Information as Power: Evolving US Military Information Operations *and their Implications for Global Internet Governance*

Dr. Milton Mueller
Dr. Karl Grindal

INTRODUCTION

The 2016 Presidential election that brought Donald Trump to the White House was a turning point in US 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.[1] Once seen as a realm of civil society subject to communications or technology policy, social media exchanges are now perceived by many as an arena of geopolitical conflict. The US, many claimed, was engaged in information warfare in a way that implicated national security.[2] This article explores the consequences of the changing perception of Internet content for US military doctrine regarding Information Operations (IO) and the US approach to Internet governance. The article seeks to answer the following two research questions (RQ):.

RQ1: What changes in US military organization, policy, doctrine, and practice regarding IO took place after 2016?

RQ2: Are the post-2016 US military organizational structures, doctrines, policies, and practices eroding the distinction between liberal-democratic and authoritarian political systems regarding free expression on the Internet?

The motivation for these two research questions is the potential clash between the free expression principles underpinning liberal democracy and concepts of information warfare or state-sponsored influence operations. Constitutional protections constrain governments from censoring and propagandizing their citizens in liberal democratic states. The freedom and autonomy of public expression are perceived to be essential components of democratic self-governance, and state-backed influence operations would undermine them.

Dr. Milton Mueller is a Professor at the Georgia Institute of Technology (Atlanta, GA, USA) in the School of Public Policy and Director of Georgia Tech's Master of Science program in Cybersecurity Policy. His most recent book is *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace* (Polity, 2017).

The long controversy over the Smith-Mundt Act of 1948 exemplifies these tensions. The law was passed during the early stages of the Cold War and it authorized US civilian agencies to engage in public diplomacy as part of the ideological competition with the Soviet Union. The law's passage was followed by six decades of controversy over whether the U.S. Information Agency (USIA) produced government propaganda and whether the government could legally disseminate its products to Americans.[3] While these concerns pertained to civilian agencies, similar suspicions about Department of Defense (DoD) support for domestic propaganda efforts repeatedly surfaced during the wars in Iraq and Afghanistan.[4]

Authoritarian states, in contrast, suffer from no such competing tensions; they openly engage in institutionalized IO against their own citizens. Moreover, their domestic censorship and propaganda activities are justified on national security grounds. Liberal democracies tolerate the instability generated by competing media outlets, political parties, and belief systems, seeing them not only as individual rights but as beneficial to accountability and effective self-governance. In contrast, authoritarian countries make the exchange of ideas and information part of the political and security interests of the state. It follows that there must be fundamental differences between the way authoritarian states and liberal democracies handle the relationship between government IO and national security. Therefore, any significant shifts in the scope or nature of military IO by a liberal-democratic power raise important policy questions.

METHODOLOGY

The researchers address RQ1 by systematically reviewing DoD memoranda and publications related to IO. This evidence enables differentiation between military doctrine, public policy, and organizations associated with IO before and after 2016. The analysis begins

Dr. Karl Grindal is a Postdoctoral Fellow and Instructor at the Georgia Institute of Technology's School of Cybersecurity and Privacy. He received his Ph.D. from Georgia Tech's School of Public Policy in 2021.

with the U.S. Special Operations Command's (USSOCOM) formation in 1987 and ends with documents published in the first half of 2020. The review included documents produced by DoD and the Joint Chiefs of Staff, publications by the different service branches (Army, Navy, Air Force, and Marines), interviews with practitioners, and journalistic sources. The review also included relevant Congressional legislation, reports, hearings, and general literature and case studies on IO published by academic scholars and military theorists. Because the article focuses exclusively on the military response, it did not review the evolution or documentation of civilian agency practices and policies.

The second research question (RQ2) builds on the answers to RQ1 to conduct a qualitative analysis of how evolution in policy, doctrine, and organization exhibits a change in the US approach to global freedom of expression on the Internet. The researchers identify the rationales for the changes and compare them to the justifications offered by authoritarian states. There is also an assessment of the consistency of the new policies with prior US positions regarding Internet governance and Internet freedom.

WHAT IS IO? DEFINITIONAL ISSUES

Information and information technology have always played a critical role in warfare. Command and control of weapons and troops, intelligence gathering, and counterespionage are central to military operations.[5] The US military uses many different labels to describe activities associaged with information and cyberspace. In addition to IO, the terms used include information warfare (IW), influence operations (another IO), psychological operations (PSYOPS), propaganda, public affairs, civil-military affairs (CMA), political warfare, active measures, and disinformation.[6] These US military concepts and practices cover an expansive, complex, and constantly evolving arena of thought and action.

For simplicity of exposition, this paper will use the label "IO" as an umbrella term for all the aforementioned labels (IW, IO, PSYOPS, CMA, active measures, disinformation). Our analysis, however, will attend to the essential differences in the definitions and connotations of each term, when necessary. The definition of Information Operations given in Joint Publication (JP) 3-13 (2012) is typical and very similar to the definitions of PSYOPS, Military Information Support Operations (MISO):

> 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. Its target audience includes not just potential and actual adversaries, but also friendly and neutral populations.[9]

Adding to the complexity, military concepts related to IO have often been lumped together with military approaches to *cybersecurity* and *cyberspace* in potentially confusing ways. Here, too, we find a host of different labels for various specialized functions, such as cyberspace operations (CO), computer network operations (CNO), and electronic warfare (EW). However, there is a critical distinction between what is defined as IO above and these cybersecurity-related functions. CO and CNO defend or attack the confidentiality, integrity, and availability of *information technology systems*, and EW focuses on attacking or protecting the availability of the electromagnetic spectrum. In other words, CO/CNO/EW manipulate *machines* in cyberspace.

On the other hand, IO produces and manipulates messages to influence the cognition, perceptions, or beliefs of *humans*. While IO may use cyber-technical means to distribute messages, the arena of action is the human mind, not the machines per se. In military parlance, they operate in different domains.[10] The critical distinction is that cybersecurity-related operations do not, for the most part, avail themselves of symbolic meaning to humans to achieve their effects.

The existence of multiple, nonintegrated concepts and labels makes the analysis of post-2016 changes in doctrine, organization, and practice more complicated but also more interesting and relevant. Do the doctrinal changes combine these heterogeneous concepts and labels into a single construct or combine them under a single military command? Is the target a state actor in foreign countries with whom the US is engaged in hostilities, or is it a broadly defined Information Environment that includes everyone? Does IO happen only in wartime or also in peacetime? We engage with each of these questions while analyzing the changes in IO before and after 2016.

TIMELINE AND EVOLUTION OF US IO

Our attempt to track the complex, often-confused evolution of IO concepts in the US military begins in 1987, with the formation of USSOCOM. Over time, this command came to operate as an almost distinct service branch, and set the baseline for IO policy, doctrine and operations for over twenty-five years, until the disruption of 2016.

The IO situation prior to 2016

During the Cold War, the USIA was the government's leading instrument of informational power.[11] After the fall of the Soviet Union, the budget and programs of USIA were rapidly curtailed. The human domain set of IO capabilities eventually found a post-Cold War refuge in the new Special Operations Forces (SOF). The Secretary of Defense assigned to USSOCOM all Army and Air Force PSYOPS and Civil Affairs (CA) units.[12] USSOCOM's second commander, General Carl Stiner, pushed through an initiative designating PSYOPS and Civil Affairs as part of the SOF and command and control of these units in peacetime as well as wartime.[13] Concurrently, information operations was added to USSOCOM's principal mission list.

Linking PSYOPS, CA, and IO with special operations sustained these capabilities and kept them stovepiped away from the other commands. The concentration of IO capabilities in SOF was reinforced by the 9/11 terrorist attacks on the US. The Global War on Terrorism (GWOT) was an arena in which the US faced issues regarding the country's reputation, conflicting ideologies, and psychological influence. Yet efforts to centralize IO capability to support GWOT repeatedly broke down. The Joint Chiefs of Staff established an Information Operations Task Force (IOTF) in the autumn of 2001 as an interagency group to direct information and influence operations and act as the single point of contact for the US government. Nevertheless, 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. Special Operations filled the vacuum, becoming "the cornerstone of the US military response to terrorism."[15]

Although advocates for integrated IO capabilities in the military criticize the siloing of IO capabilities in SOF, its base in USSOCOM mitigated the policy dilemmas associated with military involvement in propaganda and psychological operations. As one military historian said, it kept them in "a narrow organizational area focused on military and warfighting."[16] 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 suited to smaller-footprint, persistent-presence operations such as counterinsurgency in occupied foreign countries.[17] This focus meant that the targets of IO were not engaging with US citizens, and the goals were more narrowly defined and immediate (e.g., convincing locals not to join terrorist groups or to supply information about the whereabouts of insurgents).[18] IO was not perceived as a part of great power competition.

However, even under these limited circumstances, issues arose. After 2005 there was a shift in the definition of IO from an integrating function focused on disabling an enemy's military decision making to amorphous notions about informing and influencing civilian populations; this loss of focus contributed to the IO community's slip from relevance in the US military.[19] 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 MISO.[20]

A parallel thread developed what became U.S. Cyber Command (USCYBERCOM). Throughout the 1990s and 2000s, society's increasing reliance on computers and the Internet produced within the Intelligence Community a shift from passive to active signals intelligence (SIGINT). According to General Michael Hayden, the move from passive to active SIGINT involved "commuting to the target and extracting information from it, rather than hoping for a transmission we could intercept."[21]

In the early days of this shift, active SIGINT[22] went under the label of IW. By the end of 1996, however, the term IW was rejected. DoD formally changed IW to IO with the issuance of a new classified order, DoD S3600.1. An unnamed OSD IO official said in an interview with Wiener (2016) that "[t]he State Department made us change terminology from IW to IO for political reasons."[23] The "political reasons" appear to be related to the longstanding barriers between state/military propaganda and the civilian environment, which had become increasingly important with the rise of the Internet. Specifically, "the government did not want the inference to be drawn that we are militarizing cyberspace."[24] Here we see the constraints and ideals of liberal democracy and Internet governance directly constraining military labels for their doctrine, if not necessarily their operational practice. On the other hand, National Security Agency (NSA) director Lt. Gen. Kenneth Minihan supposedly welcomed the shift as it obscured NSA activities and allowed him to "build out mission capability for Computer Network Attack (CNA) and Computer Network Exploitation (CNE)."[25]

The development of cyber capabilities within the Intelligence Community (IC) led to interagency squabbling over which service should own Computer Network Defense. Over the next eleven years, the organizational home of offensive and defensive cyber operations changed hands several times and was ultimately subsumed by USCYBERCOM, created on June 23, 2009. USCYBERCOM continued to grow, activating its Cyber National Mission Force (CNMF) in 2014 and being elevated to a combatant command in 2018.[26] While CNA was envisioned as having significant warfighting potential, much of the growing scope of USCYBERCOM activities still seemed to fit within an intelligence framework.

Before the creation of USCYBERCOM, there was significant variation in the conceptual understanding of network and IW across the different military services. USCYBERCOM "had the effect of formalizing the interactions among the military services and partially standardizing the thinking."[27] Generally, following the creation of the command, the US conceptually distinguished cybersecurity, which involved CNA, CND, CNE, and Electronic Warfare (EW), from human domain actions such as IW or IO. As USCYBERCOM applied a technical understanding of CNA and CNE to its core conceptual mission, the IO community embedded within USSOCOM saw cyberspace as both a vulnerability and an opportunity to shape the cognitive domain.[28]

Evidence of change since 2016

Since 2016, the perception of information's increasing relevance to national security has led to military policy, doctrine, and organizational changes. These changes have attempted to reorient IO toward nation-state conflicts, away from its focus in irregular warfare, special operations, and terrorism.

The 2014 conflict in Ukraine already led a few analysts in the US military to focus on Russian IW, or what they called "hybrid warfare."[29] However, while the belief that Russia was pursuing a new approach to IW was gaining credence among specialists in 2014 and 2015, there were no significant changes in policy or shifts in doctrine in those years. It was the 2016 election outcome with the controversy over Russian involvement that brought widespread public attention to Russian IW (and even some exaggeration of it).[30]

Measurable changes in policy, doctrine, and organization began in 2017 (see Figure 1) when Russian IW was perceived or asserted to be directly affecting the US, and the threat analysis was enhanced by partisan conflict within the US.[31] While latent pockets of support in the military for a new approach to IO may have existed before the 2016 elections, we will show in the following sections that transformative changes to military policy, doctrine, and organizational structure were, at least in part, instigated by perceptions of Russian manipulation of the US information environment in 2016.

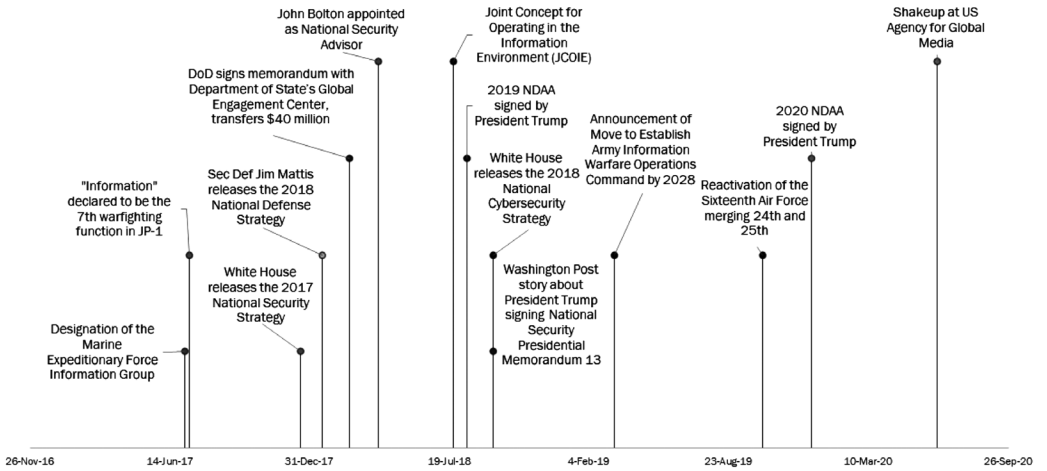

Figure 1. Timeline of Events Related to US Government IO Capabilities.

Policy

Strategic national security policy documents produced by the White House, DoD, and Congress identify high-level national security threats and set a corresponding course of action. In the years following the 2016 election interference, these policy documents highlighted the threat of foreign influence operations and sought to empower the US military to counter these threats.

The President must prepare an annual National Security Strategy (NSS), as required by law, that outlines his strategic priorities to Congress.[32] Despite President Trump's downplaying of the role of Russian election interference in 2016, the 2017 NSS contained numerous mentions of the security risks posed by foreign state propaganda and disinformation. This document described how states "weaponize information,"[33] and "use cyberattacks for extortion, information warfare, [and] disinformation."[34] Russia is specifically named for "using information tools in an attempt to undermine the legitimacy of democracies."[35] However, both "[s]tate and non-state actors" are identified as "project[ing] influence and advance[ing] their objectives by exploiting information, democratic media freedoms, and international institutions."[36] With the imprimatur of the President, this language authorized the national security apparatus to act against these threats. In contrast, the Obama administration's 2015 NSS contained only one passing reference to Russian propaganda and never used the terms information warfare, disinformation, subversion, or exploitation of information.

The 2018 National Defense Strategy (NDS)[37] altered the US approach to information. It framed information security by describing the actions of US competitors and adversaries as information warfare, political and information subversion, and propaganda. State actions like political and information subversion are identified such that "the homeland is no longer a sanctuary."[38] It further puts this activity in the context of armed conflict, describing adversaries' use of IW as an example of competition short of open warfare.[39]

The President's 2018 National Cyber Strategy[40] further solidified the linkage between information operations and cybersecurity. Unlike the NDS, the National Cyber Strategy is intended to provide guidance across multiple departments and agencies. The 2018 document proposed using all appropriate tools of national power to expose and counter the flood of online malign influence and information campaigns and non-state propaganda and disinformation. It further proposed working with the private sector, academia, and civil society to identify, counter, and prevent the use of digital platforms for malign foreign influence operations.

The Congress's 2019 and 2020 National Defense Authorization Acts (NDAAs) reaffirmed the national security implications of IO. Section 1642(a) of the 2019 NDAA provided authorities,

> [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.[41]

The 2020 NDAA under Chapter 19 – Cyber and Information Operations Matters[42] reiterates and expands on these authorities with far-reaching language that affirms DoD, "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."[43]

Civilian policy changes, including the NSS, NDS, and NCS, prioritized countering foreign influence operations. Congress then used the 2019 and 2020 NDAAs to authorize a significantly expanded role for the military in the information environment. In the subsequent section, we show that the post-2016 agenda setting and expansion of authorities were matched by evolution in military doctrine to address this expanded mission.

Doctrine

Joint Publication 1 (JP-1), the capstone of United States joint doctrine, was amended on July 12, 2017, to incorporate information as the seventh *joint function*.[44] As a joint function, information joins intelligence, fires, movement and maneuver, protection, sustainment, and command and control.[45] These categories are used to facilitate planning and employment of the joint force.[46] 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.[47]

Earlier definitions of IO "centered around the notion of attacking enemy communication systems as a way to inhibit the enemy's exercise of battlefield command and control."[48] With information's formal designation as the seventh joint function, it is clear that the Joint Chiefs assign to information a much broader concept of IO. Given that both intelligence and command and control were already designated joint functions, the addition of information cannot be understood as relating to battlefield communications or to intelligence gathering. It must mean shaping external information to influence the perceptions and behavior of any relevant actor.

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."[49] While friendly information is not defined, JP-1 notably excluded comments about how the US military will respond/react to unfriendly information. The 2013 edition of JP-1 described how the information environment "includes cyberspace" and thereby defined the cyber domain as overlapping with the information environment.

The Joint Concept for Operating in the Information Environment (JCOIE),[50] published July 25, 2018, is a formal expression of the changes in US IO doctrine. 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 JP-1. The report begins with a 1997 quotation from Richard Jensen which indicates the report's drafters are already committed to the idea that information war exists and we need to prepare for that eventuality. It implies that the so-called information environment (IE) can create vulnerabilities which can be translated into physical or territorial gains while bypassing the kinetic/physical means of combat. The JCOIE warns that US adversaries are "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."[51] This statement implies that the US military can effectively control perceptions, attitudes, and other psychological factors which drive human behavior. To do this, they need to "integrate physical and informational power ... in an increasingly pervasive and connected IE to produce enduring strategic outcomes."[52]

An acknowledged risk of the doctrine is that "integrating physical and informational power will likely challenge the boundaries of current national policy."[53] These concerns about the boundaries of current national policy expressed in the 2018 JCOIE appear to have been answered in the 2020 NDAA.[54]

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, this integration faces huge obstacles due to the US military's complex and divided structure 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 establishing a ten-year plan.

The Naval Network Warfare Command (NETWARCOM) brought the Naval Security Group Activities under its command in 2005, 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 U.S. Fleet Cyber Command.

The 16th Air Force, which was reactivated on October 11, 2019, merged the 24th and 25th Air Forces. 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 Wing from 2009 to 2013) based at Lackland Air Force Base.[55] The 16th Air Force is presently known both as Air Force Cyber and as the Information Warfare Numbered Air Force as it merged intelligence, surveillance, 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 (ARCYBER) into an Information Warfare Command by 2028. In 2020, IO capabilities were moved to Fort Gordon in Augusta,

Georgia, where ARCYBER was headquartered. At that time, Lt. Gen. Fogarty also reiterated his intentions and his vision for a convergence of capabilities.[56] While existing 1st IO brigade capabilities are focused on traditional "Operations Security (OPSEC), Military Deception (MILDEC), and IO's core synchronization and integration functions,"[57] Lt. Gen. Fogarty targets multidomain capability in 2028 to defeat "adversary Information Warfare by Operations in the Information Environment (OIE)."[58] The Army's conceptual terms continue to evolve, with reports suggesting that "information advantage" has replaced "information warfare" and that the term will soon be incorporated into doctrine.[59]

In July 2017, the Marine Corps set up its first information group, the Marine Expeditionary Force Information Group (MIG). Brig. Gen. Roberta Shea described this program as: MIG will provide Marine Corps commanders with the ability to more fully integrate information warfare capabilities into their plans.[60] 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."[61]

The previously mentioned 2020 NDAA had a significant organizational component relevant to Information Operations. Section 1631(a) describes the position of a Principal Information Operations Advisor who operates a Cross-functional Team who reports directly to the Secretary of Defense. Changes by the services have been mirrored by calls for an integration of functions under USCYBERCOM. As Lt. Gen. Fogarty stated in July of 2018, "[i]n 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."[62] A December 2020 *Washington Post* article also pointed to this integrated future, as it described how USCYBERCOM is developing IW tactics as a response to the possibility of Russian interference in the 2020 election.[63]

ANALYSIS AND DISCUSSION OF RQ1

Two clear changes have taken place in the US military's approach to information and cybersecurity since 2016. The first is a broadening of the scope of military IO from warfighting in special operations to great power competition in peacetime. This larger scope implies that IO is being elevated from the operational level to the strategic level. The second is a tendency for organizational structures to combine operations in the cyberspace domain with information operations in the human domain.

From Operational to Strategic

The post-2016 environment has broken IO out of the silo of special operations and irregular warfare. Legislation, policy, and doctrine have shifted explicitly to address ongoing great power competition with China and Russia in the absence of actual military conflict. Congress passed broad authorizations to conduct military operations in the information environment.

Policy has also shifted toward a globalized concept of the relevant Information Environment. These changes exacerbate the policy problems associated with the practice of IO by a liberal democracy. It was easier to maintain boundaries between military IO and the domestic civilian information environment when military IO doctrine was focused on counterinsurgency operations in faraway developing countries. Post-2016, these boundaries are now in tension with globalized social media and great power competition, where the IE is seen as a factor affecting strategic conflict.

Greater integration of cyber/IO capabilities

Russian activities during the 2016 election have mobilized efforts to integrate cyber and IO capabilities. There is strong advocacy within the military to merge and integrate cyberspace-domain capabilities (CO, CNE, and EW) with human domain capabilities such as PSYOPS and IO. The label, Information Warfare, has been suggested as a unifying concept.[64] Some advocates of this position hold up FM 100-6 (1996) as a model because it integrated activities in both the human and cyber domains into an organized hierarchy with IO as the umbrella concept.[65] Some advocates of this position do not recognize cyberspace operations and IO as operating in different domains. Others grasp the distinction but see cyberspace in a subordinate role as a means for delivering, disrupting, or generating information-related capabilities in the service of broader, human domain objectives. Although rarely stated explicitly, the underlying premise seems to be that control of cyber infrastructure would facilitate the ability to control or manipulate message content in ways that shape attitudes and behavior. While encouraged by the post-2016 policy environment, this tendency has not been victorious as evidenced by Lt. Gen. Fogarty's reversal on establishing an Army IW command.

ANALYSIS AND DISCUSSION OF RQ 2: IMPLICATIONS FOR GLOBAL INTERNET GOVERNANCE

There were three ways in which the post-2016 changes in IO doctrine, policy, and organization affected global Internet governance: (1) there was a tacit acceptance of certain principles regarding information advanced by authoritarian nations; (2) there was a triggering of a security dilemma in the Global Information Environment (GIE); (3) some of the military-civilian boundaries traditionally associated with liberal-democratic governance were blurred.

Parallels to the Shanghai Cooperation Organization's 2011 Code of Conduct on Information Security

One clear manifestation of the Internet governance implications of these changes comes from the de facto, but not widely noted, acceptance by the US of cyber norms promulgated by authoritarian states. The original 2011 draft of the Shanghai Cooperation Organization's (SCO) *Code of Conduct for State Behavior in Information Security*[66] included a pledge that each state would do the following:

> ...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.[67]

The US, with the support of human rights organizations, interpreted as curbing of information dissemination and as a way of justifying the restriction of international information flows that a sovereign might see as destabilizing or undesirable.

Still, almost every policy and doctrinal move the US has made since 2017 affirms the principles and norms in the SCO's approach to information security. They contain multiple references to political and information subversion. Like China, the US is moving to shut foreigners out of its own National Information Environment (NIE). The Trump administration's proposal to block Chinese apps TikTok and WeChat took this logic to an unprecedented extreme.[68] The US has, until recent years, been the world's strongest advocate of Internet freedom and a global, non-sovereignty-based approach to Internet governance.[69] For it to back away from those principles is a significant change in global Internet governance.

The Security Dilemma in Information

The security dilemma is an inevitable problem when states in an anarchic system with imperfect knowledge about each other observe and respond to the military activities of their rivals. One state's strengthening can be perceived as aggressive and threatening by another state, increasing the second state's sense of insecurity. This response can lead to a self-reinforcing spiral where both sides generate an arms race.

IO may be creating such a spiral. Ironically, both Russia and the US see IW as something that bad foreigners do, but not something they themselves do. US JP 3-13.2 (2010) defined Propaganda as a form of adversary communication, while in Russian military doctrine Information Warfare is used to describe things done to Russians, not what Russia does to other countries.[70] Indeed, the so-called Gerasimov Doctrine that the US military still uses to characterize Russia's approach to IW was not a doctrine at all. Rather, the concept was derived from a talk in which he expressed the view that the Arab Spring and other color revolutions were a form of IW by the US.[71] Yet, despite these disclaimers, both Russia and the US use the IW actions of their adversary to justify their own IW initiatives. China could easily fall into the same pattern if it has not already.

Internet-based social media, which already suffers from a deficit of trust, could be further damaged by an IW arms race in which all rival powers engage in competing, military-backed efforts to "to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives."[72] A descent into mutual IW by major nation-states could make the depredations of commercially-induced spam and phishing look tame by comparison.

Blurring Boundaries

The new doctrines and organizational structures blur the lines between war and peace, military and civilian activity, and foreign and domestic targets. Although that point is too abstract to be stated explicitly in official military doctrine, some military theorists have already asserted as such. 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."[73] A prominent advocate for having an Information Warfare Command in the US military criticized the "pigeonholing of PSYOPS into a narrow organizational area focused on military and warfighting"[74] 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."[75] This implies that operations in the information environment must be perpetual and not confined to specific zones. It is a rather explicit statement that liberal democracies need to mimic the way their adversarial authoritarian states integrate IO functions, which blurs the lines between liberal democracies and authoritarian states.

Cyberspace is so thoroughly connected that a military campaign in the information environment can no longer be targeted at a population easily segmented by nationality or territory. What is the military's role when there is no distinction between an enemy attack and a marketing campaign by a multinational public relations firm? What is the role of the military when a cultural exchange program is considered a form of IO? If the Geneva Conventions require us to differentiate our treatment of civilians and combatants, how does that happen when one is operating on Facebook's territory and everyone's identity is part of an account rather than a country?

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."[76] While it is true that an artillery barrage can be intended to send a signal or shape perceptions, does it also mean that attempts to influence psychology or perception through the exchange of messages are the moral or tactical equivalent of an artillery barrage? If so, such an approach expands our notion of what war is to practically every form of human interaction and in doing so, contributes to the militarization of all information/communications technologies and content. What then happens to the liberal order?

CONCLUSION

This article surveyed changes in US military organization, policy, doctrine, and practice that resulted from the controversies over Russian influence operations. It then explored the implications of these changes for global Internet governance. Along the way, it cataloged the many different labels applied to the military aspects of information, noting an important distinction between activities targeting the cyberspace domain and those targeting the human domain.

Our findings show that, post-2016, policy has moved IO from 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 US capabilities across the cyberspace and human domains. While the Information Warfare label remains contentious, these integrating trends show up across multiple commands. We found evidence that these changes are at risk of eroding the distinction between the information policies and practices of the US and authoritarian regimes. In addition, broader concepts of strategic IW blur the lines between war and peace, military and civilian responsibilities, foreign and domestic targets. Paradoxically, even as they blur these lines, the concept of IW pushes its adherents to impose national borders on Internet exchanges, a tacit embrace of sovereigntist and nationalist cyber norms that the US explicitly rejected less than a decade prior.

NOTES

1. U.S. Senate, Subcommittee on Cybersecurity, April 27, 2017, Hearings on Cyber-enabled Information Operations, https://www.armed-services.senate.gov/hearings/17-04-27-cyber-enabled-information-operations. U.S. Senate, 116th Congress, 1st Session. Report of the Select Committee on Intelligence: Russian Active Measures Campaigns and Interference in the 2016 U.S. Election.
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: 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).
3. Matthew Armstrong, "A Brief History of the Smith-Mundt Act and Why Changing It Matters," MountainRunner.us (blog), February 23, 2012, https://mountainrunner.us/2012/02/history_of_smith-mundt/#.UeBLBD4wY0I.
4. Lawrence Sellin, "The Caldwell information ops allegations: It's just military office politics gone wild." Foreign Policy, February 28, 2011.
5. Jon Lindsay, *Information Technology and Military Power,* Ithaca, NY: Cornell University Press, 2020).
6. 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.; see also the historical list of "Joint Cyberspace Doctrine" definitions in Sarah White, *Subcultural Influence on Military Innovation: The Development of U.S. Military Cyber Doctrine,* doctoral dissertation, Harvard University, Graduate School of Arts and Sciences, 2019, 12.
7. George F. Kennan, "The Inauguration of Organized Political Warfare [Redacted Version]," April 30, 1948, History and Public Policy Program Digital Archive.
8. Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020). PAGE NUMBER?
9. Joint Publication 3-13. Information Operations (27 November 2012 Incorporating Change 1 20 November 2014).
10. Milton L. Mueller, "Against Sovereignty in Cyberspace," *International Studies Review* 22:4 (2020) 779-801.
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.
13. In 1993, General Stiner's successor (General Wayne 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, 12).
14. Lt. Col. Susan L. Gough, "The Evolution of Strategic Influence" (Carlisle Barracks, PA: U.S. Army War College, 2003), https://fas.org/irp/eprint/gough.pdf.
15. USSOCOM, "United States Special Operations Command History: 1987-2007," 22.
16. 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/.
17. Thomas M. Scanzillo and Edward M. Lopacienski, "Influence Operations and the Human Domain," CIWAC Case Studies (Newport, RI: U.S. Naval War College, March 2015), ii https://digital-commons.usnwc.edu/ciwag-case-studies/13.
18. Reports in the military focused on operations in the Philippines, Afghanistan, the Sahel, and operations against ISIS.
19. White, *Subcultural Influence on Military Innovation: The Development of U.S. Military Cyber Doctrine,* 76-77.
20. Secretary of Defense Memorandum, "Changing the Term Psychological Operations (PSYOP) to Military Information Support 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/.
21. Michael V. Hayden, *Playing to the Edge: American Intelligence in the Age of Terror* (New York: Penguin Press, 2016), Chapter 8. This shift seems to have been advanced by NSA leadership without significant institutional buy-in or congressional direction.

NOTES

22. Ibid, 134. Active SIGINT is defined by Michael Hayden as "commuting to the target and extracting information from it, rather than hoping for a transmission we could intercept in traditional passive SIGINT."
23. C. Wiener, "Penetrate, Exploit, Disrupt, Destroy: The Rise of Computer Network Operations as a Major Military Innovation," Ph.D. dissertation, George Mason University, 2016, 156.
24. Ibid, 156.
25. Ibid, 155.
26. White, *Subcultural Influence on Military Innovation: The Development of U.S. Military Cyber Doctrine*, 389.
27. Ibid, 24.
28. Joint Publication 3-13 (2014) defines cyberspace as part of the information environment.
29. Timothy Thomas, "Russia's 21st Century Information War: Working to Undermine and Destabilize Populations," *Defense Strategic Communications: The Official Journal of the NATO Strategic Communications Center of Excellence,* 1:1 (2015) 10-25.; Mark Galeotti, "The 'Gerasimov Doctrine,' and Russian Non-Linear War." Peter Pomerantsev, "How Putin is reinventing warfare," Foreign Policy, May 5, 2014. Pomerantsev's original article was widely reproduced, https://foreignpolicy.com/2014/05/05/how-putin-is-reinventing-warfare/.
30. Mark Galeotti, "I'm sorry for creating the 'Gerasimov Doctrine,'" *Foreign Policy,* March 5, 2018. Page number?
31. Office of the Director of National Intelligence, Russia's Influence Campaign Targeting the 2016 U.S. Presidential Election (January 6, 2017).
32. H.R.3622 - 99th Congress (1985-1986): Goldwater-Nichols Department of Defense Reorganization Act of 1986, https://www.congress.gov/bill/99th-congress/house-bill/3622.
33. Donald J. Trump, "National Security Strategy of the United States of America" (Executive Office of the President, December 18, 2017), 34.
34. Ibid, 31.
35. Ibid, 14.
36. Ibid, 37.
37. 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.
38. Ibid, 3.
39. Ibid, 3.
40. 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.
41. H.R.5515 - 115th Congress (2017-2018): John S. McCain National Defense Authorization Act for Fiscal Year 2019, https://www.congress.gov/bill/115th-congress/house-bill/5515/.
42. S.1790 - National Defense Authorization Act for Fiscal Year 2020, 116th Congress (2019-2020). https://www.congress.gov/bill/116th-congress/senate-bill/1790
43. H.R.2500 - 116th Congress (2019-2020): National Defense Authorization Act for Fiscal Year 2020, https://www.congress.gov/bill/116th-congress/house-bill/2500/.
44. Joint Publication 1, Doctrine for the Armed Forces of the United States. 25 March 2013 Incorporating Change 1 12 July 2017 (hereafter, JP-1).
45. JP-1, xii.
46. JP-1, I-18.
47. JP-1, I-19.
48. White, *Subcultural Influence on Military Innovation: The Development of U.S. Military Cyber Doctrine*, 53.
49. JP-1, I-19.
50. Joint Chiefs of Staff, "Joint Concept for Operating in the Information Environment (JCOIE)" (Washington, DC, July 25, 2018).
51. Ibid, ix.

NOTES

52. Ibid, vii-viii.
53. Ibid, 40.
54. H.R.2500 - 116th Congress (2019-2020): National Defense Authorization Act for Fiscal Year 2020. The 2020 NDAA 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.
55. Lackland AFB also hosts the Joint Information Operations Warfare Center, which coordinates information operations.
56. 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.
57. Ibid, 22.
58. Ibid, 24.
59. Mark Pomerleau, "U.S. Army emphasizes 'information advantage'," C4ISRNet.com, May 5, 2021, https://www.c4isrnet.com/information-warfare/2021/05/25/us-army-emphasizes-information-advantage/
60. U.S. Marine Corps Forces Cyberspace Command, "Marine Corps Creates First Information Group to Prepare for Modern Battlefield," accessed August 11, 2021, https://www.marforcyber.marines.mil/News/Article/1407775/marine-corps-creates-first-information-group-to-prepare-for-modern-battlefield/.
61. Ibid.
62. 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/.
63. Ellen Nakashima, "U.S. Cybercom Contemplates Information Warfare to Counter Russian Interference in 2020 Election," *The Washington Post,* December 25, 2019.
64. Fogarty and Sparling, "Enabling the Army in an Era of Information Warfare."
65. Crane, "The United States Needs an Information Warfare Command: A Historical Examination."
66. The full text of the SCO proposal can be found here: https://undocs.org/A/66/359. The SCO Code was revised and resubmitted to the UN in 2015.
67. Ibid.
68. Donald J. Trump, "Executive Order on Addressing the Threat Posed by TikTok," Executive Office of the President, August 6, 2009.
69. U.S. support for the administration of the domain name system by the Internet Corporation for Assigned Names and Numbers (ICANN), and the decision to release ICANN from U.S. Commerce Department supervision in 2016 are examples of its commitment to a global governance approach.
70. 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.
71. *Military-Industrial Courier* (February 2013), https://www.vpk-news.ru/articles/14632.
72. This is the definition of "PSYOPS" from JP-1.
73. Lauren Elkins, "The 6th Warfighting Domain," *Over the Horizon*, November 5, 2019, https://othjournal.com/2019/11/05/the-6th-warfighting-domain/.
74. Crane, "The United States Needs an Information Warfare Command: A Historical Examination."
75. Ibid.
76. Major General Graham Binns, General Officer Commanding, 1st (UK) Armoured Division, cited in the JCOIE (2018), 16.