy interests 35, 35, no. 1 (2013): 31–44. https://doi.org/10.1080/10803920.2013.757946.
- Burns, William J. "The Lost Art of American Diplomacy: Can the State Department Be Saved?" Foreign affairs (New York, N.Y.) 98, 98, no. 3 (2019): 98.
- Carr, Edward Hallett. The Twenty Years' Crisis, 1919-1939; an Introduction to the Study of International Relations London: Macmillan & co. ltd, 1946.

- Cederberg, Gabriel, Jordan D'Amato, Corinna Fehst, Simon Jones, Kunal Kothari, Aleksandra Milcheva, and Irene Solaiman. "National Counter-Information Operations Strategy." Belfer Center for Science and International Affairs. Belfer Center for Science and International Affairs: Harvard Kennedy School Belfer Center, February 2019. Accessed 25 November 2020, https://www.belfercenter.org/publication/national-counter-information-operationsstrategy.
- Colgan, Jeff D. "Three Visions of International Order," The Washington quarterly 42, 42, no. 2 (2019): 85–98. https://doi.org/10.1080/0163660X.2019.1621657.
- Condliffe, J. B. 1944. "Economic Power as an Instrument of National Policy." *The American Economic Review* 34 (1): 305-314. Accessed 25 November 2020, https://www.jstor.org/stable/1818703?seq=1
- Cordesman, Anthony H. 2019. *China's New 2019 Defense White Paper*: Center for Strategic and International Studies, Accessed 25 November 2020, https://www.csis.org/analysis/chinas-new-2019-defense-white-paper.
- Diamond, Schell. *China's Influence and American Interests: Promoting Constructive Vigilance. China's Influence and American Interests.* Chicago: Hoover Institution Press, 2019. Accessed 25 November 2020, https://www.hoover.org/sites/default/files/research/docs/diamond-schell_corrected-april2020finalfile.pdf.
- Herpen, Marcel H. van, 1945. 2016. Putin's Propaganda Machine: Soft Power and Russian Foreign Policy. Lanham: Rowman & Littlefield.
- Kozloski, Robert. "The Information Domain as an Element of National Power," Strategic Insights, v. 8, Issue 1, 2009. Accessed 25 November 2020, https://www.hsdl.org/?abstract&did=232244.
- Lewis, James A. "Can we Compete in Cyberspace?", last modified 2 November, accessed Jan 16, 2021, https://www.csis.org/analysis/can-we-compete-cyberspace.
- Lowenthal, Mark M. "The U.S. Intelligence Community," Chapter 3 in Intelligence: From Secrets to Policy (CQ Press, 2019), pp. 37-66.
- Mazarr, Michael J., Astrid Stuth Cevallos, Miranda Priebe, Andrew Radin, and Kathleen Reedy. Measuring the Health of the Liberal International Order. Santa Monica, Calif: Rand Corporation, 2017.
- Menn, Joseph. 2016. "U.S. Government Loses to Russia's Disinformation Campaign: Advisers." *Reuters*, -12-21. Accessed 25 November 2020, https://www.reuters.com/article/us-usa-russia-disinformation-analysis-idUSKBN1492PA.

- Meserole, Chris and Alina Polyakova. 2018. *The West is Ill-Prepared for the Wave of "deep Fakes" that Artificial Intelligence could Unleash*. Washington: The Brookings Institution. Accessed 25 November 2020, https://www.brookings.edu/blog/order-from-chaos/2018/05/25/the-west-is-ill-prepared-for-the-wave-of-deep-fakes-that-artificial-intelligence-could-unleash/.
- Mills, James H. and Danelle Barrett. 2015. "Harnessing Information Power: Leveraging Information Dominance Warfare as an Instrument of Naval Power." *Chips (Norfolk, Va.)*.
- Murphy, Dennis and Daniel Kuehl. 2015. "The Case for a National Information Strategy." *Military Review* 95 (5). Accessed 25 November 2020, https://www.armyupress.army.mil/Portals/7/militaryreview/Archives/English/MilitaryReview_20151031_art013.pdf#:~:text=The%20Case%20f or%20a%20National%20Information%20Strategy%20Col.,Strategy%20in%20the%2021st %20Century,%20but%20better%20known.
- Robinson, Linda, Todd C. Helmus, Raphael S. Cohen, Alireza Nader, Andrew Radin, Madeline Magnuson, and Katya Migacheva. Modern Political Warfare : Current Practices and Possible Responses. Santa Monica, Calif: RAND Corporation, 2018.
- Theohary, Catherine A. 2018. *Information Warfare: Issues for Congress*: Federation of American Scientists. https://fas.org/sgp/crs/natsec/R45142.pdf
- Truitte, Kevin. "An American National Information Security Strategy." Georgetown Security Studies Review, 2019. Accessed 25 November 2020, https://georgetownsecuritystudiesreview.org/2019/03/11/an-american-national-information-security-strategy/.
- Underwood, Kimberly. 2018. "A New Front in Information Warfare." *SIGNAL Magazine*, 1 May. Accessed 25 November 2020, https://www.afcea.org/content/new-front-informationwarfare-0.
- U.S. Department of Defense. Summary of The National Defense Strategy of the United States of America (Washington, DC: 2018).
- U.S. President. *The National Cyber Strategy of the United States of America* (Washington, DC: White House, 2018).
- U.S. President. *The National Security Strategy of the United States of America* (Washington, DC: White House, 2017).
- Worley, D. Robert 1949. 2012. Orchestrating the Instruments of Power: A Critical Examination of the U.S. National Security System. Raleigh: Lulu Press.