Journal of Strategic Security

Volume 12 | Number 4 Article 4

The Future of Strategic Information and Cyber-Enabled Information Operations

Ben Hatch
United States Air Force, benjamin.hatch@yahoo.com

pp. 69-89

Recommended Citation
Hatch, Ben. "The Future of Strategic Information and Cyber-Enabled Information Operations." *Journal of Strategic Security* 12, no. 4 (2019) : 69-89.
DOI: https://doi.org/10.5038/1944-0472.12.4.1735
Available at: https://scholarcommons.usf.edu/jss/vol12/iss4/4

The Future of Strategic Information and Cyber-Enabled Information Operations

Abstract

To prepare for future challenges across the continuum of conflict, the United States (US) must optimize how it manages, counters, defends, and exploits the effects of information by organizing for strategic information and cyber-enabled information operations across and through multiple domains. Currently, information related capabilities are fielded across the United States Government (USG) among multiple organizations and agencies, and therefore lack efficiencies normally gained through combined action, unity of command, and unity of effort. In considering a solution to these challenges, this study examines historic and current examples of successful information operations to show organization matters, and reviews options to organize for future engagements. The methodology used to conclude a new approach is necessary is patterned after a 1941 study on production requirements for the US to enter World War II. This article similarly considers answers to related questions, and shows the creation of an organization and the designation of a senior official responsible for strategic information and cyber-enabled information operations empowers the nation to integrate, synchronize, and harmonize activities pursuant to a national and defense information strategy, thereby making the joint force more lethal, and posturing the USG for dominance in the information environment.

Acknowledgements

I would like to thank Dr. John Geis, Director, Airpower Research Task Force, Air War College, Air University, Maxwell AFB, AL, for his advice, guidance, and assistance in developing this article. Your efforts have helped shape a generation of defense thinkers.

Introduction

Russian cyber-enabled influence and information operations have a proven record of challenging United States and NATO interests. Over the past few years, Russia has conducted a global influence campaign using the Internet and social media assessed to be the most successful in history.[1] Russia refined its thinking on strategic influence in places like Crimea and Georgia, where it had created a hybrid approach to conventional warfare. Employing a whole of government effort, Russia leverages its military and intelligence capabilities to conduct global strategic influence operations, which includes the exploitation of online media platforms, financial support to criminal organizations, and the use of propaganda to shape international opinion and counter perceived Western influence attempts.[2] The Stockholm International Peace Research project found Russia spent $61.4 billion on defense in 2018, which was sixth in the world.[3] Of their total budget, Russia dedicates an estimated $400–$500 million annually on its foreign information efforts.[4]

A January 2018 U.S. Senate report chronicled Russian disinformation efforts in 19 countries.[5] Russia has focused operations not only against the United States and NATO members, but also former Soviet States, and in Syria, where it has integrated and synchronized its online activity with its information campaign to project power and advance Putin's political goals.[6] In the Brexit case alone, University of California at Berkeley research identified 150,000 Twitter accounts with ties to Russia that disseminated messages in favor of Britain leaving the European Union (EU).[7] Polling before the vote indicated a majority of British citizens wished to remain a part of the EU; however, the final vote was closer, with 51.9 percent of the votes to leave with 48.1 percent voting to remain.[8] Strategists anticipate that Russia will continue to evolve its information capabilities to affect friendly, neutral, or hostile audiences.[9] Hence, the Brexit example clearly presage that Russia's use of information will continue to destabilize and weaken United States interests globally if unchecked.

In addition to Russia, the threat from other foreign information operations is increasing. Research published in the Washington Post cites Iran, Saudi Arabia, China, Israel, Venezuela and others as employing influence operations across borders to advance geopolitical goals.[10] Former

Secretary of the Air Force Heather Wilson identified information operations as a rising threat that requires the Pentagon's focus. "Our adversaries are often better at shaping the perception of what's going on than we are…Russia and China are better at that than we are because we just don't think that way," she said in May 2019.[11]

The effectiveness of a government's information capabilities is a reflection of how it is organized. The United States Government (USG) and DoD oftentimes struggle to organize for information and cyber-enabled information campaigns that would afford decision makers flexible options to advance and defend political ideals. Frequently, the USG holds its vast information capabilities in uncoordinated stovepipes, and misses potential strategic advantages gained through combined action, unity of command, and unity of effort.[12] Russia has overcome these organizational barriers, and according to RAND analyst Bruce McClintock, "The Russian information operations system, combined with the Russian form of centralized government control, allows it to launch cyber-operations with greater speed, agility, and brazenness than most analysts believe is possible in the West."[13]

The United States must improve its ability to compete in the information environment. The methodology used here to examine what improvements are required follows a pattern of inquiries similar to those employed in Major Albert Wedemeyer's 1941 study to estimate production requirements for the United States to enter World War II.[14] His thinking was in order to know how to organize for the future, he had to know what missions the military would execute. Therefore, Maj Wedemeyer turned his attention to understanding national policy, linking the strategic end state to an estimate for increased military capacity. This article similarly considers answers to a series of questions:

1. What is the national objective of the United States when it comes to information operations and cyber-enabled information operations?
2. What strategy will accomplish the national objective?
3. What organizational construct is necessary to execute the strategy?
4. What resources are required to execute the strategy?
5. What is necessary to constitute, equip, and train those forces?

https://scholarcommons.usf.edu/jss/vol12/iss4/4
DOI: https://doi.org/10.5038/1944-0472.12.4.1735

The first two questions have answers in existing guidance. The national objective for strategic information operations has the broad definition of informing and shaping the perceptions of specific audiences in order to gain or maintain a competitive advantage.[15] The 2016 *DoD Strategy for Operations in the Information Environment* provides a roadmap to achieve the national objective.[16]

This article focuses on questions 3-5. In order to answer how the DoD should organize for and execute strategic operations in the information environment, a historical review is necessary. It will help frame the problem and illuminate lessons that should apply towards preparing for future approaches. To this end, this article will begin by discussing case studies to provide an organizational framework for strategic influence. It will then offer recommendations for an organizational construct to enable the USG to win future information wars.

Organization Matters

History illustrates the value of an organized capability to conduct and defend against strategic information operations. The British during World War II established an organization for controlling the dissemination of specific information to the Germans.[17] The design of the British system included centralized control of the strategic influence initiative focusing on the employment of turned foreign agents and other human sources. According to J.C. Masterman, the W. Board, comprised of Britain's senior leaders, specifically the three directors of intelligence, Chief of the Security Service, and the head of the B. Division in M.I.5 (similar to the U.S. Federal Bureau of Investigations), oversaw the strategic direction of plans and operations using agents as information pathways to deliver select messages to desired recipients. Subordinate to the W. Board, the Twenty Committee (XX Committee) oversaw the general day-to-day management of the specific operations, and became the focal point for all information transmitted to the enemy. Masterman stressed that the British successfully used this system to integrate and synchronize information used to steer German thinking and behavior in part because there was a section dedicated to the special work.[18] In other words, there was centralized control of the system, but also decentralized execution through multiple departments. Such a model highlights that a government's ability to engage in strategic information operations is most successful when there is

an integrated organizational and operational construct, with access to strategic levels of government, to manage influence operations conducted across multiple agencies, departments, and domains.

Documents recovered from the archives of the Stasi secret police and East Germany's Politburo highlights a similar approach employed by the Soviets during the Cold War.[19] At the time, General Ivan Ivanovich Agayants, the first director of the KGB Disinformation Department, devised an information operation to suggest the resurgence of Nazism in order to generate fear and distrust of West Germans.[20] Soviet agents painted swastikas and anti-Semitic slogans on synagogues and other buildings in major cities worldwide. The global response was damaging to West Germany. Some viewed the paintings as representative of a rising tide of Nazism, and leading newspapers published articles along this theme. It also marginalized West German diplomats. There were economic impacts as storeowners removed German goods from stores and supervisors fired German employees. Religious leaders viewed the anti-Sematic messages as "proof that the German nation had not overcome its past."[21] In an act that suggested the potential fracturing of post-World War II alliances, some questioned if West Germany could be trusted as a NATO member. Author John Barron, in his book *KGB: The Secret Work of Soviet Secret Agents*, wrote the practice of Russian disinformation and organized deception is a "legacy of Lenin imbedded in Soviet custom," and the use of information operations remained an instrument consistent with Soviet national policy.[22] Therefore, information operations from the Russian perspective remain calculated in a systematic approach to mislead, confound, or inflame foreign opinion.

More recently, there have been isolated attempts within the U.S. Defense Department to posture organizational resources to fight effectively in the information domain. For example, in the global conflict against the Islamic State, one combatant command implemented a reorganization to integrate and synchronize lethal and non-lethal effects, notably by aligning Information Related Capabilities (IRCs) previously located and managed by leaders in their J2, J3, and J6 offices under a single advocate for information operations in the operations division (J3). A senior defense official noted, "We must be organized properly" to be effective at information operations.[23] This example shows that organization was the

https://scholarcommons.usf.edu/jss/vol12/iss4/4
DOI: https://doi.org/10.5038/1944-0472.12.4.1735

solution to harmonize the effects of multiple strategic communication tools found in otherwise disjointed and stove-piped IRCs.

The British, Soviet experiences, and the Islamic State example illustrate that strategic information operations are more successful when an organization dedicated to information related activities, both offensive and defensive, is responsible for management and oversight of the operations. The World War II and Cold War examples show that when centrally managed, information operations inform and shape specific audience perceptions in order to gain a competitive advantage. The United States presently lacks a unified framework to identify, defend, counter, integrate, and synchronize its available information capabilities for multi domain operations, and it should consider a new organizational construct to address these challenges in the future.

Preparing for the Strategic Future

The Joint Staff in the Joint Operating Environment (JOE) 2035 predicted future activities would include adversaries focused on espousing or reinforcing information warfare and propaganda efforts with military action.[24] Cyber intelligence consultant Emilio Iasiello cites Russian strategists who stress information warfare "will be the starting point of every action now called the new-type of warfare (a hybrid war) in which broad use will be made of the mass media and, where feasible, the global computer networks (blogs, various social networks, and other resources)."[25] These future activities will not be limited to state actors, such as Russia. The U.S. Marine Corps security environment forecast for 2030-2045 envisioned that "information operations and strategic communication as part of a whole-of-government approach will grow in importance."[26] Even non-state actors in the future will "wage a propaganda war on terms far more favorable to them than to conventional militaries or governments."[27]

To prepare for challenges across the continuum of conflict, including hybrid warfare, DoD must manage and exploit the effects of information by conducting and defending against strategic information operations. To be successful, the Joint Force will need to engage in operations through all domains to capture data and process intelligence to identify malign actors and understand their intentions in order to counter the use of "ideas,

images, and violence designed to manipulate the United States and its allies."[28] Concurrently, it will need to employ information offensively to support achievement of military objectives.

The military services have begun to adapt their organization frameworks in an attempt to prioritize information operations, although inconsistently. For example, the Marine Corps has a new deputy commandant for information.[29] The Air Force created a new information operations career field, and a dedicated technical training school opened in fiscal year (FY) 2019.[30] The Navy stood-up the Naval Information Warfare Development Center to grow a skilled cadre of information warfare professionals for battlefronts of the future.[31] The Army established a pilot program to identify where service information operations capabilities should reside, budgeting $14.7 million for training in FY 2019.[32] The inconsistent application for how to organize for strategic operations in the information environment reflects how widely debated the topic remains among policy makers.

A leading organizational proposal under consideration is the creation of a national information office. In testimony to the Senate Armed Service committee, The Honorable Michael D. Lumpkin, former Assistant Secretary of Defense for Special Operations and Low Intensity Conflict (ASD/SOLIC), argued the merits for creating a national information office. He considered a model for the office advocated for by former Director of National Intelligence James Clapper, which was the resurrection of the now defunct United States Information Agency (USIA), although Director Clapper opined the reestablished USIA would need to be more robust based on the emerging information landscape.[33] While agreeing there would be benefits with reconstituting the USIA, Lumpkin acknowledged there were also challenges and other issues that led to its disestablishment. Instead of the USIA, Lumpkin argued for elevating the U.S. State Department's Global Engagement Center (GEC) to a position similar in status to the Director of National Intelligence. In doing so, it would align authority, responsibility, and accountability for information operations under a single office, and a single information strategy.[34]

At present, the GEC, charged with "leading the USG's efforts to counter propaganda and disinformation from international terrorist organizations and foreign countries," has limited resources and capacity.[35] According to

https://scholarcommons.usf.edu/jss/vol12/iss4/4
DOI: https://doi.org/10.5038/1944-0472.12.4.1735

Thomas Hill, a former House senior staffer, "If people were serious about combating Russian propaganda, you have to be honest -- $80 million and 50 people in the basement of the State Department [are] not going to cut it. That is not enough."[36] A January 2018 U.S. Senate report specified, "In early 2017, Congress provided the State Departments [GEC] the resources and mandate to address the Kremlin disinformation campaigns, but operations have been stymied by the Department's hiring freeze and unnecessarily long delays by its senior leadership in transferring authorized funds to the office."[37] In April 2018, a U.S. Combatant Command senior representative engaged in information operations said he was unaware of any GEC messaging efforts, pithily stating, "They ain't talking to us."[38] Another official familiar with the GEC's efforts in Europe's Black Sea Region described them in terms that were limited in scope to ensuring that ongoing individual U.S. government efforts were "complementary."[39] Consequently, the GEC may not be a suitable option to oversee strategic information operations without significant additional investments. Therefore, assigning the lead for strategic information and cyber-enabled information operations within the DoD may be a more attractive alternative.

The 2018 NDAA might enable such an alternative. This act directs the Secretary of Defense to designate a senior official responsible for multi-domain strategic information operations. Further, it directs the creation of a "cross-functional task force to integrate DoD organizations responsible for information operations, military deception, public affairs, electronic warfare, and cyber operations."[40] According to Dr. Christopher Paul, "It seems self-evident that if we are to avoid information fratricide, we need to be coordinating all the messages and signals."[41] The office's primary responsibility would be to produce strategy, conduct planning, and champion a budget meant to "counter, deter, and conduct strategic information operations and cyber-enabled information operations."[42] The office would be responsible for determining what information to disseminate to a given audience, and what information to protect from disclosure. Establishing the office would clarify roles and responsibilities, and reduce bureaucracy by implementing an integrated structure for offensive and defensive information operations that can move at the speed of our adversaries.

There are two cogent options under the current defense structure to consider for implementation of the NDAA direction. The first is to align information responsibilities to the Under Secretary of Defense for Intelligence (USD(I)). Information operations, however, are military operations and require intelligence support, but they are not directly intelligence operations. While OUSD(I) could assume a greater role, it does not appear to be the most appropriate office for information operations. Alternatively, the Office of the Under Secretary of Defense for Policy (USD(P)) could assume these new responsibilities. On face value, this would be a logical placement as current policy assigns responsibility to the OUSD(P) for oversight of information operations in the DoD, and USD(P) acts as the principal staff advisor to the Secretary of Defense for information.[43] History suggests, however, there are disadvantages to a more robust OUSD(P) role.

A previous attempt to align strategic information operations under OUSD(P) ended with great controversy.[44] In 2001, OSD created the Office of Strategic Influence and it reported directly to the USD(P).[45] Although originally focused on defense issues linked to constructing strategy and objectives targeting specific audiences, OSD envisioned the Office would eventually become an established interagency organization with the charter to conduct strategic influence campaigns. However, someone with knowledge of the office and its mission leaked information to the media suggesting the Office would seed foreign media with misinformation and false messages. Public uproar ensued, and as a result, then Secretary Rumsfeld closed the office.

The controversy could recur if there was a repeat of the initiative. In her 2003 Army War College article, LTC Susan Gough interviewed a senior official with knowledge of OUSD(P) inner dynamics.[46] She quotes the senior official as stating there remained fears that "whoever sabotaged [the Office of Strategic Influence]" will sabotage future efforts as well.[47] Although this incident occurred in 2001, senior leaders would need to evaluate the risk of a greater OUSD(P) role for information operations. Ultimately, revisiting the approach of reassigning strategic information operations to OUSD(P) may have a similar outcome as experienced in 2001.

https://scholarcommons.usf.edu/jss/vol12/iss4/4
DOI: https://doi.org/10.5038/1944-0472.12.4.1735

Additionally, there are challenges with the current construct of aligning information operations under either OUSD(I) or OUSD(P) during a crisis. According to LTG P.K. Keen, a key observation from Joint Task Force (JTF)-Haiti was the need to communicate with a multitude of audiences in one voice.[48] To assist in this effort, the JTF established a Joint Information and Interagency Center (JIIC), an organizational construct LTG Keen recommended be codified for future JTFs. Within the JIIC, there would be a team dedicated to social media, blogs, websites, and other resources, such as public affairs media professionals, ready to advance the strategic narrative and counter any misinformation through cyber-enabled information operations. Further, the center would serve as a centralized information coordination and synchronization hub for all messaging and information sharing from the tactical to strategic levels.[49]

More senior defense leaders believe that centralized organization matters for how to conduct information operations in the future and are making changes. The Secretary of Defense assigned the U.S. Special Operations Command (USSOCOM) as the Joint Proponent for Military Information Support Operations (MISO), and directed USSOCOM to establish a centralized DoD MISO Global Messaging/Counter Messaging capability, with $1.8 million allocated in FY 2019 for the initiative.[50] Further, LTG Stephen Fogarty, U.S. Army Cyber Commander, said the Army is moving towards merging its cyber and electronic warfare functional areas. LTG Fogarty believes, “It’s time to think seriously about absorbing other historically-distinct mission areas – or tribes – including information operations.”[51]

Another option available consistent with LTG Fogarty’s August 2019 announcement to absorb information operations into U.S. Army Cyber Command, and change its name to the Army Information Warfare Command, is the potential for U.S. Cyber Command (USCYBERCOM) to assume responsibility as global synchronizer for United States strategic information operations and cyber-enabled information options.[52] Moreover, USCYBERCOM could restructure into an Information Warfare Command similar to the Army model. USCYBERCOM hosted a panel that considered this option. An October 2018 USCYBERCOM Cyber Strategy Symposium highlighted the ongoing challenges experienced by the current practice of subdividing information operations and cyberspace capabilities, however, the proposed solutions focused on what

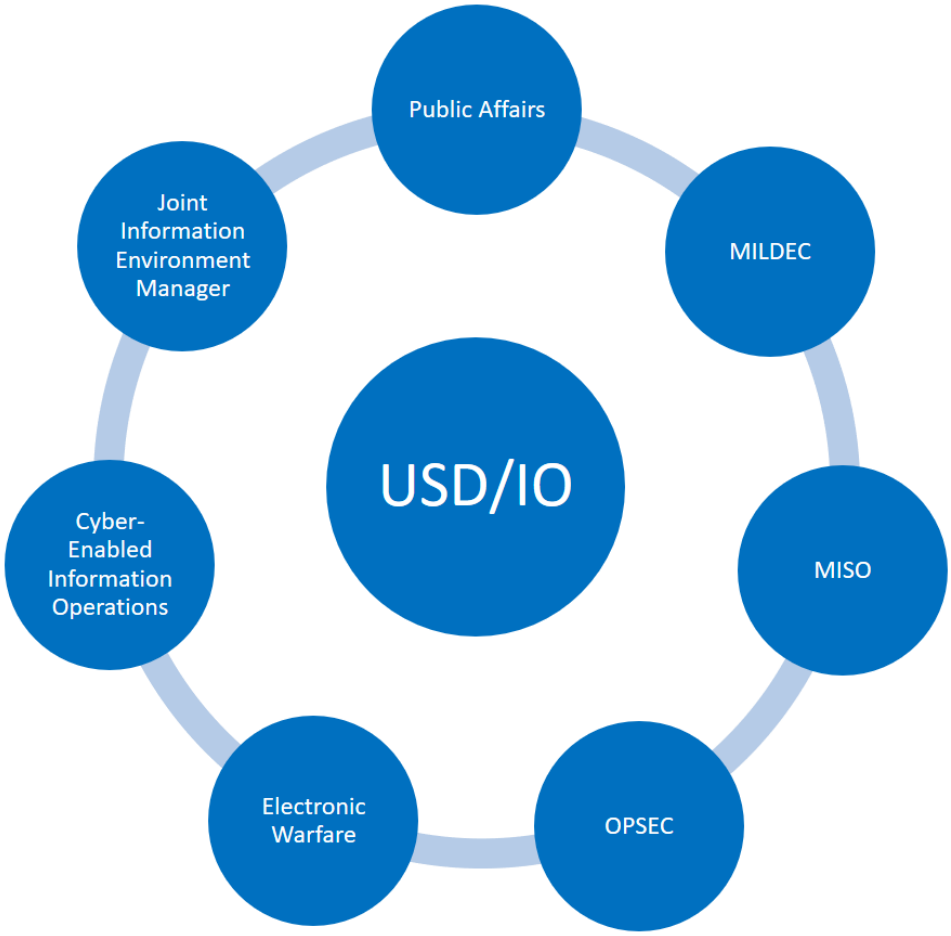
USCYBERCOM could do to augment the nation's ability to conduct strategic influence operations rather than moving to oversee these operations.[53] While USCYBERCOM is postured to deliver operationalized information or defend against an adversary's information attacks in cyberspace, the multi domain nature of the mission and associated requirements for the information enterprise appear to align more with NDAA direction to assign these responsibilities to a senior official at the undersecretary of defense level.

Recommendations to Organize for Strategic Information Operations

An organizational construct led by an Under Secretary of Defense for Information Operations (USD(IO)) would posture the United States for dominance in the information environment. The new undersecretary, consistent with NDAA 2018 direction, would be responsible for oversight of strategic information policy and guidance.[54] Further, the USD(IO) would hold responsibility for resource management leading to Department-wide integration of information operations and cyber-enabled operations. It would also create a strategic framework and guidance for cross-functional information and cyber-enabled operations. Additionally, it would be responsible for a common operating paradigm and guidance to counter adversary propaganda, influence, and deception activities targeting the United States.[55] It would take appropriate action to maintain the integrity of elections, and prevent a foreign power from adversely influencing the outcome of an initiative such as Brexit. The following diagram outlines the notional alignment of IRCs under the USD(IO).

https://scholarcommons.usf.edu/jss/vol12/iss4/4
DOI: https://doi.org/10.5038/1944-0472.12.4.1735

Figure 1. Notional Alignment of IRCs under a proposed USD(IO).



Legend:

USD(IO)	Proposed Under Secretary of Defense for Information Operations
MISO	Military Information Support Operations
MILDEC	Military Deception
OPSEC	Operations Security

Source: Author.

In addition to the above responsibilities, one particular function the OUSD(IO) would conduct is a dedicated effort to identify and understand funding of adversary online propaganda tools. Law enforcement, financial, counterintelligence and other intelligence capabilities would have significant roles in mapping the network. As appropriate, this effort would provide decision makers with information on how an adversary resources

propaganda generation to support policy decisions on countering propaganda. According to a foreign senior official familiar with Russian propaganda efforts in Europe, a capability to identify and counter Russia's ability to fund their information operations would serve as the most critical measure to combat disinformation efforts.[56] To prevent the misuse of authorities, the U.S. Government should create an Inspector General for Information.

The proposed organizational framework enables a sophisticated mechanism to generate, coordinate, "deconflict," and manage the delivery of strategic United States messaging to achieve national and departmental informational objectives through the full spectrum of intelligence, counterintelligence, diplomatic, economic, and other appropriate capabilities.[57] Further, it would better afford the USG the ability to identify and counter adversary misinformation, deceptions, and propaganda, linking defensive and offensive capabilities. Additionally, the organization should include a dedicated staff of trained planners and associated specialists whom have access to national and defense senior leaders, to include the National Security Council, in order to shape an information narrative to advance policy goals consistent with a national information strategy.

This evolving capability forms the basis for DoD strategic communication. Dr. Paul describes strategic communication as the "coordinated actions, messages, images, and other forms of signaling or engagement intended to inform, influence, or persuade selected audiences in support of national objectives."[58] Professor Phil Taylor identifies four pillars of strategic communication, including 1) Information Operations; 2) Psychological Operations (the official DoD term is MISO); 3) Public Diplomacy; and 4) Public Affairs.[59] Appointing a single advocate responsible for integrating each of the strategic communication pillars will prove essential in building out the currently disjointed framework in order to harmonize the effects of information operations across the continuum of conflict.[60]

In this light, promoting an office focused on any one single information related capability, for example one with an emphasis only on MISO or Public Affairs, would fail to capitalize on the potential advantages afforded through aligning the multitude of IRCs under a unifying framework. With an organizational construct to better orchestrate a synchronized

https://scholarcommons.usf.edu/jss/vol12/iss4/4
DOI: https://doi.org/10.5038/1944-0472.12.4.1735

information campaign, the department will need to develop and consolidate a robust operational approach, which will enable the dissemination and facilitation of messaging to reach key networks and audiences.

A DoD Information Operations Center (DIOC) is required to effectively integrate and synchronize the elements and organizations that implement and support information operations. A critical function of a DIOC then would be the coordination and "deconfliction" of messaging across organizations, combatant commands, agencies, and departments. The intent is to harmonize the delivery and effects of messaging, while avoiding the potential for information fratricide. The Joint Staff National Military Command Center or the National Counter Terrorism Center may offer a framework for managing information operations worth benchmarking.

Figure 2. Notional Defense Information Operations Center as part of the OUSD(IO).

Legend:

MISO	Military Information Support Operations
MILDEC	Military Deception
OPSEC	Operations Security
J-2	Intelligence Directorate
J-2X	Counterintelligence and Human Intelligence
J-3	Operations Staff
J-4	Logistics Directorate
J-5	Plans Directorate
J-6	Communications Systems Directorate
J-7	Force Development Directorate
J-9	Civil-Military Operations Directorate
SOF	Special Operations Forces
STO	Special Technical Operations

Source: Author.

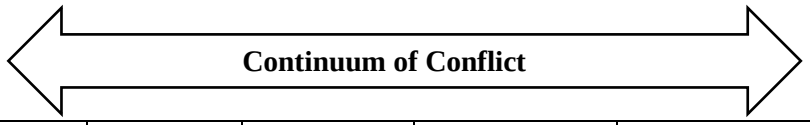
https://scholarcommons.usf.edu/jss/vol12/iss4/4
DOI: https://doi.org/10.5038/1944-0472.12.4.1735

The OUSD(IO) should be designated the centralized authority responsible for the overall information strategy and nested themes. A centralized authority ensures that all the IRCs, department heads, and defense agencies are working towards a common goal, and would therefore synchronize and integrate the previously uncoordinated initiatives of stove-piped IRCs. This approach is consistent with the United States desired end state, where

> "through 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."[61]

The following matrix assists in understanding how organizing for strategic and cyber-enabled information operations across all phases and the continuum of conflict may promote integrating, synchronizing, and harmonizing civil and military efforts. As such, it can aid representatives responsible for a specific information related capability with identifying priorities and measures of effectiveness for each operational phase. The OUSD(IO) must ensure that strategic and cyber-enabled information operations are not only coordinated and "deconflicted," but also harmonized as the sum of the parts move towards unity of effort. New cyber tools may be necessary to optimize effectiveness, as well as updated authorities to use them offensively when appropriate.

Table 1. Information Operations Integrating, Synchronizing, and Harmonizing Matrix.



Phases	Shaping/Deter	Seize Initiative	Hostilities	Termination	Post-Hostility	Stabilization
Objectives	Describe Policy Goals / Conduct Operations to Inform and Shape JIE	Obtain Surprise	Dominate JIE / Deliver themes to inform and shape behaviors	Assessment of Attitudes	Describe Current and Desired Behaviors	Describe Behavior to Inform and Shape Perceptions

Note: The author adopted this matrix from a tool the Army War College originally developed in 1992 that William Flavin later updated and referenced to assist in Planning for Conflict Termination and Post-Conflict Success.
Legend: JIE – Joint Information Environment.
Source: Author.

Summary and Conclusions

This article used an approach similar to Maj Wedemeyer's 1941 assessment for constructing the World War II victory plan: In order to know how to organize for operations in the future, one first must know what missions one will execute. To prepare for future challenges across the continuum of conflict, the United States must be postured to manage and exploit the effects of information by conducting and defending against strategic information operations. Toward this end, the United States will need to engage in operations through multiple domains to capture data and process intelligence to identify malign actors and understand their intentions in order to counter the use of "ideas, images, and violence designed to manipulate the United States and its allies." [62] Practitioners must employ defensive activities concurrently with offensive information operations to support achievement of national and military objectives. As the USG currently fields these capabilities among multiple stove-piped organizations and agencies, it therefore lacks efficiencies normally gained through combined action, unity of command, and unity of effort. These efforts include public affairs, political warfare, political advocacy, public diplomacy, and psychological (MISO) operations.

A solution to remedy these challenges, consistent with 2018 NDAA congressional direction, is for the DoD to create a new organization and designate an Under Secretary of Defense for Information Operations (USD(IO)) responsible for strategic information and cyber-enabled information operations. The USD(IO)'s responsibilities would include strategy development and coordination authority for all information related capabilities. The new organizational framework enables a sophisticated mechanism to generate, coordinate, "deconflict," and manage the delivery of strategic messaging to achieve national and departmental information objectives through the full spectrum of intelligence, counterintelligence, diplomatic, economic, and other appropriate capabilities. Similarly, the organization would be responsible for countering an adversary's use of their information capabilities.

https://scholarcommons.usf.edu/jss/vol12/iss4/4
DOI: https://doi.org/10.5038/1944-0472.12.4.1735

Without an information office responsible for countering Russian or another adversary's messaging with truthful, reliable, and credible information, disinformation or propaganda will trammel the effectiveness of USG diplomatic efforts abroad, or contribute to a loss of confidence in the government and its systems.

The creation of an organization responsible for strategic information and cyber-enabled information operations postures the USG for dominance in the information environment. Further, a cognizable organizational framework will enable integration, synchronization, and harmonization of information and cyber-enabled activities making the joint force more lethal. It will take time and resources to achieve maturation in how the United States and DoD organizes for strategic information and cyber-enabled information operations. Presidential and Congressional engagement may prove necessary. There will be risk with an organizational change that may inadvertently or adversely impact associated efforts, and adjustments may be required. Ultimately, operationalizing the USD(IO) organizational construct can overcome these challenges to unify and focus America's vast information capabilities to win engagements fought across multiple domains in the future.

Endnotes

[1] Clint Watts, "Russia and 2016 Elections," Testimony to U.S. Senate Select Committee on Intelligence, March 30, 2017, https://www.c-span.org/video/?426227-1/senate-intelligence-panel-warned-russians-play-sides.
[2] Pavel Koshkin, "The Paradox of Kremlin Propaganda: How It Tries to Win Hearts and Minds," *Russia Direct*, April 2, 2015, http://www.russia-direct.org/analysis/paradox-kremlin-propaganda-how-it-tries-win-hearts-and-minds.
[3] Aaron Mehta, "Here's How Much Global Military Spending Rose in 2018," *DefenseNews*, April 28, 2019, https://www.defensenews.co/global/2019/04/28/heres-how-much-global-military-spending-rose-in-2018.
[4] Emilio Iasiello, "Russia's Improved Information Operations: From Georgia to Crimea," *Parameters* 47, no. 2 (2017): 62, https://www.hsdl.org/?view&did=803998
[5] Patrick Wintour, "Russian Bid to Influence Brexit Vote Detailed in New U.S. Senate Report," *The Guardian*, January 10, 2018, https://www.theguardian.com/world/2018/jan/10/russian-influence-brexit-vote-detailed.
[6] Jane's Defense Industry and Markets Intelligence Center, "Cyber-Enabled Information Operations: The Battlefield Threat Without a Face," 2018, https//www.janes.com/images/assets/438/77438/Cyber-enabled_information_operations_The_battlefield_threat_without_a_face.pdf.
[7] U.S. Senate Report, "Putin's Asymmetric Assault on Democracy in Russian and Europe: Implications for US Nations Security," Committee on Foreign Relations, 115th Congress, 2nd Session, (U.S. Government Publishing Office Washington: 2018), https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf.
[8] Caroline Baylon, "Is the BREXIT Vote Legitimate if Russia Influenced the Outcome?" *Newsweek*, December 2, 2016, https://www.newsweek.com/brexit-russia-presidential-election-donald-trump-hacker-legitimate-527260.
[9] Morgan Maier, "A Little Masquerade: Russia's Evolving Employment of Maskirovka," School of Advanced Military Studies, United States Army Command and General Staff College, 2016, 4, https://apps.dtic.mil/dtic/tr/fulltext/u2/1022096.pdf
[10] Craig Timberg and Tony Romm, "It's not just the Russians Anymore as Iranians and Others Turn Up Disinformation Efforts ahead of 2020 Vote," *The Washington Pos*t, July 25, 2019, https://washingtonpost.com.
[11] Oriana Pawlyk, "SecAF Wilson: Mattis' Departure Made it Easier for Me to Resign," *Military.Com*, May 15, 2019, https://www.military.com/daily-news/2019/05/15/secaf-wilson-mattis-departure-made-it-easier-me-resign.html.
[12] USCYBERCOM 2018 Cyberspace Strategy Symposium Proceedings, 1, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Cyberspace%20Strategy%20Symposium%202018.pdf?ver=2018-07-11-092344-427.
[13] Bruce McClintock, "Russian Information Warfare: A Reality that Needs a Response," *US News & World Report,* July 21, 2017, https://www.rand.org/blog/2017/07/russian-information-warfare-a-reality-that-needs-a.html.
[14] Charles E. Kirkpatrick, "An Unknown Future and a Doubtful Present; Writing the Victory Plan of 1941," (CreateSpace Independent Publishing Platform, 2015), 60-61.
[15] The 2016 DoD Strategy for Operations in the Information Environment identifies the desired end state as, "Through 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." Also, there is no definition of strategic operations in the information environment in joint or service doctrine, therefore, this article defines the term in a manner consistent with established DoD strategy.
[16] The DoD Strategy for Operations in the Information Environment outlines an approach of supporting a broad whole of government effort. The strategy specifies, "The Department has a role to be trained, equipped, and prepared to counter such activities [misleading or false information as propaganda] in this uneasy, steady-state environment

https://scholarcommons.usf.edu/jss/vol12/iss4/4
DOI: https://doi.org/10.5038/1944-0472.12.4.1735

traditionally referred to as phase zero. To maintain unity of effort, DoD must closely coordinate operations, actions, and activities with other United States Government departments and agencies to facilitate horizontal and vertical continuity of strategic themes, messages, and actions." The mission this strategy is to support is not available at the time of writing, and the creation of a strategy linked to a specific mission would likely provide necessary input to refine the framework for how the DoD would organize for strategic information operations and cyber-enabled operations.

[17] J.C. Masterman, *The Double Cross System: The Incredible True Story of How Nazi Spies Were Turned into Double Agents* (Original work published New Haven, Conn.: Yale University Press, 1972), 10-13.

[18] Masterman*, Double Cross*, 15.

[19] Marc Fisher, "East Germany Ran Anti-Semitic Campaign in West in '60s," *Washington Post*, February 28, 1993, https://www.washingtonpost.com/archive/politics/1993/02/28/e-germany-ran-antisemitic-campaign-in-west-in-60s/418db6f8-fc45-4504-94c0-95184f8f11a6/?utm_term=.6d7bfe4fb180.

[20] John Barron, *KGB: The Secret Work of Soviet Secret Agents*, (New York: Reader's Digest Press 1974), 174.

[21] Barron, *KGB*, 173.

[22] Barron, *KGB*, 165.

[23] Author's discussion with a senior defense official assigned to a combatant command, April 23, 2018.

[24] Joint Operating Environment (JOE) of 2035, The Joint Force in a Contested and Disordered World, July 14, 2016, 23.

[25] Timothy L. Thomas, "The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and New-Type Thinking," *Journal of Slavic Military Studies* 29, no. 4. (October 2016): 554–575, as cited by Emilio Iasiello, "Russia's Improved Information Operations: From Georgia to Crimea," *Parameters* 47, no. 2 (2017): 51.

[26] The Marine Corps Security Environment Forecast, Futures 2030-2045, 66, https://www.mcwl.marines.mil/Portals/34/Documents/2015%20MCSEF%20-%20Futures%202030-2045.pdf.

[27] Marine Corps Security Environment Forecast, 70.

[28] JOE of 2035, 42.

[29] Todd South, "Deputy Commandant Leans on Intel Community for Future Fight," *Marine Times Online,* September 29, 2017, https://www.marinecorpstimes.com/news/your-marine-corps/2017/09/29/deputy-commandant-leans-on-intel-community-for-future-fight/.

[30] Stephen Losey, "Information Operations Officers Get Their Own School," *Air Force Times Online*, March 13, 2018, https://www.airforcetimes.com/news/your-air-force/2018/03/13/information-operations-airmen-get-their-own-school/.

[31] Mark Pomerleua, "Here's How the Navy is Developing Information Warfare Top Guns," *C4ISRNET*, May 29, 2018, https://www.c4isrnet.com/intel-geoint/2018/05/29/heres-how-the-navy-is-developing-information-warfare-top-guns/.

[32] Mark Pomerleau, "Here's How the Army is Spending in Information Operations," *DefenseNews Online,* February 13, 2018, https://www.defensenews.com/smr/federal-budget/2018/02/13/heres-how-the-army-is-spending-in-information-operations/.

[33] Cyber-enabled Information Operations: Hearings before the Armed Services Committee, Subcommittee on Cybersecurity, Senate, 115th Cong., (April 27, 2017) (Testimony of Michael Lumpkin, quoting James Clapper).

[34] Another argument is for the creation of a new information organization, the Office of Strategic Narratives, as a component of the National Security Council. The benefits of a national information office, similar to advantages afforded in the now debunk USIA, and without the challenges of a "too peripheral" GEC highlight significant benefits to counter the status quo. The proposed Under Secretary of Defense for Information Operations (USD(IO)) framework would dovetail nicely into an executive level information organization, and could feed specific public diplomacy or public affairs narratives from the NSC into the Defense Information Operations Center for enhanced integration and

"deconfliction." Maj Luke Karl, Maj Joseph Lane, and Cmdr David Sanchez, "How to Stop Losing the Information War," *Defense One*, July 26, 2018, https://www.defenseone.com/ideas/2018/07/how-stop-losing-information-war/150056/.
[35] US Department of State, Global Engagement Center, online description, accessed on September 13, 2018, https://www.state.gov/r/gec/.
[36] Abigail Tracy, "A Different Kind of Propaganda: Has American Lost the Information War?" *Vanity Fair*, April 23, 2018, https://www.vanityfair.com/news/2018/04/russia-propaganda-america-information-war.
[37] US Senate Report, "Putin's Asymmetric Assault on Democracy in Russian and Europe: Implications for US Nations Security," Committee on Foreign Relations, 115th Congress, 2nd Session, (U.S. Government Publishing Office Washington: 2018), 3.
[38] Author's discussion with a senior defense official, April 23, 2018.
[39] Discussion between the author and an official familiar with the GEC's efforts in Europe's Black Sea Region during the author's research on this topic while visiting Ukraine, Georgia, and Armenia in February and March 2018.
[40] NDAA 2018, Section 1637.
[41] Dr. Christopher Paul, "Strategic Communication Origins, Concepts, and Current Debates," (Santa Barbara, CA, 2011), 29.
[42] NDAA 2018, Senate Summary, 8, https://www.armedservices.senate.gov/imo/media/doc/FY18%20NDAA%20summary2.pdf
[43] DoDD 3600.01, *Information Operations*, May 2, 2013, incorporating Change 1, May 4, 2017, 5, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/360001p.pdf?ver=2019-08-12-094732-187.
[44] Donald Rumsfeld, "War in the Information Age," *Los Angeles Times*, February 23, 2006, https://www.latimes.com/archives/la-xpm-2006-feb-23-oe-rumsfeld23-story.html
[45] "New Pentagon office to spearhead information war," *CNN.Com*, February 20, 2002, http://www.cnn.com/2002/US/02/19/gen.strategic.influence/.
[46] LTC Susan L. Gough, "The Evolution of Strategic Influence," (Carlisle Barracks, PA: U.S. Army War College, 2003), 31.
[47] Gough, *Strategic Influence*, 31.
[48] P.K. Keen, Matthew Elledge, Charles Nolan, Jennifer Kimmey, "Foreign Disaster Response Joint Task Force-Haiti," *Military Review* (November/December 2010), 91, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20101231_art015.pdf.
[49] Keen*, Foreign Disaster Response*, 92.
[50] Fiscal Year 2019 President's Budget Operation and Maintenance*, Defense-Wide United States Special Operations Command*, February 2018, Int-874, https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2019/budget_justification/pdfs/01_Operation_and_Maintenance/O_M_VOL_1_PART_1/SOCOM_OP-5.pdf.
[51] Jared Serbu, "Army's Top Cyber Officer Pushes Other Disciplines, Information Operations," *Federal News Radio*, August 28, 2018, https://federalnewsradio.com/dod-reporters-notebook-jared-serbu/2018/08/armys-top-cyber-officer-pushes-other-disciplines-information-operations/.
[52] Sydney Freedberg Jr., "Army to Build New Info War Force – Fast," August 22, 2019, https://breakingdefense.com/2019/08/the-armys-information-warfare-build-up/.
[53] USCYBERCOM 2018 Cyberspace Strategy Symposium Proceedings, 9, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Cyberspace%20Strategy%20Symposium%202018.pdf?ver=2018-07-11-092344-427.
[54]DoDD 3600.01, *Information Operations*, May 2, 2013, incorporating Change 1, May 4, 2017, 5-6, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/360001p.pdf?ver=2019-08-12-094732-187. This directive provides an overview of the responsibilities.

https://scholarcommons.usf.edu/jss/vol12/iss4/4
DOI: https://doi.org/10.5038/1944-0472.12.4.1735

[55] Iasiello, "Russia's Improved Information Operations," 62-63. Iasiello offered three recommendations for the U.S. to more effectively address hostile information activities from its adversaries, 1) Establish a National counter-information center and strategy; 2) Protect against fake news, and 3) International engagement. The proposed OUSD(IO) is a solution to implement these recommendations.
[56] Interview with author, March 2018.
[57] Joint doctrine specifies JFCs and their staffs are responsible for integrating, synchronizing, employing, and assessing the IRCs used to create effects, accomplish tasks, or achieve specific objectives intended to influence a target audience's decision-making. It does so within and across the joint functions, while protecting the decision making of the United States and its allies. To enable desired effects, coordination and "deconfliction" among information operation subgroups, public affairs, defense support to public diplomacy and civil affairs is necessary. While Joint doctrine defines the requirement to integrate and synchronize the various elements of information operations, however, it does not prescribe to JFCs an organizational structure of have a definition of the proposed construct as outlined in the NDAA. In effect, the NDAA direction serves as an enabler to initiate action and move forward in establishing a national capability for strategic information operations and cyber-enabled information operations. Joint Publication 3.0, *Joint Operations*, January 17, 2017, Incorporating Change 1, October 22, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf?ver=2018-11-27-160457-910, IV-1. The joint military community employs the verb 'deconflict' in an official military capacity. Office of the Chairman of the Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*, (Washington DC: The Joint Staff, July 2019), ii. In 2005, the Oxford English Dictionary defined 'deconflict' as: To reduce the risk of collision in (a combat situation, airspace, etc) by separating the flight paths of one's own aircraft or airborne weaponry. Matthew Weaver, "Deconflict: Buzzword to prevent risk of a US-Russian Clash over Syria," *The Guardian*, October 1, 2015, https://www.google.com/amp/s/amp.theguardian.com/us-news/2015/oct/01/deconflict-buzzword-to-prevent-the-risk-of-a-us-russian-clash-over-syria.
[58] Paul, *Strategic Communication*, 3.
[59] Philip M. Taylor, "Public Diplomacy and Strategic Communications," in *Introduction, Routledge Handbook of Public Diplomacy*, Nancy Snow and Philip M. Taylor, eds., (New York: Routledge, 2009), 14.
[60] There is a senior leader vision to adapt the Joint approach to the information environment. Gen Martin E. Dempsey, *Joint Information Environment White Paper, January 22, 2013, https://www.jcs.mil/Portals/36/Documents/Publications/environmentalwhitepaper.pdf.*
[61] Department of Defense, DoD Strategy for Operations in the Information Environment, (Washington DC: 2016), 2, https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf.
[62] JOE of 2035, 42.