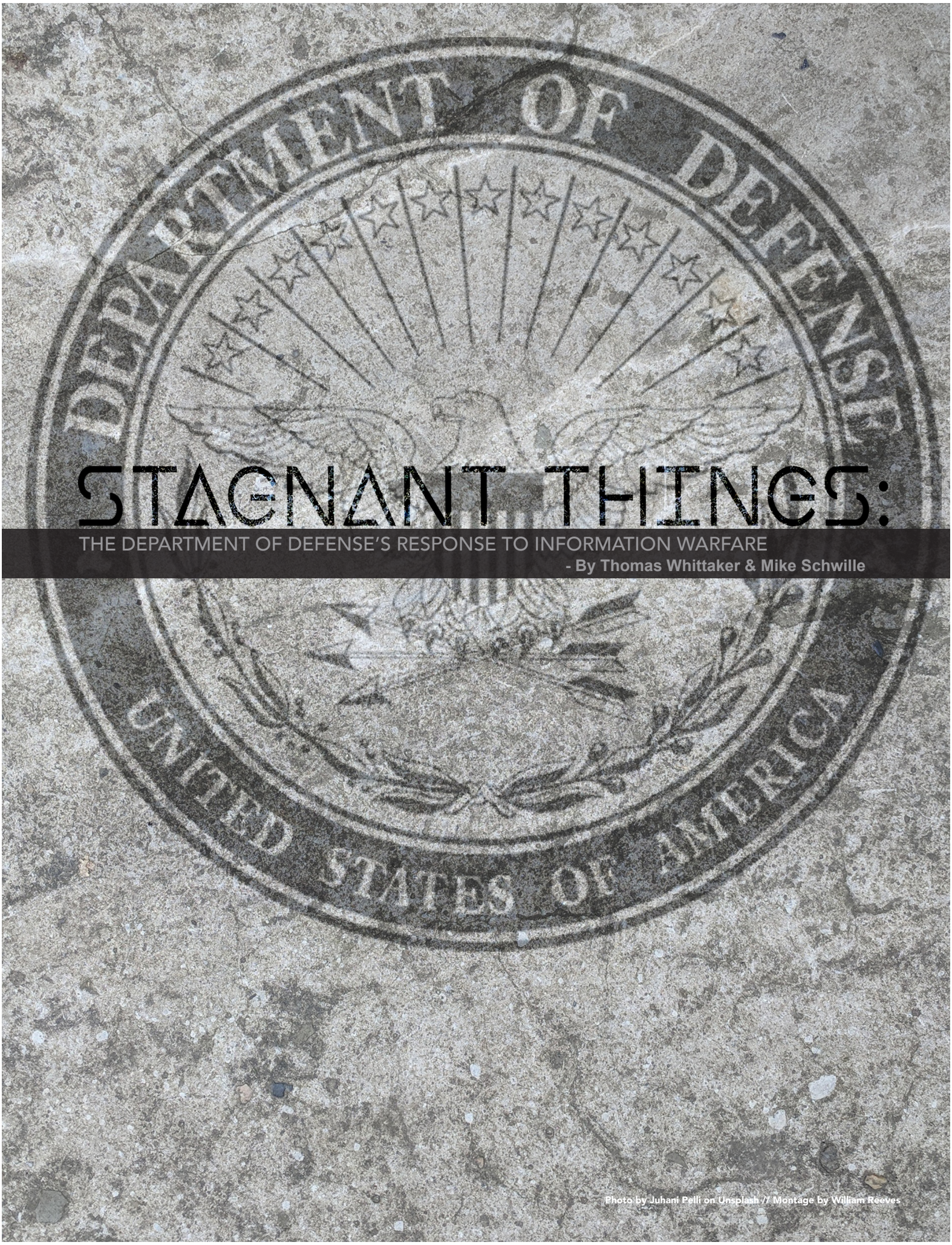



# STAGNANT THINGS:

## THE DEPARTMENT OF DEFENSE'S RESPONSE TO INFORMATION WARFARE

- By Thomas Whittaker & Mike Schwille

Photo by Juhani Pelli on Unsplash // Montage by William Reeves


## OVERVIEW

The information environment — too often a buzzword for defense technology firms and military academics — is the highly energetic arena where foreign adversaries and non-state actors alike shape the narrative of the great power competition.

Adversaries engage in operations in the information environment (OIE) as part of strategic posturing, to gain and maintain influence, and to project national power. Nations like China and Russia leverage their centralized governmental and military structures, as well as sociocultural predispositions, to create systems and tactics that enable them to adeptly exploit this space. Their tighter control on instruments of national power enables them to deliver influence with agility and speed. This strategic advantage begs the question: What has the United States done to develop and implement a whole-of-government response to compete effectively in the information environment?

## THE NEED

The evolving landscape of social media networks, web-based communications, and other technological advances offers an arsenal of low-cost of entry capabilities through which a user can influence global audiences.

Modern communications technologies empower American adversaries by providing efficient, flexible mechanisms through which adversaries can foster strategic narratives, transmit disinformation and propaganda, and shape global perceptions to their advantage.

Case in point: in 2018, the United States indicted 13 Russian individuals and three companies for providing support to the Kremlin-backed Internet Research Agency (IRA). According to the House Intelligence Committee, more than 126 million Americans had been exposed to content created by the IRA and more than 288 million impressions were linked to content generated by Russian Twitter bots.[138] More concerningly, Russian military operations in Ukraine have demonstrated the campaign-level successes of integrating physical and informational power to influence soldiers on the front line.

This is not a new concept for Russia, which has continually modernized and refined its concepts of "*dezinformatsiya*" and "active measures." The term, *dezinformatsiya*, meaning "disinformation," traces its lineage back to the Russian empire of the early 1900s.[139] So-called active measures have existed since the beginning of the Cold War and serve to influence global attitudes, values, and beliefs toward outcomes more favorable to Russian interests.

China is also using a modern interpretation of an even older strategic construct around exercising informational power for advantage and influence to achieve military objectives. In 2003, Beijing started to formalize this approach as the "Three Warfares" concept. The approach advises on the application of legal, public opinion, and psychological warfare to achieve desired effects against an adversary.[140] Adding to the problem are concerns that China and Russia are borrowing techniques from each other to bolster their respective approaches to OIE.[141]

### What are the **Three WARFARES**?

### Overview

- China's **Three Warfares** 三种战争 or shortened to 三战 *san zhan* are complementary, asymmetric, concurrent campaigns to win without fighting.
- Approval in 2003 by China's Communist Party, Central Committee and the Central Military Commission indicates support from Party, Government and Military – three main levers of power.
- Specific details in Chapter 2, Section 18 of Chinese People's Liberation Army Political Work Regulations.
- **Psychological Warfare** 心里战争 *xinli zhanzheng*
- **Media Warfare** 舆论战争 *yulun zhanzheng NOTE:* more correctly translated as public opinion warfare
- **Legal Warfare** 法律战争 *falv zhanzheng*

## CONGRESSIONAL PRIORITIZATION AND TREATMENT

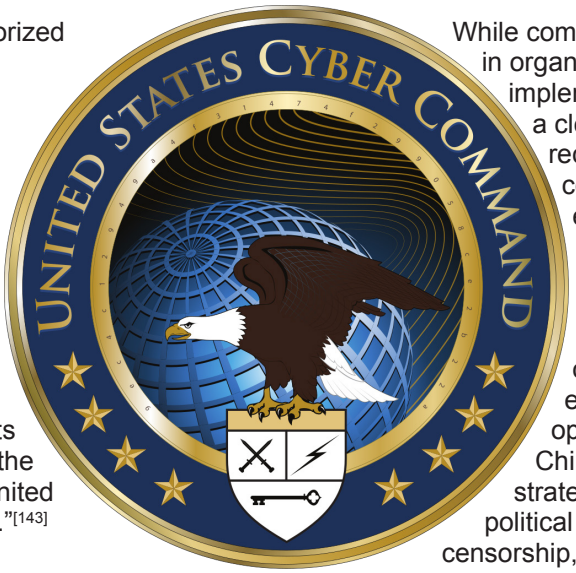
American democratic principles and values give primacy to the role of Congress in shaping the instruments of national defense and strategy. The National Defense Authorization Act (NDAA) is an annual Congressional bill that authorizes spending and sets defense policies for the Department of Defense (DoD). The NDAA is where the rubber meets the road for prioritization across the spectrum of defense programs and military operations.

Looking at the last six years of NDAAs, Congressional decisions have produced some noteworthy steps toward forming the building blocks of a more integrated DoD/interagency plan of action for OIE. Nevertheless, when these five NDAAs are analyzed as a whole, the story flow makes evident some concerning patterns: while

prioritization has been increasingly directed, the concrete development and implementation of DoD OIE strategy has yet to be effectively activated by DoD.


In general, NDAA 17 was relatively quiet on a direct treatment of the OIE issue. However, this NDAA provisioned and empowered key players in the information space. Perhaps most significantly, Section 923 established a unified combatant command for cyber operations, U.S. Cyber Command (USCYBERCOM). NDAA 17 further granted the command with authorities comparable in flexibility to those of U.S. Special Operations Command.[142] In addition to the traditional responsibilities levied on a combatant command to develop strategy, doctrine, and tactics, this legislation further empowered USCYBERCOM with authorities to organize, train, and equip the force.

Beyond the DoD, Section 1287 authorized defense resourcing for the Global Engagement Center (GEC), a newly minted player established in 2016 by Executive Order in the Department of State. The GEC's original focus was on counterterrorism-related messaging and communications. The mission of the GEC has since evolved into a broader coordination of federal and interagency efforts "to recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining or influencing the policies, security, or stability of the United States, its allies, and partner nations."[143]





NDAA 18 brought a more direct treatment of the OIE issue, albeit mostly under the legacy term of information operations. Building upon the increasing momentum of USCYBERCOM, Section 1637 brought a particular focus on fusing the cross-cutting elements within cyber operations with OIE.[144] As detailed in the bill, this legislation required the secretary of defense to establish processes and procedures for the integration of "strategic information operations and cyber-enabled information operations."[145] This bill further required that a senior DoD official be designated to lead efforts in development and oversight of strategy, policy, and guidance, as well as to sustain ongoing efforts (such as DoD coordination with the GEC). It directed concrete efforts toward the development of requirements and planning for OIE, driving down new strategy formation responsibilities to the combatant command level.

This legislation also established a 180-day timeline for delivery of an implementation plan of DoD strategy for OIE. As defined in the NDAA, this implementation plan would require the DoD to determine and define its own roles and responsibilities within a whole-of-government approach, including efforts to create defined actions, establish performance metrics, determine implementation requirements, and project timelines for execution of all tasks contained within the DoD OIE strategy.


Compared to its predecessors, NDAA 19 did not generate new guidance for a whole-of-government response. Section 1069 directed a check on actions taken and resources needed for cyber-enabled information operations. Similarly, Section 1632 provided clarifications on the secretary of defense's authority to conduct "military activities or operations in cyberspace short of hostilities," including information operations.[146]

While comparatively silent on progression in organizational alignment or implementation action, NDAA 19 took a clear position on the imperative to recognize and respond to global competition within the information environment, with a particular interest in defending against Russian and Chinese activities. Section 1248 directed the DoD to focus training activities in Europe on responding to adversary cyber electronic warfare and information operations. Section 1261 called for a China-focused strategy that included strategic assessments on "the use of political influence, information operations, censorship, and propaganda to undermine democratic institutions and processes, and the freedoms of speech, expression, press, and academic thought."[147] Similarly, Section 1642 called for "Active Defense" in cyberspace against the Russian Federation, the People's Republic of China, as well as North Korea and Iran.


NDAA 20 reinvigorated many elements contained in NDAA 18. Section 1631 established the DoD Principal Information Operations Advisor (PIOA) to assert senior DoD leadership over OIE. The PIOA assumed the role of "oversight of policy, strategy, planning, resource management, operational considerations, personnel, and technology development across all the elements of information operations of the Department."[148] The position and its additionally defined responsibilities bore much similarity to those levied upon the defense secretary in NDAA 2018. Similarly, we find another reversion to precedent direction on strategy and implementation.

The newly appointed PIOA was tasked with development and updates to the DoD strategy for OIE; a review of DoD posture in OIE; management of joint training and OIE lexicon; and a determination on the combat capabilities to be included in related activities.

This legislation reflected a heightened degree of desired accountability to DoD efforts, with newly defined responsibilities, new congressional reporting requirements, and defined timelines for updates. The undeniably repetitive quality of the 2020 NDAA, coupled with the more nuanced provision regarding common treatment of related DoD lexicon, reflected telling signs of a prevailing issue: The DoD's struggle to implement precedent NDAA guidance.


Like its predecessor, the 2021 NDAA revealed continued difficulties in implementation, most notably in Section 1749, appropriately titled, "Implementation of Information Operations Matters." This section delivered a vigorous forcing function to a stagnating DoD posture in OIE. The first unfulfilled Congressional report was required to provide an overview of the structuring and manning of information operations capabilities and forces across the DoD.[149] Similarly, NDAA 20 had directed the completion and reporting of a "Strategy and Posture Review" for the purpose of developing an OIE strategy. Both reports had been directed in Section 1631 of NDAA 20 and were not yet complete as of NDAA 21.

Interestingly, the 2021 NDAA also called for the designation of a DoD entity to "develop, apply, and continually refine an assessment capability for defining and measuring the impact of Department information operations, which entity shall be organizationally independent of Department components performing or otherwise engaged in operational support to Department information operations."[150]

Whereas military actions conducted in the traditional warfighting domains usually result in discernable and objective impacts, OIE operations do not easily fit in the template for a standard battle damage assessment. As a result, they present a true head-scratcher for determining what actions exceed the threat threshold of competition, short of armed conflict. The second- and third-order effects of OIE cannot be discounted, so what does it look like to effectively assess cause and effect as strategic messaging becomes manifest in attitudes, values, beliefs, and behaviors?


NDAA 22 continues to call for more action by DoD to include and fund OIE efforts. Section 1049 is yet another follow-up to NDAA 18 Section 1631. However, it now limits the use of funds until DoD completes the posture review of the information environment. Section 1504 and Section 1509 call for an evaluation of the DoD cyber governance and an assessment of a cyber posture to include the integration and coordination with OIE. These sections call on the DoD to increase its ability to conduct cyber operations and OIE.

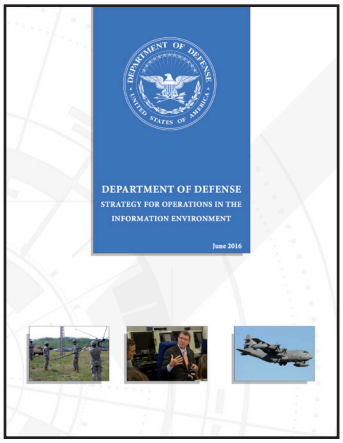
## THE DOD RESPONSE

Despite highly engaged adversaries and mounting pressure from Congress to act, the DoD has been slow to generate real momentum regarding OIE. And so, the multi-billion-dollar question: what has the DoD accomplished?

Without a clear path forward for implementation and action, the DoD has failed to realize the full gains of OIE. Nevertheless, the storyline of efforts to this point merit acknowledgement. Arguably, the most proactive steps the DoD has taken toward strategy and implementation were manifested in three efforts: the DoD Strategy for Operations in the Information Environment (2016); the addition of information as a joint function (2017); and the Joint Concept for Operating in the Information Environment (2018).[151]

## STRATEGY FOR OPERATIONS IN THE INFORMATION ENVIRONMENT

The 2016 Strategy for Operations in the Information Environment (SOIE) acknowledged the need to integrate OIE through all levels of command, but more importantly, it recognized the need to facilitate DoD support of the whole-of-government effort. Published more than six years ago, the document identified 15 task areas across people, programs, policies, and partnerships as the path forward for the DoD. It also provided a desired end-state: "[t]hrough operations, actions, and activities in the information environment, DoD has the ability to affect the decision-making and behavior of adversaries and designated others to gain advantage across the range of military operations."[152]




To meet this end-state, it described several activities that must take place. Initially, the SOIE sought to develop necessary changes to DoD policy, doctrine, and professional military education efforts. These actions aimed to align processes to conduct OIE and prepare the organization for broader integration within the government. The SOIE then sought to enhance organizational structures and capabilities responsible for the conduct of OIE. It focused on concept development, policy and authorities, and the creation of new modes for interagency coordination to "facilitate effective DoD operations in the information environment." [153]

Finally, the SOIE outlined the goals for OIE throughout the DoD, with the intent of achieving a normalization of

posture and organizational readiness within the whole-of-government effort to exercise informational power. In this phase, the SOIE sets the goal of sustaining "a well-trained, educated, and ready IO and total-force to meet emerging requirements."[154]

## THE INFORMATION JOINT FUNCTION

In July 2017, General Joseph F. Dunford, Jr., (then-chairman of the joint chiefs of staff) approved an update to Joint Publication (JP) 1, "Doctrine for the Armed Forces of the United States." This major doctrinal update elevated "information" to the level of a seventh joint function, alongside the traditionally established joint functions of command and control (C2), intelligence, fires, movement and maneuver, protection, and sustainment. The joint functions are a group of related capabilities and activities that help synchronize, integrate, and direct joint operations.[155] This update marked the first time a new forcing function was created and indicates the level of importance that DoD assigned to the role information.

The creation of the "Information Joint Function" demonstrated a concrete step toward increasing the importance of information within the DoD and remains a significant doctrinal update for the treatment of OIE. By including this change in the bedrock doctrine of JP 1, the DoD created a new forcing function which prioritizes "information" alongside with other joint functions. More specifically, this development delivers a strong foundation for generating momentum and normalization across the military services in the integration of information.[156] While it was a much-needed step, by itself, the elevation of information to a joint function isn't enough to address the policy, organizational, and educational deficiencies related to OIE.

## JOINT CONCEPT FOR OPERATING IN THE INFORMATION ENVIRONMENT

The 2018 Joint Concept for Operating in the Information Environment (JCOIE) represented an important element of the OIE storyline — it demonstrated continued commitment of the DoD to acknowledge the phased development timeline and desired outcomes of the SOIE. The JCOIE prescribed three primary areas that that must be pursued in order to achieve desired outcomes: (1) Understand information, the informational aspects of military activities, and informational power; (2) Institutionalize the integration of physical and informational power; (3) Operationalize the integration of physical and informational power.[157] The JCOIE provided a further overview of concept-required capabilities needed to support the outcomes. This included a broad scope of requirements with clear implications for future DoD resourcing, acquisition, and authorities.

While the JCOIE clearly recognized the need for developing capabilities and mechanisms to make better sense of the information environment and the impacts of operations therein, many of the requirements have yet to be fulfilled.

## ADDRESSING THE REAL CHALLENGES

In many ways, the raw materials for a cohesive DoD and whole-of-government approach to OIE are already there. So why haven't the existing efforts amounted to effective implementation and integration?

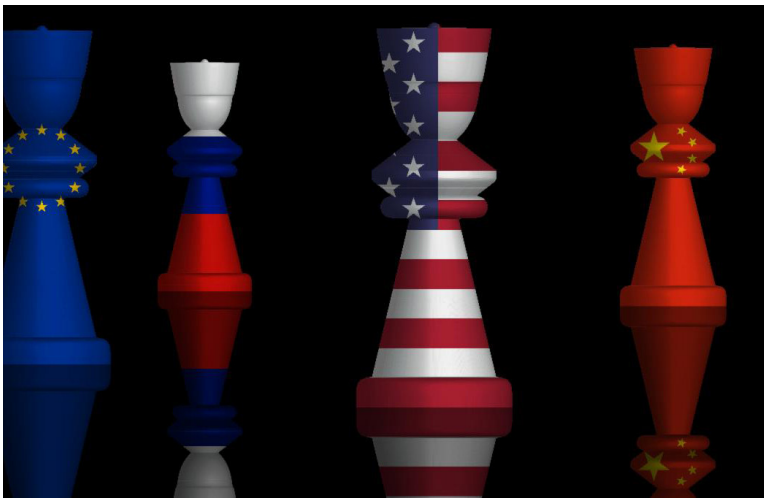
The DoD has become a victim of its own design. As stated in the Joint Concept for Operations in the Information Environment, the DoD has been "hampered by its policies, conventions, cultural mindsets, and approaches to information, has built barriers fostering a disconnected approach to conducting activities in and through a pervasive information environment."[158] The DoD largely acclimated to conducting OIE against asymmetric threats, most obviously in the vein of counterterrorism.

Frankly, the multi-dimensional use of information capabilities by great power competitors and near-peer adversaries has caught the DoD off guard. To be sure, the implications of great power competition within the information space are not an altogether new arena for the DoD. Nevertheless, decades of conflict against terrorist groups and other non-state actors have stagnated the DoD playbook for OIE and hindered the development of the required capabilities needed to execute it. Now, the DoD must compete in a more global information fight against bigger players and faster technology, with more dire consequences. This requires tanks, planes, and ships to confront U.S. adversaries. Yet, it hasn't much affected budgeting requests by the military services to fund the creation of organizations and capabilities directed toward OIE.

While the Marine Corps has created the Marine Information Group, the Air Force has created the 16th Air Force (its own Information Warfare organization), and the Army and Navy have developed increasingly detailed concepts (Information Advantage and Information Dominance, respectively), these efforts are just a drop in the bucket of the individual military service budgets. The development of real OIE capabilities will require a more substantial portion of these budgets to adequately address capability shortfalls. Even as the geographic combatant commands request forces trained and equipped to conduct OIE, the military services have yet to fully invest in the development of these capabilities.

Frankly, the multi-dimensional use of information capabilities by great power competitors and near-peer adversaries has caught the DoD off guard.

Limited understanding and a low-risk tolerance for OIE are two additional reasons more substantial progress has not been made toward institutionalizing OIE. There is a clear lack of training and education for the joint force to truly answer "What is OIE?" and "How does OIE directly contribute to a commander's mission?"



Given the obvious concerns over unintended consequences of information campaigns, there is a prevailing sense that the DoD needs to predict and understand the potential second- and third-order effects of OIE more fully. However, OIE goes far beyond second- and third-order effects, as impacts extend into the infinite cycle of human consciousness. The expectation that OIE outcomes can be fully calculated is a Sisyphean pursuit that will only result in continued inaction by the United States. The DoD needs to accept the fact that there will always be risk involved in the information fight, as is the case with all military operations. We should take some comfort that U.S. adversaries also bear the consequences for failed OIE. The DoD should be willing to determine (and accept) a true sense of risk tolerance within OIE.

Moving forward, the DoD should focus on building the capability to alleviate the tensions over risk tolerance. As identified in the JCOIE and in NDAA 21, DoD needs to augment its ability to better understand the dynamics and activities of the information environment. More specifically, the DoD needs a more integrated enterprise capability that fuses data streams from across all relevant communications forums of the global information environment to provide a real-time insight on trends in human attitudes, values, beliefs, and behavior.

Partnerships and programs (as defined in the SOIE) are key to the execution of DoD strategy. The U.S. private sector remains a largely untapped player in this space. While adversarial nations enjoy a certain degree of flexibility from centralized structures where tech industries and military apparatuses are joined, the U.S. free market society enables a unique environment for technological advancement. The DoD and government writ large should seek to capitalize on the ability of the U.S. private sector to innovate in ways that our adversaries political and economic systems cannot. Leading American tech firms possess innovative artificial intelligence and machine learning capabilities that could offer a means to detect, collect, analyze, and respond to actions in the information environment.

In this capability, the DoD should connect across the federal space and private sector to obtain, integrate, and operationalize data sources that provide high fidelity into global human interactions. When enabled by algorithmic and analytic tools, these data can be used to provide insights in behavioral modeling across the scope of potential target audiences and to identify patterns and trends in prevailing strategic, operational, and tactical narratives as they relate to political, military, economic, and social systems. By responding to the clear need for this capability (as mandated in NDAA 21 and requested under CPCs in the JCOIE), the DoD may succeed in breaking the biggest logjam to an effective DoD response for OIE.

---

**[138]** "Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements," *U.S. House of Representatives Permanent Select Committee on Intelligence*, https://intelligence.house.gov/social-media-content/ (accessed February 11, 2022).
**[139]** Aristedes Mahairas and Mikhail Dvilyanski, "Disinformation – Дезинформация (Dezinformatsiya)," *The Cyber Defense Review* 3 (3) (2018): 21–28. https://www.jstor.org/stable/26554993.
**[140]** Peter Mattis, "China's Three Warfares in Perspective," *War on the Rocks*, January 30, 2018, https://warontherocks.com/2018/01/chinas-three-warfares-perspective/.
**[141]** Daniel Kliman, Andrea Kendall-Taylor, Kristine Lee, Joshua Fitt, and Carisa Nietsche, "Dangerous Synergies: Countering Chinese and Russian Digital Influence Operations," *Center for New American Security*, May 2020, https://www.cnas.org/publications/reports/dangerous-synergies.
**[142]** Charley Snider and Michael Sulmeyer, "Decoding the 2017 NDAA's Provisions on DoD Cyber Operations," *Lawfare Blog*, January 30, 2017, < https://www.lawfareblog.com/decoding-2017-ndaas-provisions-dod-cyber-operations > (accessed February 11, 2022); *National Defense Authorization Act for Fiscal Year 2017*, 114th Cong., Public Law No. 114-328, December 23, 2016, S.2943, https://www.congress.gov/bill/114th-congress/senate-bill/2943.
**[143]** "Global Engagement Center: Core Mission & Vision," *U.S. Department of State*, https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/global-engagement-center/ (accessed February 11, 2022).
**[144]** *National Defense Authorization Act for Fiscal Year 2018*, 115th Cong., 1st Session, Public Law No. 115-91, December 12, 2017, H.R. 2810, https://www.congress.gov/bill/115th-congress/house-bill/2810.
**[145]** Ibid.
**[146]** *John S. McCain National Defense Authorization Act for Fiscal Year 2019*, 115th Cong., 2nd Session, Public Law No. 115-232, August 13, 2018, H.R. 5515, https://www.congress.gov/bill/115th-congress/house-bill/5515.
**[147]** Ibid.
**[148]** *National Defense Authorization Act for Fiscal Year 2020*, 116th Cong., 1st Session, Public Law No. 116-92, December 20, 2019, S. 1790, https://www.congress.gov/bill/116th-congress/senate-bill/1790.
**[149]** *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*, 116th Cong., 1st Session, Public Law No. 116-283, (last modified) January 1, 2021 H.R. 6395, https://www.congress.gov/bill/116th-congress/house-bill/6395.
**[150]** Ibid.
**[151]** "Strategy For Operations In The Information Environment," *U.S. Department of Defense*, June 2016, https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf; Joint Concept for Operating in the Information Environment (JCOIE), *U.S. Joint Chiefs of Staff*, July 25, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf.
**[152]** Ibid.
**[153]** Ibid.
**[154]** At of the time of this article, the DoD is rewriting the SOIE because 1) the document is six years old and 2) many of the stated goals and objectives of the SOIE were not met.
**[155]** DOD Dictionary of Military and Associated Terms, *U.S. Department of Defense*, November 2021, https://www.supremecourt.gov/opinions/URLs_Cited/OT2021/21A477/21A477-1.pdf.
**[156]** Christopher Paul, "Is It Time to Abandon the Term Information Operations?," *The Rand Blog*, < https://www.rand.org/blog/2019/03/is-it-time-to-abandon-the-term-information-operations.html> (accessed February 12, 2022).
**[157]** "Joint Concept for Operating in the Information Environment (JCOIE)," *U.S. Joint Chiefs of Staff*.
**[158]** Ibid.

Thomas Whittaker is an operations researcher and defense consultant. His primary research and areas have included Operations in the Information Environment, Psychological Operations, strategic communications, and behavioral science. As a defense contractor, he has worked in various research and consultancy roles in support to the Department of Defense, intelligence community, and the U.S. Army special operations community. He is a U.S. Army reservist qualified in the Psychological Operations field. Mr. Whittaker is currently completing his M.S. in National Security from Liberty University and received his B.A. in Political Science from Grove City College.

Mike Schwille is senior policy analyst at RAND. His primary research interest focuses on the integration of information into combined arms warfare. He has experience with Joint, Army and Marine Corps concept development, Operations in the Information Environment, countering A2AD strategies, strategic workforce analysis and force development. While at RAND, he has led projects relating to Information Operations Intelligence Integration, the creation of the Army's Information concept, and tactically focused Information Operations. He also has intelligence community and military experience focusing on target development, mapping social and cultural networks, and building partner capacity. He is qualified as a Civil Affairs, Psychological Operations and Information Operations Army Reservist and has deployed multiple times with the U.S. Army to the Middle East and Africa. He earned his M.A. in international development studies from George Washington University.