Information as power

Evolving US Military Information Operations and their Implications for Global Internet Governance

Milton Mueller and Karl Grindal

Georgia Institute of Technology School of Public Policy

1. Introduction

The 2016 election that brought Donald Trump to the U.S. Presidency can be seen as a turning point in American policies and attitudes toward internet governance. The discovery of organized Russian influence operations, combined with the unexpected election result, led to a fundamental reappraisal of the security implications of the content flowing over global social media. The aftermath can be seen as a textbook case of *securitization*. Securitization theory in international relations explains how political issues are reframed as existential threats to enable stronger or less constrained policy measures.[1] It involves successfully labelling a phenomenon as *dangerous*, *menacing*, or *threatening* to a nation by an actor with the social and institutional power to move the issue into a special, extranormal type of politics to alleviate the danger. (Eroukhmanoff, 2018) This is what happened in the aftermath of the 2016 elections. Social media exchanges, once seen as a realm of civil society subject to communications or tech policy, became perceived by many as an arena of geopolitical conflict or national security.[2]

[1] Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder, Colo: Lynne Rienner Pub, 1998).

[2] Kathleen Hall Jamieson, Cyberwar: How Russian Hackers and Trolls Helped Elect a President: What We Don't, Can't, and Do Know (New York, NY: Oxford University Press, 2018). "Open Hearing: Social Media Influence in the 2016 U.S. Election," Pub. L. No. 27-398 PDF, § Select Committee on Intelligence (2017), https://www.intelligence.senate.gov/hearings/open-hearing-social-media-influence-2016-us-elections#.

Myriam Dunn Cavelty (2008) has applied securitization theory to the emergence of a cybersecurity regime in the U.S.[3] This paper takes a different approach. Our goal is not to explore the *process* by which securitization took place; instead, we take the securitization of social media policy after 2016 as a given and try to explore its *consequences* for American military doctrine regarding Information Warfare (IW) and the U.S. approach to Internet governance. Given the securitization of social media following the 2016 election, how has the U.S. military acted on the perception that we are engaged in information warfare (IW) and are vulnerable to influence operations (IO) by adversary nations? The paper seeks to answer the following research questions:

1. What changes in US military organization, policy, doctrine and practice took place after 2016 as a result of American reactions to Russian influence operations?
2. What are the implications of these changes for global Internet governance, particularly for the control or shaping of content by states? Specifically, we want to find out whether the new US organizational structures, doctrines, policies and practices are eroding the distinction between liberal-democratic political systems and authoritarian political systems regarding free expression on the Internet?

As will become evident, there is a tension between the free expression principles underpinning liberal democracy and concepts of "information warfare." IW implies that exchanges of information are coercive and manipulative; liberal democracy is based on the premise that free expression facilitates knowledge, persuasion and voluntary choice. IW often involves the deliberate transmission of falsehoods; advocates of liberal communicative freedom believe that it facilitates sorting truth from falsehood by citizens. There are legal barriers to governments lying or propagandizing their own citizens in democratic states,[4] whereas authoritarian states might be described as engaged in routine IO/IW against their own citizens.

[3] Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, CSS Studies in Security and International Relations (Milton Park, Abingdon, Oxon ; New York: Routledge, 2007).

[4] The Smith-Mundt Act of 1948 is a good example of the limitations a liberal-democratic ideology imposes on state action in information. Its passage was motivated by concerns that the U.S. Government would create Nazi-style propaganda or resurrect the World War 1-era Committee on Public Information, which tried to influence domestic public opinion to favor entry into the war. It originally contained a prohibition on domestic dissemination of materials intended for foreign audiences by the State Department.

Liberal theory requires separating belief systems and media from state dominance, whereas IW makes exchanges of ideas and information part of the political and security interests of the state. If it is not carefully scoped and regulated, IW in the name of national security can push the state into regulation and control of the information environment in ways that undermine the pluralism and voluntarism of a liberal-democratic system. It follows that there has to be fundamental differences between the way authoritarian states and liberal democracies conduct IO/IW.

That fundamental tension means that any major shifts in the scope or nature of military IO/IW by a liberal-democratic power raises important policy questions. When do informational activities constitute a form of war that justifies a military, as opposed to civilian response? How does the US military define its targets for IO/IW and how are those choices authorized and legitimated? If organizational structures and doctrines are predicated on a boundary between the domestic and foreign scope of action, how can those boundaries be maintained in an era of global social media platforms and globally shared data communication standards? Arethe emerging military doctrines, practices and organizational structures recognizing and adjusting to this tension?

2. Methodology

Methodologically, the researchers conducted a systematic review of U.S. Defense Department (DoD) memoranda and publications related to IO. The time period selected began with publications after the first Iraq war (1991) and ended with documents published in the first half of 2020. That periodization was based on reports from interviewees and reinforced by our review of documents. Several reports and interviewees indicated that the first Iraq war (1991) stimulated a qualitative shift in military understanding of the role of information in war.

The researchers reviewed documents in that time span produced by DoD and the Joint Chiefs of Staff (the organizational structure that coordinates the different military branches), as well as publications by the different service branches (Army, Navy, Air Force and Marines). Some journalistic and scholarly sources were used. The researchers interviewed three US Army experts involved in IO. We reviewed relevant Congressional legislation, reports and hearings, as

well as general literature and case studies on IO/IW published by academic scholars and military theorists.

The U.S. military openly publishes its doctrine and many reports accessible to researchers. Changes in military operations on the other hand are inherently less transparent, though some reports are accessible *ex post*. The more recent the operations are, the more likely it is that they will be classified or otherwise made inaccessible to external parties. Even if it were possible to access operational evidence in a systematic way, the changes we are discussing are recent and the effects on the global information environment probably are too incipient to support any quantitative assessment of their effects. Hence we offer a largely qualitative analysis of changes in policy, doctrine and organization. The documents and interviews are used to construct a narrative that describes the post-2016 changes and adjustments in IO doctrine and identifies the rationales and events that motivated them. From this analysis, we move on to assess the consistency of the changing policies with prior U.S. positions regarding internet governance and internet freedom. Answering RQ2 involves exploring the logical implications of the changes for US Internet governance policy.

We did not systematically review the evolution or documentation of civilian agency practices and policies, such as the State Department or Global Engagement Center, as the focus of this paper is on the military response. We did, however, try to identify relevant points of intersection between civilian and military activity in the post-2016 study period.

3. What is IO/IW? Definitional issues

Information and information technology have always played a critical role in warfare. Command and control of weapons and troops, intelligence gathering and counter-espionage are unavoidable aspects of military operations. But U.S. military concepts and practices regarding IO/IW cover an expansive and complex arena of thought and action. A host of different labels are used in the U.S. military to describe different aspects of military doctrines pertaining to information. They include information warfare (IW), information operations (IO), influence operations (another IO), psychological operations (PSYOP), propaganda, public affairs, and

civil-military affairs, among others.[5] The terms political warfare[6], active measures[7] and disinformation are also sometimes used. For simplicity of exposition, this paper will use the label "IO/IW" as an umbrella term for all of those things, though our analysis will attend to the important differences in the definitions and connotations of each one when necessary.

Concepts related to IO/IW are often lumped together with concepts related to cyberspace operations (CO), computer network operations (CNO) and electronic warfare (EW). But there is a critical distinction between the IO/IW functions enumerated above and CO, CNO and EW. Cyberspace Operations pertains to defending and attacking the confidentiality, integrity and availability of information technology systems and the data they hold; CNO is about exploiting networks and information systems, and EW focuses on attacking or protecting the availability of the electromagnetic spectrum. The critical distinction between CO/CNO/EW and IO/IW is that the former does not, for the most part, avail itself of symbolic meaning to humans to achieve its effects. Cyber/CNO/EW manipulates *machines* in cyberspace using electromagnetism and computer code. IO/IW manipulates the minds, perceptions or beliefs of humans. In military parlance, they operate in different domains.[8] Cyberspace is the domain in which CO/CNO/EW take place.[9] The human domain is the realm where IO/IW work. On the other hand, some conceptions of IO, especially those closely related to military operations, involve multiple domains. Table 1 lists many of the extant labels, provides the definitions typically used by the U.S. military, and maps them to a particular domain(s).

The existence of multiple, unintegrated concepts and labels testifies to the inherent complexity of considering "information" a dimension of warfare. Analyzing the extent to which

[5] Herbert Lin, "Doctrinal Confusion and Cultural Dysfunction in DoD: Regarding Information Operations, Cyber Operations, and Related Concepts," *The Cyber Defense Review* 5, no. 2 (2020): 89–108, https://doi.org/10.2307/26923525.

[6] George F. Kennan, "'The Inauguration of OrganizedPolitical Warfare' [Redacted Version]," April 30, 1948, History and Public Policy Program Digital Archive, https://digitalarchive.wilsoncenter.org/document/114320.pdf?v=941dc9ee5c6e51333ea9ebbbc9104e8c.

[7] Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020).

[8] Domains are defined by the military as "any potential operating 'space' through which the target system can be influenced." This includes not only the traditional physical domains of land, sea, air, and space, "but also the virtual (information and cyber) and human (cognitive, moral, and social) domains." Defense Department (2005), p. 16. Much of the IO/IW literature confuses or conflates the cyberspace domain and the human domain.

[9] See Mueller 2019 for a detailed discussion of cyberspace as a domain.

these heterogeneous concepts and labels combine into a single construct (whether it is called IW or Cyber or IO) is one of the most interesting aspects of research into the post-2016 changes. One of the key measures of the outcome of doctrinal and policy change is how and why these functions and labels are grouped or separated. Organizationally, are all these activities combined under a single military command, or are they separated into specialized commands? Another key measure is to assess which aspects of these activities are primarily under military control and which are handled primarily by civilian authorities. The target and context of these different activities is also a major concern. Are the targets of military IO/IW operations restricted to military or state actors in foreign countries with whom the U.S. is engaged in hostilities, or are they more diffusely targeted at a broadly defined "Information Environment" that everyone participates in?

The grouping of IO/IW with cybersecurity or cyberspace operations[10] happens for several reasons. One reason is just unclear thinking. Because so much of the messages and social interactions we are involved in now take place via cyberspace, it is common to conflate the medium with the message. Combining the two can also occur because of real interdependencies among them. There is a point of tangency between Cyberspace operations and IO/IW when deceptive messages, such as phishing emails, are used to gain authentication credentials to break into systems. In that case, deception or disinformation in the Human domain contributes to action in the Cyberspace domain. Conversely, cyber-enabled breaches can provide access to confidential message content that might provide fodder for IO/IW campaigns, such as when the breach of the Democratic National Committee gave the intruders access to emails that could be published to discredit or compromise Democratic Party politicians. In that case, action in the Cyberspace domain contributed resources to an IO/IW campaign. However, interdependent operations across domains does not mean the domains are the same; air operations may contribute to success on land or sea, for example, but we know of no advocates for fusing the Army and the Navy. If one recognizes Human domain and Cyberspace as distinct domains, it is

[10] See, e.g., Congressional Research Service (2018)

not difficult to maintain a clear distinction among IO/IW and Cyber activities, even when they intersect operationally.

Table 1. Information-related concepts mapped to domains		
Label	**Definition**	**Domain**
Cyberspace Operations	Offensive Cyberspace Operations: Missions intended to project power in and through cyberspace Defensive Cyberspace Operations: Missions to preserve the ability to utilize blue cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity. JP 3-12 (2018)	Cyberspace
Computer Network Operations	Attack, defend, and exploit (gain valuable information from) computer networks	Cyberspace
Electronic Warfare	Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. EW consists of three divisions: electronic attack, electronic protection, and electronic warfare support. JP 3-13.1 (2007)	Cyberspace
Psychological Operations (Psyop)	Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups and individuals. The purpose is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. JP 1-02; JP 3-13.2	Human
Disinformation	Intentional release of false or misleading information to deceive or disrupt an adversary	Human
Propaganda	Any form of adversary communication, especially of a biased or misleading nature, designed to influence the opinions, emotions, attitudes, or behavior of any group in order to	Human

	benefit the sponsor, either directly or indirectly. JP 3-13.2 (2010)	
Civil Affairs Civil-Military Operations	Establish, maintain, influence or exploit relations among military forces, civil authorities, and the civilian populace in an area of operation. FM 100-6 (1996); JP 3-13, (2012)	Human
Public Affairs	Public information, command information, and public engagement activities directed toward both internal and external publics with interest in DoD. JP 3-13, (2012)	Human
Public Diplomacy	Overt international public information activities of the U.S. Government designed to promote U.S. foreign policy objectives by seeking to understand, inform, and influence foreign audiences and opinion makers, and by broadening the dialogue between American citizens and institutions and their counterparts abroad. (JP 1-02)	Human
Influence Operations	Term used by the US Air Force to group Psyop, Military deception (Mildec), and Opsec	Human
Information Operations	Military operations within the MIE that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations; IO include interacting with the GIE and exploiting or denying an adversary's information and decision capabilities. FM 100-6, (1996) Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior or foreign governments, organizations, groups and individuals. Its target audience includes not just potential and actual adversaries, but also friendly and neutral populations (JP 3-13-2, 2010)	Mixed/Combined

	The integrated employment, during military operations, of Information-Related Capabilities (IRCs) in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own. JP 3-13 (2012/2014)	
Military Information Support Operations	Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior or foreign governments, organizations, groups and individuals. Its target audience includes not just potential and actual adversaries, but also friendly and neutral populations. JP 3-13, (2012)	Mixed/Combined
Information Warfare	Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks. FM 100-6 (1996)	Mixed/Combined
Political Warfare	[E]mployment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures (as . . . the Marshall Plan), and 'white' propaganda to such covert operations as clandestine support of 'friendly' foreign elements, 'black' psychological warfare and even encouragement of underground resistance in hostile states. - George Kennan (1948)	Mixed/Combined

4. Timeline and Evolution of US IO

4.1. From the first Iraq war to 2016

Information has been considered an "instrument of national power" by the U.S. military at least since World War 2.[11] During the Cold War, the U.S. Information Agency (USIA) was the government's leading instrument of informational power. After the fall of the Soviet Union the budget and programs of USIA were rapidly curtailed as part of the peace dividend. In 1999 a shrunken U.S. Information Agency was folded into the State Department as the Broadcasting Board of Governors.

Insofar as IO/IW capabilities were maintained, they found refuge in the U.S. military's Special Operations Forces. During the 1980s, following the failure of the Carter Administration's Iranian hostage rescue mission and difficulties coordinating forces during the Reagan administration's Grenada invasion, a consensus developed among Congress and certain military leaders that Special Operations Forces needed to be reformed. In 1987 a new US Special Operations Command (USSOCOM) was formed which, over time, came to operate almost as a distinct service branch (the equivalent of the Army or Navy).

The new USSOCOM then became the haven for IO/IW capabilities. The Secretary of Defense assigned all Army and Air Force PSYOP and CA units to SOCOM.[12] The second commander of the new USSOCOM, General Carl Stiner, pushed through an initiative designating PSYOP and CA, which had suffered severe cutbacks in the years following the Vietnam War, as part of the Special Operations Force. This decision enabled USSOCOM to command and control these units

[11] Donald M. Bishop, "DIME, Not DiME: Time to Align the Instruments of U.S. Informational Power," *The Strategy Bridge*, June 20, 2018, https://thestrategybridge.org/the-bridge/2018/6/20/dime-not-dime-time-to-align-the-instruments-of-us-informational-power.

[12] USSOCOM, "United States Special Operations Command History: 1987-2007," USSOCOM History (MacDill AFB, FL: USSOCOM/SOCS-HO, 2007), http://www.fas.org/irp/agency/dod/socom/2007history.pdf.

in peacetime as well as wartime.[13] Concurrently, "information operations" was added to the list of SOCOM's principal missions.

Linking PSYOPS, civil affairs and IO with special operations served to sustain these capabilities, but also kept them stovepiped away from the other commands. The concentration of the IO capabilities in SOF was accelerated by the 9/11 terrorist attacks on the United States. The Global War on Terrorism (GWOT) was clearly an arena in which Americans had to face issues regarding the country's reputation, conflicting ideologies and psychological influence. Yet efforts to create a more centralized IO/IW capability repeatedly broke down. The Joint Chiefs of Staff established an Information Operations Task Force (IOTF) in the autumn of 2001 as an interagency group that would direct information and influence operations and act as the single point of contact for the U.S. Government. But according to one military observer "no other agencies or departments would participate" and its alerts and activities were largely ignored.[14] The IOTF was disbanded in July 2002. The Office of Strategic Influence (OSI) was created by the U.S. Department of Defense on October 30, 2001, to support the War on Terrorism through psychological operations in targeted countries. But Congressional concern over potential U.S. military involvement in disinformation and propaganda resulted in the closure of the OSI only five months later.[15] Hence, Special Operations became "the cornerstone of the U.S. military response to terrorism."[16] Its budget doubled in five years and progressive increases were scheduled for FYs 2006-2011.

---

[13] In 1993, General Stiner's successor (General Downing) revised the command's mission statement to read: "Prepare SOF to successfully conduct worldwide special operations, civil affairs, and psychological operations in peace and war in support of the regional combatant commanders, American ambassadors and their country teams, and other government agencies." (USSOCOM, 2007)

[14] Ltc. Susan L. Gough, "The Evolution of Strategic Influence" (Carlisle Barracks, PA, US Army War College, 2003), https://fas.org/irp/eprint/gough.pdf.

[15] Ibid. ---- According to Gough, "OSI was sabotaged internally within DoD... Someone in DoD leaked information to the press that OSI intended to plant false messages and misinformation in overseas media, news that would then be reported in the U.S. as factual. This type of action was not in OSI's charter, and the charge was never substantiated. Nonetheless, Rumsfeld felt that the damage caused by the media controversy and exposure were too great to overcome, and he closed the office." See also Arturo Munoz and Erin Dick, "Information Operations: The Imperative of Doctrine Harmonization and Measures of Effectiveness" (Santa Monica, CA: RAND National Defense Research Institute, January 1, 2015), https://apps.dtic.mil/sti/citations/ADA624367.

[16] USSOCOM, "United States Special Operations Command History: 1987-2007," USSOCOM History, p. 22.

Although advocates of more integrated IW/IO capabilities in the military tend to criticize it, the "siloing" of IO/IW capabilities in Special Forces and the GWOT diminished the policy dilemmas associated with military involvement in propaganda and psychological operations. It kept psyops in "a narrow organizational area focused on military and warfighting."[17] It also imposed natural limits on the geographic scope of the activity. As two SOF practitioners noted in a 2015 report, the pre-2016 "influence operations mindset" was particularly suited to "smaller-footprint, persistent-presence operations" such as counter-insurgency in occupied foreign countries.[18] This meant that the targets of IO/IW were easily separated from U.S. citizens, and the goals were more narrowly defined and immediate (e.g., convincing locals not to join terrorist groups or to cooperate in the supply of information about the whereabouts of insurgents).[19] IO was not perceived as a part of great power competition.

However, even under these limited circumstances issues arose. In Afghanistan in 2010, an Army IO unit was ordered to aid General Caldwell's attempt to manipulate visiting US Senators into providing more troops and funding for the war. The unit was asked to compile profiles and to help shape messages to the visiting dignitaries. When one of the IO officers objected to the legality of this measure it led to newspaper articles and a bit of a scandal. As the possible manipulation of information by the government was viewed with increasing suspicion, a December 2011 Secretary of Defense Memorandum rebranded "psychological operations" as "military support information operations" (MISO).[20]

During the Global War on Terror a new security challenge arose from the increasing connectedness and reliance on global information networks: the cybersecurity threat. This led to

---

[17] Conrad Crane, "The United States Needs an Information Warfare Command: A Historical Examination," *War on the Rocks* (blog), June 14, 2019, https://warontherocks.com/2019/06/the-united-states-needs-an-information-warfare-command-a-historical-examination/.

[18] Thomas M. Scanzillo and Edward M. Lopacienski, "Influence Operations and the Human Domain," CIWAC Case Studies (Newport, RI: US Naval War College, March 2015), p. ii https://digital-commons.usnwc.edu/ciwag-case-studies/13.

[19] Reports in the military focused on operations in the Philippines, Afghanistan, the Sahel, and ISIS.

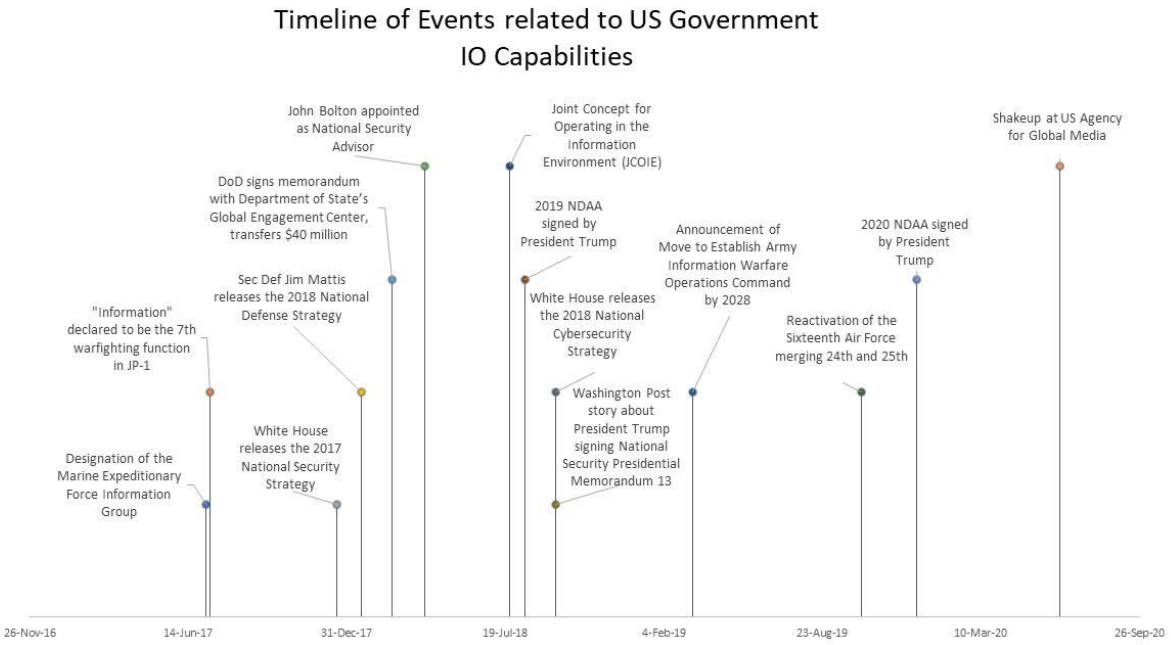
[20] Secretary of Defense Memorandum, "Changing the Term Psychological Operations (PSYOP) to Military Support information Operations (MISO), December 12, 2011. https://www.marines.mil/News/Messages/Messages-Display/Article/887791/changing-the-term-psychological-operations-to-military-information-support-oper/

a new line of development that was largely independent of IO/IW capabilities. The development of cyber capabilities within the military rapidly grew from a Joint Task Force for Computer Network Defense created in 1998 to Cyber Command on June 23, 2009. Cyber Command was headed by the Director of the National Security Agency, who consequently had access to both war fighting (Title 10) and intelligence authorities (Title 50). Throughout this development, the United States conceptually distinguished cybersecurity from information security or IO. The US contrasted the technical dimensions of cybersecurity with the content focus of Russia's and China's desire to assert sovereignty in cyberspace and counter foreign messaging, as demonstrated by their promotion of a "Code of Conduct on Information Security" before the UN General Assembly in September 2011. However, while Cyber Command resisted developing information capabilities, the IO community embedded within SOCOM saw cyberspace as both a vulnerability and opportunity to shape the cognitive domain.[21]

4.2. Evidence of change since 2016

Since 2016, the increasing salience and securitization of information has led to changes in military policy, doctrine and organization. These changes have attempted to re-orient IO towards nation-state conflicts, particularly Russia, China, Iran and North Korea, and away from its prior locus in irregular warfare, special operations and terrorism.

[21] Joint Publication 3-13 (2014) defines cyberspace as part of the information environment.



4.2.1. Policy

One of the key outcomes of securitization is policy change. The US military is civilian-led and the policy documents produced by the White House, DoD, and language articulated by Congress in the National Defense Authorization Act (NDAA) identify high-level national security threats and a corresponding course of action.

Mandated by Section 603 of the 1986 Goldwater-Nichols Act, each year the President must prepare an annual National Security Strategy (NSS) that outlines the Executive branch's strategic priorities to Congress.[22] President Trump's 2017 NSS[23] outlined "An America First National Security Strategy" that would 1) protect the American people, the homeland, and the American way of life; 2) promote American prosperity; 3) preserve peace through strength; and 4) advance American influence. Despite President Trump's contestations over the role of

[22] US Congress, "Goldwater-Nichols Department of Defense Reorganization Act of 1986," Pub. L. No. Public Law 99-433, H.R. 3622 (1986), https://www.govinfo.gov/content/pkg/STATUTE-100/pdf/STATUTE-100-Pg992.pdf.

[23] Donald J. Trump, "National Security Strategy of the United States of America" (Executive Office of The President, December 18, 2017) https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf

Russian election interference in 2016, the 2017 NSS contained numerous mentions of the security risks posed by state propaganda and disinformation. This document framed both state and non-state actors as being capable of "exploiting information" and "information warfare." The document characterized rival state actors as employing these techniques to "undermine the legitimacy of democracies."

- Rival actors use propaganda and other means to try to discredit democracy. They advance anti-Western views and spread false information to create divisions among ourselves, our allies, and our partners. (p 3)
- Today, actors such as Russia are using information tools in an attempt to undermine the legitimacy of democracies. Adversaries target media, political processes, financial networks, and personal data. (p 14)
- Malicious state and non-state actors use cyberattacks for extortion, information warfare, disinformation, and more. (p 31)
- America's competitors weaponize information to attack the values and institutions that underpin free societies, while shielding themselves from outside information. They exploit marketing techniques to target individuals based upon their activities, interests, opinions, and values. They disseminate misinformation and propaganda. (p 34)
- State and non-state actors project influence and advance their objectives by exploiting information, democratic media freedoms, and international institutions. (p 37)

This language, with the imprimatur of the President, authorizes the national security apparatus to take action against these threats.

The 2018 National Defense Strategy,[24] released under Secretary of Defense Jim Mattis, reoriented U.S. priorities away from terrorism and towards great power rivalry. It stated that the central challenge facing our Nation is the reemergence of long-term strategic competition with

[24] Jim Mattis, "Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge" (Defense Technical Information Center, January 1, 2018), https://apps.dtic.mil/sti/citations/AD1045785.

Russia and China, and that this competition replaces terrorism as the primary concern in U.S. national security. As part of this reorientation, the 2018 NDS advanced the securitization of the information domain. It framed information security by describing the actions of US competitors and adversaries as "information warfare," "political and information subversion", and "propaganda." Rather than frame this issue within the context of a clash of ideals like the NSS, the NDS emphasizes how this subversion falls short of armed conflict.

- Some competitors and adversaries seek to optimize their targeting of our battle networks and operational concepts, while also using other areas of competition short of open warfare to achieve their ends (e.g., information warfare, ambiguous or denied proxy operations, and subversion). These trends, if unaddressed, will challenge our ability to deter aggression. (p 3)

- It is now undeniable that the homeland is no longer a sanctuary. America is a target, whether from terrorists seeking to attack our citizens; malicious cyber activity against personal, commercial, or government infrastructure; or political and information subversion. (p 3)

- Counter coercion and subversion. In competition short of armed conflict, revisionist powers and rogue regimes are using corruption, predatory economic practices, propaganda, political subversion, proxies, and the threat or use of military force to change facts on the ground. (p 5)

The President's 2018 National Cyber Strategy[25] further solidified the linkage between information operations and cybersecurity. The National Cyber Strategy was intended to provide guidance across multiple Departments and Agencies in order to:

> COUNTER MALIGN CYBER INFLUENCE AND INFORMATION OPERATIONS: The United States will use all appropriate tools of national power to expose and counter the flood of online malign influence and information campaigns and non-state

[25] Donald J. Trump, "National Cyber Strategy of the United States of America" (Executive Office of The President, September 2018), https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

> propaganda and disinformation. This includes working with foreign government partners as well as the private sector, academia, and civil society to identify, counter, and prevent the use of digital platforms for malign foreign influence operations while respecting civil rights and liberties. (p 21)

Note the close linkage between cyberspace operations and information operations. The 2018 Strategy was shaped in part by National Security Advisor John Bolton.[26] Concurrently with his work on the National Cybersecurity Strategy, Amb. Bolton emphasized that a critical component of this policy was developing an expeditious decision-making structure, to give both the military and intelligence services greater independence by replacing President Obama's PPD 20 with National Security Presidential Memorandum 13.[27]

The U.S. Congress's 2019[28] and 2020 National Defense Authorization Acts (NDAAs) have reaffirmed the national security implications of information operations. Subsection a) of Section 1642 of the 2019 NDAA established new authorities for the Commander of the United States Cyber Command:

> "[If] the National Command Authority determines that Russian Federation, People's Republic of China, Democratic People's Republic of Korea, or Islamic Republic of Iran is conducting an active, systematic, and ongoing campaign of attacks [...] including attempting to influence American elections and democratic political processes.

The 2020 NDAA[29] under "Chapter 19 – Cyber and Information Operations Matters" reiterates and expands on these authorities with new language that seems far-reaching:

---

[26] Col. (Ret) Bryan Sparling, Interview on Changes in IO Doctrine, Video Call, June 27, 2020.

[27] Shannon Vavra, "Here's What John Bolton Had to Say about Cybersecurity Policy in His New Book," *CyberScoop* (blog), June 22, 2020, https://www.cyberscoop.com/john-bolton-book-cybersecurity-nspm-13-crowdstrike/.

[28] US Congress, "John S. McCain National Defense Authorization Act for Fiscal Year 2019," Pub. L. No. Public Law 115-232, H.R. 5515 (2018).

[29] National Defense Authorization Act for Fiscal Year 2020. https://www.congress.gov/bill/116th-congress/house-bill/2500

> "Congress affirms that the Secretary of Defense is authorized to conduct military operations, including clandestine operations, in the information environment to defend the United States, allies of the United States, and interests of the United States"

4.2.2. Doctrine

Joint Publication 1 (JP-1) is the capstone of United State's joint doctrine. It was amended on July 12, 2017 to incorporate "information" as the seventh joint function. As a "joint function," *information* joins *command and control*, *intelligence*, *fires*, *movement and maneuver, protection*, and *sustainment*. These categories are used to "facilitate planning and employment of the joint force." Commanders are expected to integrate and balance these functions for effective combat operations. The information function is defined as follows:

> The information function encompasses the management and application of information and its deliberate integration with other joint functions to influence relevant-actor perceptions, behavior, action or inaction, and human and automated decision making.

As both intelligence and command and control are already joint functions, the addition of information should not be understood as relating to internal information flows, but rather understanding and shaping external information to "influence" perceptions and behavior. The incorporation of language around "automated decision making" expands the scope of traditional information operations to include advanced big-data and machine learning capabilities. As for the scope of this function, "relevant-actor" provides a prescribed but obtuse and largely borderless description of who the commander might influence. As for how information might be "managed", this function is later described as giving joint force commanders "the ability to integrate the generation and preservation of friendly information." While "friendly information" is not defined, JP-1 notably excludes comments about how the US military will respond/react to un-friendly information. The 2013 edition of JP-1 described how the information environment "includes cyberspace" and thereby defined the cyber domain as part of the information environment.

The Joint Concept for Operating in the Information Environment (JCOIE),[30] published 25 July 2018, is a formal expression of the changes in American IO/IW doctrine underway. As the preface notes, the Chairman of the Joint Chiefs of Staff felt that addressing the role of information in warfare was so critical that he issued an out-of-cycle change to Joint Publication 1.

The report begins with a 1997 quotation from Richard Jensen: "...the substantive issues of information warfare will not be addressed until the United States is actually engaged in an information war." That statement signals that the drafters of this report are already committed to the idea that "information war" exists, and that we need to prepare for one. "Information is changing the character of modern warfare," according to the introduction. The rising importance of information technology means that "the physical dominance of the US military is no longer as significant" as it was before. The doctrine thus implies that adversaries can, using the so-called information environment (IE), weaken the country to the point that military superiority doesn't matter. Information is assumed to create a vulnerability that can be translated into physical or territorial gains while bypassing the kinetic/physical means of combat. In addition to flagging an alleged new vulnerability, the JCOIE warns that we are not keeping up with our competitors. US adversaries are, the report claims, 'bolder and accept more risk operating in this changing IE. As a result, they create political, social, and military advantages that exceed their traditional combat power.'

The JCOIE describes the "military challenge" of Information as one of maintaining "perceptions, attitudes, and other elements that drive desired behaviors." To do this they need to "integrate physical and informational power … in an increasingly pervasive and connected IE to produce enduring strategic outcomes." (p vii-viii) This statement implies that the US military can exercise effective control of perceptions, attitudes and any other psychological factors that drive human behavior. At the same time, the focus on *integrating* informational power with physical power sometimes implies a more limited, operational support role for IO, one that influences

[30] Joint Chiefs of Staff, "Joint Concept for Operating in the Information Environment (JCOIE)" (Washington, D.C., July 25, 2018).

behavior of both enemies and allies in warfare, or in limited zones of warfare, not in normal, peacetime business and civil society.

An acknowledged risk of the doctrine is that "integrating physical and informational power will likely challenge the boundaries of current national policy." By that the report implies that such integration rebalances the power relations between military, warfighting capability and civilian authority. The Joint Force may not be able to get approval from civilian authorities quickly enough:

> "The JCOIE's goal to dissuade conflict or prepare the environment to win decisively may not be attainable if operational commanders do not receive the necessary approval for timely and anticipatory actions from the Nation's civilian leaders. Without early and preemptive efforts, the Joint Force, along with its partners, will be incapable of averting or diminishing conflict."

But these concerns about the boundaries of current national policy (expressed in the 2018 JCOIE) seem to have been answered in the 2020 NDAA, which provides a blanket authorization for the Secretary of Defense to "conduct military operations, including clandestine operations, in the information environment" to defend the US and its interests (see 4.2.1 above).

4.2.3. Organizational

Organizational changes within DoD are moving toward consolidating information capabilities with cyber capabilities. Although there are strong advocates for such consolidation in conceptual terms, any such integration faces huge obstacles due to the incredibly complex and divided structure of the vast US military, and the overlaps between different informational functions. Inconsistent and contested terminology has left ambiguity over the names of these consolidated entities, particularly as service level Cyber Commands merge intelligence and information operations capabilities. The rate of change across the service branches varies, with the Navy having in some way anticipated the trend, the Air Force taking a quick pivot, and the Army

setting a ten year plan. Yet these organizational shifts suggest that the growing importance of cyberspace as a medium has elevated and centered information operations activities.

In 2005, the Naval Network Warfare Command (NETWARCOM) brought the Naval Security Group Activities under its command, incorporating the Naval Information Operations Command (NIOC) into the same organization as the one focused on cybersecurity capabilities. In 2010 this relationship was solidified with the creation of the US Fleet Cyber Command. Other operations have only recently begun to integrate their information and cyber training and provisioning.

The Sixteenth Air Force (reactivated 11 Oct 2019) was created as a merger of the 24th and 25th Air Force. The 24th Air Force served as a cyberspace combat force from 2010 to 2019, while the 25th provided intelligence, surveillance and reconnaissance. While heavily focused on intelligence, the 25th Air Force included the 688th Cyberspace Wing (known as the Information Operations Wings from 2009-2013) based at Lackland Air Force Base.[31] The 16th Air Force at present is known both as Air Force Cyber and as the Information Warfare Numbered Air Force as it merged intelligence, surveillance, and reconnaissance, cyber warfare, electronic warfare, and information operations capabilities under a single command.

On March 13, 2019 at AFCEA's 2019 Army Signal Conference, Lt. Gen. Stephen Fogarty announced his intent to transform Army Cyber Command into an Information Warfare Command by 2028. Already in 2020, IO capabilities would be moved to Fort Gordon in Augusta, Georgia, where Army Cyber Command is headquartered. Lt. Gen. Fogarty wrote the article "Enabling the Army in an Era of Information Warfare"[32] in the 2020 *Cyber Defense Review* which describes a desire to converge capabilities.

In July of 2017 the Marine Corps set up their first information group, the Marine Expeditionary Force Information Group (MIG). Brig. Gen. Roberta Shea, emphasizing that the Marines have been engaged in the information environment for many years, stated that the "MIG

[31] Lackland AFB also hosts the Joint Information Operations Warfare Center which coordinates information operations.

[32] Stephen G. Fogarty and Bryan N. Sparling, "Enabling the Army in an Era of Information Warfare," *The Cyber Defense Review* 5, no. 2 (2020): 17–28, https://doi.org/10.2307/26923519.

will provide Marine Corps commanders with the ability to more fully integrate information warfare capabilities into their plans." While described as an information group, the officer's description of MIG capabilities sounded more like traditional cybersecurity capabilities, as they seek to "degrade and detract from our enemy's ability to access their own networks while also defending our commanders' ability to maneuver in the information environment."

The 2020 NDAA, mentioned previously, had a significant organizational component relevant to Information Operations. Section 1631(a) creates the position of a Principal Information Operations Advisor who operates a Cross-functional Team reporting directly to the Secretary of Defense. While the Service Branches are training and equipping information capabilities, an increased organizational role within the Department of Defense will prioritize IO operations by more rapidly bringing issues and opportunities to the attention of DoD leadership.

These changes by the services have been mirrored by calls for an integration of functions under CyberCommand. As Lt. Gen. Fogarty stated in July of 2018, "In the future [...] maybe it's not going to be U.S. Cyber Command, maybe it's going to be U.S. Information Warfare Operations Command."[33] A December 2020 Washington Post article, also points to this integrated future, as it described how Cyber Command is developing information warfare tactics as a potential response to Russian interference in the 2020 election.[34]

5. Analysis and Discussion of RQ1

Two clear changes have taken place in the US military's approach to information and cybersecurity since 2016: 1) a broadening of the scope of military IO/IW from warfighting in

[33] Mark Pomerleau, "Where Do Information Operations Fit in the DoD Cyber Enterprise?," Fifth Domain, July 26, 2018, https://www.fifthdomain.com/c2-comms/2018/07/26/where-do-information-operations-fit-in-the-dod-cyber-enterprise/.

[34] Ellen Nakashima, "U.S. Cybercom Contemplates Information Warfare to Counter Russian Interference in 2020 Election," *Washington Post*, December 25, 2019, https://www.washingtonpost.com/national-security/us-cybercom-contemplates-information-warfare-to-counter-russian-interference-in-the-2020-election/2019/12/25/21bb246e-20e8-11ea-bed5-880264cc91a9_story.html.

special operations to great power competition in peacetime; 2) a tendency to collapse cyberspace operations with information operations.

5.1. Broadened scope

The post-2016 environment has broken IO/IW out of the "silo" of special operations and irregular warfare. Legislation, policy and doctrine have shifted explicitly toward a focus on continuous great power competition in which the presence of actual military conflict is irrelevant. A very broad authorization to conduct military operations in the information environment has been passed by Congress. Policy has also shifted towards a more globalized conception of the relevant Information Environment. This shift, as explained in more detail in Section 6 below, exacerbates the policy problems associated with the practice of IO/IW by a liberal democracy. When military IO doctrine was focused on counter-insurgency operations in faraway developing countries, it was easier to maintain boundaries between military IO and the domestic civilian information environment in the United States. If post-2016 IO doctrine is more focused on interactions in globalized social media, and on great power competition, it will likely be more difficult to maintain those distinctions.

5.2. Greater integration of cyber/IO capabilities

Although the process is still playing out, there is a strong advocacy within the military to merge and integrate cyberspace-domain capabilities, such as CO, CNE and EW, with human domain capabilities such as PSYOP and IO. Some openly advocate the label "Information Warfare" as the unifying concept.[35] Some advocates of this position hold up FM 100-6 (1996) as a model, because it managed to integrate the diverse and tangled field into an organized hierarchy with IO as the umbrella concept.[36] Some advocates of this position do not even realize that cyberspace operations and IW/IO refer to different domains, and regularly conflate operations in the two domains with each other. Others do grasp the distinction but see cyberspace in a subordinate role, solely as a means for delivering, disrupting or generating information-related capabilities, a

[35] Fogarty and Sparling, "Enabling the Army in an Era of Information Warfare."
[36] Crane, "The United States Needs an Information Warfare Command: A Historical Examination."

function in the service of broader IW/IO objectives. Although it is not explicitly stated, the underlying premise seems to be that control of cyber infrastructure would facilitate the ability to control or manipulate message content and shape behavior.

6. Analysis and Discussion of RQ 2: Implications for global Internet governance

The perception of the Internet as a national security threat used to be confined to authoritarian countries. It was only the dictatorships, we were told, who feared an open internet. The reaction to Trump's election, and the exaggeration of Russian influence on American society by partisan politics, has contributed to the perception of social media and cyberspace as both a weapon and a vulnerability. Proponents of "information warfare" are luring the U.S. into seeing their open public sphere and the commercial and political success of their platform businesses as vulnerabilities in a geopolitical competition, rather than as strengths. If the United States makes strong military moves in this direction, other countries, both friendly liberal democracies and authoritarian adversaries, will likely follow suit - just as they imitated the creation of a cyber command.

These developments have profound consequences for global Internet governance. They are likely to intensify nationalistic pressures on global internet connectivity and the global free flow of information. The same barriers to trade in telecommunication equipment that were justified by cybersecurity concerns at layers 3 and 4 are now being erected at the application and content layers in response to perceived IO/IW threats from foreign states.

In July of 2020 a Trump administration Executive Order blocked TikTok and WeChat because their owners were Chinese. Notably, Trump relied entirely on national security claims for his legal authority.[37] Securitization allowed the President to claim that the presence of these

[37] The International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) and the National Emergencies Act (50 U.S.C. 1601 et seq.)

apps constituted a "national emergency," which allowed him to unilaterally censor them. These threats to the liberal informational order are coming from the civilian authority, not the military. But the new view of IW among civilian political authorities can easily clear the path for a more permanent, institutionalized presence in the military, making the blocking of foreign information sources, allegations of disinformation, the manipulation of public opinion, influence operations and "information dominance" the central organizing principle of a unified IW command. In a classic security dilemma, a step in this direction by the U.S. is likely to further encourage Russian and Chinese efforts to strengthen their own IW efforts (see 6.2 below).

6.1. The SCO's 2011 Code of Conduct on Information Security

One clear manifestation of the global internet governance implications of these changes comes from the *de facto*, but not widely noted, acceptance by the United States of key cyber norms promulgated by authoritarian states.

The original 2011 draft of the Shanghai Cooperation Organization's *Code of Conduct for State Behavior in Information Security*[38] included a pledge that each state would agree to uphold certain norms related to ICTs. Items 2(a) and 2(c) attracted a lot of critical attention from the U.S. government and human rights advocates. The SCO's Code stated that states should:

> 2 (a) ...comply with the Charter of the United Nations and universally recognized norms governing international relations that enshrine, inter alia, respect for the sovereignty, territorial integrity and political independence of all States, respect for human rights and fundamental freedoms and respect for the diversity of history, culture and social systems of all countries;

[38] The full text can be found here: https://eucyberdirect.eu/content_knowledge_hu/2011-sco-international-code-of-conduct-for-state-behaviour-in-information-security/. The SCO Code was revised and resubmitted to the UN in 2015. A comparison and interpretation of the two texts from a Human Right law perspective can be found here: https://citizenlab.ca/2015/09/international-code-of-conduct/

> 2 (c) ...cooperate in ... curbing the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment."

The United States, with the support of human rights organizations, interpreted 2(a) as elevating sovereignty over fundamental freedoms in the information space, and 2(c) as a way of justifying the restriction of international information flows that a sovereign might see as destabilizing or undesirable. When the SCO code of conduct was placed before the United Nations, the US State Department issued the following statement in November 2012:

> [The SCO] "draft Code of Conduct for Information Security ... calls for multilateral governance of the Internet that would replace the multi-stakeholder approach, where all users have a voice, with top down control and regulation by states. It would legitimize the view that the right to freedom of expression can be limited by national laws and cultural proclivities, thereby undermining that right as described in the Universal Declaration on Human Rights.

The US reaction implied that information content and cybersecurity were separate things, and that cybersecurity norms should not be used to support censorship and authoritarianism. And yet, almost every policy and doctrinal move the U.S. has made since 2016 basically affirms the principles and norms in the SCO's approach to information security:

- The President's 2017 National Security Strategy (NSS) and the 2018 National Defense Strategy contain multiple references to "political and information subversion" and foreign propaganda that "exploits" our information environment. Foreign information sources are perceived as a national security threat, a threat to sovereignty, or as a threat to our cultural and political values, just as they were in the SCO Code of Conduct.
- Instead of promoting a principle of open access and free flow of information, the U.S. now complains about the asymmetry between its open system and the censored/protected national information environments (NIEs) of authoritarian countries, thereby implying that the U.S. is justified in shutting foreigners out of its own NIE.

- Politically and in military doctrine, the US has shifted to a far more sovereigntist approach to cyberspace. The definition of cyberspace as a "global domain" in the Cyberspace Operations document from 2013[39] has been replaced with an interesting qualification: "Cyberspace, while part of the information environment, is dependent on the physical domains of air, land, maritime, and space."[40]

The United States has until recent years been the world's strongest advocate of Internet freedom and a global, non-sovereignty-based approach to Internet governance. For it to back away from those principles is a very important change in global Internet governance.

6.2. The Security Dilemma in Information

The security dilemma is an intrinsic problem when states in an anarchic system with imperfect knowledge about each others' intentions observe and respond to the military activities of their rivals. One state tries to strengthen itself due to its own sense of insecurity, but this strengthening can be perceived as aggressive and threatening by another state, increasing the second state's sense of insecurity. This can lead to a self-reinforcing spiral in which both sides generate an arms race or even foment a conflict.

The Internet, which is already suffering from a deficit of trust, could suffer heavy damage from an IW arms race in which all major states are engaged in competing, military-backed efforts to "to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives."[41] A descent into mutual IW/IO by major nation-states could make commercially induced spam and cybercrime look tame by comparison.

Ironically, both Russia and the US have traditionally maintained that IW is something that bad foreigners do but not something that they themselves do. America's JP 3-13.2 (2010) defines "Propaganda" as a form of "adversary communication." American military theorists

[39] JP 3-12 (R) "Cyberspace Operations," February 5, 2013. https://fas.org/irp/doddir/dod/jp3_12r.pdf

[40] JP-12 (2018) "Cyberspace Operations," June 8, 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

[41] Definition of Psyop from JP-1.

favoring a more integrated approach to IW claim that the U.S. must do this because its adversaries possess "psychological operations that are also tightly linked to all their public affairs efforts." Similarly, in Russian military doctrine, the term "Information Warfare" is used to describe things that are happening to Russia, not what Russia is doing to other countries.[42] The so-called "Gerasimov doctrine" that the U.S. military still uses to characterize Russia's approach to IW was not really a doctrine at all, but a talk in which he expressed the view that the Arab Spring and other "color revolutions" was a form of IW *by the United States*. Yet despite these disclaimers, both Russia and the United States use the IW actions of their adversary to justify their own IW initiatives - a classic recipe for a security dilemma. China would easily fall into the same pattern, if it hasn't already.

One Australian military theorist, in a paper published by the US Army's Modern War Institute, sounded a warning note about the long-term implications of an IW race that is worth heeding:

> "...the United States and its allies, many of whom remained open, democratic, convention-based societies, stood to lose much more than they would gain from allowing, or enabling via neglect and mishandling, the information environment to become a zone of mass-targeted, multi-layered manipulation. And further, the debasement of the information environment would render efforts to influence an adversary with measures short of war sharply diminished. The irony of the age of information would be that it could herald the end of influence.[43]

---

[42] ВОЕННАЯ ДОКТРИНА РОССИЙСКОЙ ФЕДЕРАЦИИ (Military Doctrine of the Russian Federation, 2014) http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=172989&fld=134&dst=1000000001,0&rnd=0.29957666907029545#03764223477202755

[43] Zac Rogers, "The End of Information Warfare?" Modern War Institute at West Point, June 18, 2020. https://mwi.usma.edu/end-information-warfare/

6.3. Blurring boundaries

The new doctrines and organizational structures can affect global Internet governance by blurring the lines between war and peace, military and civilian activity, and foreign and domestic targets. Although that point is too abstract to be explicitly stated in official military doctrine, some military theorists have already asserted as such. Elkins (2019) believes that the expansion of warfare from the physical to virtual domains "allows state and non-state actors to bypass military forces to directly reach adversary populations – the human domain – through virtual...means," and that such "direct access to the human domain in 21st century warfare blurs the lines between civilian and military targets."[44] A prominent advocate within the US military of an Information Warfare Command, criticized the "pigeonholing of Psyops into a narrow organizational area focused on military and warfighting" as "a vulnerability that can be exploited by potential adversaries with pervasive and integrated psychological operations that are also tightly linked to all their public affairs efforts." Limiting IO to the military, this person says, "make[s] it harder to see that psychological operations were relevant in times of peace, crisis and war alike."[45] This implies that operations in the information environment must be perpetual, continuing and not confined to conflict zones. Global cyberspace is so thoroughly connected that a military campaign in the information environment can no longer be targeted at a population that can be easily segmented as "foreign" or outside the U.S.

The blurred line between the military and civilian spheres is especially puzzling. What is the role of military IO when there is no distinction between an enemy attack and a marketing campaign by a multinational public relations firm, or a cultural exchange program? If the Geneva Conventions require us to differentiate in our treatment of civilians and combatants, how does that happen when you are operating on Facebook's territory and everyone's identity is part of an "account" rather than a "country"?

[44] Lauren Elkins, "The 6th Warfighting Domain," *Over the Horizon*, November 5, 2019, https://othjournal.com/2019/11/05/the-6th-warfighting-domain/.

[45] Crane, 2019.

Indeed, this expansive concept of war can even blur the line between informational and physical operations. The JCOIE quotes a UK General as saying, "We conduct all operations in order to influence people and events, to bring about change, whether by 155mm artillery shells or hosting visits: these are all influence operations."[46] While it is true that a bombing can be intended to send a signal or shape perceptions, can the relationship be reversed? That is, are attempts to influence psychology or perception through the exchange of messages the equivalent of a bombing run? If so, such an approach expands our notion of what is war to practically every form of human interaction, and in so doing contributes to the securitization of all information and communications technologies and content.

7. Conclusion

This paper tracked some of the key effects of the securitization of the Internet and social media after 2016. It surveyed changes in US military organization, policy, doctrine and practice that took place as a result of the controversies over Russian influence operations. It then explored the implications of these changes for global Internet governance. Along the way, it catalogued and attempted to make sense of the many different labels applied to the military aspects of information, noting that there is an important distinction between activities targeting the Cyberspace domain and those targeting the Human domain.

Our findings show that post-2016, policy has taken IO/IW out of the tactical and operational limits of special operations and pushed it up to the strategic level. It is also fostering a merger and integration of U.S. capabilities across the Cyberspace and Human domains, often using the label “Information Warfare” to describe the desired command. We found evidence that these changes are eroding the distinction between the information policies and practices of liberal democracies and authoritarian states. In addition, broader concepts of strategic information warfare blur the lines between war and peace, military and civilian responsibilities, foreign and

[46] Major General Graham Binns, General Officer Commanding 1st (UK) Armoured Division, cited in the JCOIE (2018), p. 16.

domestic targets. Securitizing internet information exchanges represents a tacit embrace of sovereigntist and nationalist cyber norms that the U.S. explicitly rejected only 6-8 years ago.

Works Cited

Bishop, Donald M. "DIME, Not DiME: Time to Align the Instruments of U.S. Informational Power." *The Strategy Bridge*, June 20, 2018. https://thestrategybridge.org/the-bridge/2018/6/20/dime-not-dime-time-to-align-the-instruments-of-us-informational-power.

Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security: A New Framework for Analysis*. Boulder, Colo: Lynne Rienner Pub, 1998.

Col. (Ret) Austin Branch. Interview on Changes in IO Doctrine. Video Call, June 24, 2020.

Col. (Ret) Bryan Sparling. Interview on Changes in IO Doctrine. Video Call, June 27, 2020.

Crane, Conrad. "The United States Needs an Information Warfare Command: A Historical Examination." *War on the Rocks* (blog), June 14, 2019. https://warontherocks.com/2019/06/the-united-states-needs-an-information-warfare-command-a-historical-examination/.

Department of the Army. "FM 100-6 Information Operations." Washington, D.C., August 27, 1996. https://fas.org/irp/doddir/army/fm100-6/index.html.

Dept of State, Office of the Spokesperson. "State-Defense Cooperation on Global Engagement Center Programs and Creation of the Information Access Fund to Counter State-Sponsored Disinformation." *State.Gov* (blog), February 26, 2018. https://www.state.gov/state-defense-cooperation-on-global-engagement-center-programs-and-creation-of-the-information-access-fund-to-counter-state-sponsored-disinformation/.

Dunn Cavelty, Myriam. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. CSS Studies in Security and International Relations. Milton Park, Abingdon, Oxon ; New York: Routledge, 2007.

Elkins, Lauren. "The 6th Warfighting Domain." *Over the Horrizon*, November 5, 2019. https://othjournal.com/2019/11/05/the-6th-warfighting-domain/.

Eroukhmanoff. "'It's Not a Muslim Ban!' Indirect Speech Acts and the Securitisation of Islam in the United States Post-9/11." *Global Discourse* 8, no. 1 (January 2, 2018): 5–25. https://doi.org/10.1080/23269995.2018.1439873.

Fogarty, Stephen G., and Bryan N. Sparling. “Enabling the Army in an Era of Information Warfare.” *The Cyber Defense Review* 5, no. 2 (2020): 17–28. https://doi.org/10.2307/26923519.

Gough, Ltc. Susan L. “The Evolution of Strategic Influence.” US Army War College, 2003. https://fas.org/irp/eprint/gough.pdf.

Gregg, Heather S. “The Human Domain and Influence Operations in the 21st Century.” *Special Operations Journal* 2, no. 2 (July 2, 2016): 92–105. https://doi.org/10.1080/23296151.2016.1239978.

Hoffman, Frank, and Michael C. Davies. “Joint Force 2020 and the Human Domain: Time for a New Conceptual Framework?” *Small Wars Journal*, June 10, 2013. https://smallwarsjournal.com/jrnl/art/joint-force-2020-and-the-human-domain-time-for-a-new-conceptual-framework.

Jamieson, Kathleen Hall. *Cyberwar: How Russian Hackers and Trolls Helped Elect a President: What We Don’t, Can’t, and Do Know*. New York, NY: Oxford University Press, 2018.

Joint Chiefs of Staff. “Joint Concept for Operating in the Information Environment (JCOIE).” Washington, D.C., July 25, 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf?ver=2018-08-01-142119-830.

———. “JP 1-02 Department of Defense Dictionary of Military and Associated Terms.” Washington, D.C., February 15, 2016. https://fas.org/irp/doddir/dod/jp1_02.pdf.

———. “JP 3-12 Cyberspace Operations.” Washington, DC, June 8, 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

———. “JP 3-13 Information Operations.” Washington, D.C., November 20, 2014. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.

———. “JP 3-13.1 Electronic Warfare.” Washington, D.C., January 25, 2007. http://www.acqnotes.com/Attachments/Joint%20Publication%203-13.01%20Electronic%20Warfare%2025%20Jan%2007.pdf.

———. “JP 3-13.2 Military Information SupportOperations.” Washington, D.C., December 20, 2011. https://www.bits.de/NRANEU/others/jp-doctrine/JP3-13.2C1(11).pdf.

———. “JP-1 Doctrine for the Armed Forces of the United States.” Washington, D.C., July 12, 2017. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf.

Kennan, George F. “‘The Inauguration of Organized Political Warfare’ [Redacted Version],” April 30, 1948. https://digitalarchive.wilsoncenter.org/document/114320.

Lin, Herbert. "Doctrinal Confusion and Cultural Dysfunction in DoD: Regarding Information Operations, Cyber Operations, and Related Concepts." *The Cyber Defense Review* 5, no. 2 (2020): 89–108. https://doi.org/10.2307/26923525.

Lt. Col. Robert Ross. Interview on Changes in IO Doctrine. Video Call, June 10, 2020.

Mattis, Jim. "Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge." Defense Technical Information Center, January 1, 2018. https://apps.dtic.mil/sti/citations/AD1045785.

Munoz, Arturo, and Erin Dick. "Information Operations: The Imperative of Doctrine Harmonization and Measures of Effectiveness." Santa Monica, CA: RAND National Defense Research Institute, January 1, 2015. https://apps.dtic.mil/sti/citations/ADA624367.

Nakashima, Ellen. "U.S. Cybercom Contemplates Information Warfare to Counter Russian Interference in 2020 Election." *Washington Post*, December 25, 2019. https://www.washingtonpost.com/national-security/us-cybercom-contemplates-information-warfare-to-counter-russian-interference-in-the-2020-election/2019/12/25/21bb246e-20e8-11ea-bed5-880264cc91a9_story.html.

Pomerleau, Mark. "5 Questions with the Marine Corps' Deputy Commandant for Information." *C4ISRNET* (blog), April 3, 2020. https://www.c4isrnet.com/information-warfare/2020/04/03/5-questions-with-the-marine-corps-deputy-commandant-for-information/.

———. "Where Do Information Operations Fit in the DoD Cyber Enterprise?" Fifth Domain, July 26, 2018. https://www.fifthdomain.com/c2-comms/2018/07/26/where-do-information-operations-fit-in-the-dod-cyber-enterprise/.

Rid, Thomas. *Active Measures: The Secret History of Disinformation and Political Warfare*. New York: Farrar, Straus and Giroux, 2020.

Rogers, Zac. "The End of Information Warfare?" *Motern War Insitute at West Point* (blog), June 18, 2020. https://mwi.usma.edu/end-information-warfare/.

Scanzillo, Thomas M., and Edward M. Lopacienski. "Influence Operations and the Human Domain." CIWAC Case Studies. Newport, RI: US Naval War College, March 2015. https://digital-commons.usnwc.edu/ciwag-case-studies/13.

Statement by Delegation of the United States of America. "Other Disarmament Issues and International Security Segment of Thematic Debate in the First Committee of the Sixty-Seventh Session of the United Nations General Assembly." *U.S. Department of State* (blog), November 2, 2012. https://2009-2017.state.gov/t/avc/rls/200050.htm.

Trump, Donald J. “National Cyber Strategy of the United States of America.” Executive Office of The President, September 2018. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

———. “National Security Strategy of the United States of America.” Executive Office of The President, December 18, 2017. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf.

U.N. General Assembly. “Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General,” January 13, 2015. undocs.org/en/A/69/723.

US Congress. Goldwater-Nichols Department of Defense Reorganization Act of 1986, Pub. L. No. Public Law 99-433, H.R. 3622 (1986). https://www.govinfo.gov/content/pkg/STATUTE-100/pdf/STATUTE-100-Pg992.pdf.

———. John S. McCain National Defense Authorization Act for fiscal year 2019, Pub. L. No. Public Law 115-232, H.R. 5515 (2018).

USSOCOM. “United States Special Operations Command History: 1987-2007.” USSOCOM History. MacDill AFB, FL: USSOCOM/SOCS-HO, 2007. http://www.fas.org/irp/agency/dod/socom/2007history.pdf.

Vavra, Shannon. “Here’s What John Bolton Had to Say about Cybersecurity Policy in His New Book.” *CyberScoop* (blog), June 22, 2020. https://www.cyberscoop.com/john-bolton-book-cybersecurity-nspm-13-crowdstrike/.