Military Authorizations in a Connected World: DoD's Role in Cyber Influence Operations

Michelle Albert
Tom Barth
Dr. George Thompson

ABSTRACT

The open nature of the Internet, allowing the unprecedented free flow of information, has given rise to a new type of attack surface. Cyber activities in the gray zone, which falls between diplomatic engagement and military action, includes disinformation campaigns and influence operations. These activities raise questions regarding responsibility and proportionate response. This article examines the distinction between influence operations and more traditional conflict, specifically in a gray zone of blended activity. It also addresses the role and authorities of the Department of Defense (DoD) governing cyberspace activity. Deterring and countering adversary influence operations require a multipronged approach of regulation, education, and government agency action to focus agency authorities and resources where they are needed most. DoD has the technical resources to lead the government's efforts to counter and deter such operations but is limited by policy and law. This article considers how DoD can effectively operate under its Title 10 and Title 50 authorities in the gray zone and introduces a heuristic construct for the role of influence operations in the continuum of conflict.

Michelle Albert is a Research Associate in the Information Technology and Systems Division at the Institute for Defense Analyses. Prior to that, she worked as a speechwriter for the Department of Defense Chief Information Officer. She has an M.A. in Journalism.

INTRODUCTION

The global balance of power has changed dramatically in the past two decades. While the US military was focused on the Middle East, Russia and China focused on great power competition, spending considerable time and effort developing substantial cyber capabilities and the supporting doctrines for their use. The US Intelligence Community's (IC) "high confidence" that Russia's Internet Research Agency conducted a sophisticated influence campaign in the run-up to the 2016 US Presidential election[1] informed the public of an Internet-based attack surface that is difficult to understand, categorize, bound, or defend and that presents a rash of new vulnerability risks to US national security.

The open nature of the Internet blurs boundaries and responsibilities. Foreign-led cyber campaigns with a major domestic impact, like Russia's in 2016, create confusion regarding who has the authority to respond. Cyber activities like these occur in the gray zone,[2] which falls between diplomatic engagement and military action and rely on Internet anonymity and the lack of accepted international standards or norms for cyber activity to discourage a conventional military response. Gray zone cyber threats include espionage, threats to critical infrastructure, disinformation campaigns, and influence operations, and originate from foreign and domestic sources. While government responsibilities in the US are traditionally split between foreign and domestic threats and by the type of threat, this split does not directly translate to cyberspace.

This article examines media- and technology-driven disinformation campaigns and influence operations in the context of established trends in military doctrine and gray zone activities. It considers the relationship between influence operations and a traditional state of war, specifically techniques that fall both inside and outside Title 10 authorities for US military activities and Title 50 authorities for intelligence activities.

Tom Barth is a Research Staff Member in the Information Technology and Systems Division at the Institute for Defense Analyses. He previously served as a U.S. Army Infantry officer, with final active duty assignment as Chief, Future Operations, U.S. Army Cyber Command. He is a graduate of the U.S. Military Academy, the U.S. Army Command and General Staff College's School of Advanced Military Studies, and the U.S. Army War College.

This article also addresses those instruments of national power that should be responsible for defending against foreign influence operations.

Doctrine Development in a Changing World

The character of war is subject to change. War is an interaction between communities, and its character depends on the tools and technologies used to shape those interactions.[3] The DoD's *2018 National Defense Strategy* recognizes that the current and future operational environments are "affected by rapid technological advancements and the changing character of war."[4] The microelectronics revolution is central to these technological advancements as it has changed how society collects, manages, and acts on information, both in civilian life and during defense and intelligence activities.

Microelectronics-based technologies have been developed at a rapid pace that far outstrips the development of governing regulatory and usage frameworks in the civilian sector. Predicting new applications of microelectronics is difficult, especially if the applications are disruptive or differ qualitatively from prior applications. The current trend in emerging technologies facilitating the tracking of individual opinions, biases, interests, and beliefs will continue. Recent use of social media to sow discord in targeted populations exemplifies these difficulties.

THE EVOLUTION OF INFLUENCE OPERATIONS

Characteristics of Information Operations and Influence Operations

DoD defines *information operations* as "the integrated employment, during military operations, of information-related capabilities[5] 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."[6] Military operations include defense support of civil authorities, peace

Dr. George Thompson is a Research Staff Member in the Information Technology and Systems Division at the Institute for Defense Analyses, and previously worked in the semiconductor industry. He has a Ph.D. in Physical Chemistry.

Dr. George Thompson passed away before publication of this article.

operations, noncombatant evacuation, foreign humanitarian assistance, and nation building.[7] Authority to conduct information operations involves a detailed and rigorous legal interpretation of authority and/or the legality of specific actions.[8]

Information operations occur within the *information environment*, which DoD defines as "individuals, organizations, and systems that collect, process, disseminate, or act on information."[9] They also comprise different types of operations. *Psychological operations* involve the use of propaganda to shape the motives and behavior of a government, group, or individuals. *Military deception* uses false information or disinformation to mislead.[10] *Cyberspace operations* involve "employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."[11] These objectives range from accessing information, to spreading information (or disinformation), to creating some physical effect, such as attacking critical infrastructure. DoD doctrine separates cyberspace operations and information operations, but they are inextricably linked. Cyberspace is where many information operations occur today.

DoD lacks a formal definition of influence operations, which, for purposes of this article, refers to use of information, whether true or false, as propaganda, misinformation (unintentionally false information), and disinformation (intentionally false information) to achieve a desired outcome. According to RAND, *influence operations* refers to the coordinated application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and post-conflict to foster and promote certain attitudes, decisions, or behaviors in a target audience.[12] Influence operations may take place during either military operations or gray zone activities, and its practitioners reside in military, government, and private sector organizations that cooperate to various extents.

Figure 1, below, highlights the differences between DoD-defined information operations and influence operations. Target audiences range from individuals, to groups, to entire populations, and there are varying methods for reaching an intended target. Influence operations have two main components: the message and the delivery method. One method is the use of regulated mass media, such as TV, newspapers, radio, etc., to reach the broadest possible audience. However, using mass media subjects a message to editing and often creates a means for determining the message's provenance. Another method is to use less regulated means of communication to ensure the message is unadulterated and difficult to trace back to its creators. These means include flyers, posters, word of mouth, postings on social media sites or other message boards, and using anonymizing software such as TOR to hide or obfuscate a user's identity online.[13]

Influence Operations = (Information Operations – Physical Effects) + Misinformation + Disinformation

Figure 1. Information and Influence Operations

Conducting effective influence operations requires thorough knowledge and understanding of the target audience's demographics, ideals, beliefs, attitudes, values, decision-making processes, and receptiveness to information. The source of the information needs to appear authentic and credible to gain the audience's trust, and the information itself must be packaged for maximum appeal.[14] The environment today is saturated with information. To succeed, any influence operations campaign must reach the target audience.

How Technology Has Affected Influence Operations

While the basic tenets of propaganda and influence operations remain the same over time, the Internet has changed how they are employed and how information is presented and consumed. This change is a strategic inflection point in technology development that created a new attack surface for influence operations.

Internet site owners, publishers, and advertisers rely on algorithms that control content seen by users on search engines and social media sites. The algorithms gather as much information about users as possible, including location, age, education, political beliefs, contacts, pop culture preferences, and what posts garner the most likes or activity. The algorithms then tailor content to suit each user's preferences while also considering whether the site was paid to promote a post and how other people in the user's network interact with a post.[15] Personalized content drives continued use of the site, which increases advertising revenues and gives the algorithm even more information. Algorithms are unconcerned whether a post is true, false, innocuous, provocative, or extremist, as long as it fosters engagement.[16]

The Internet's immediacy and ease of access also precipitated the rise of niche publications and blogs that cater to specific audiences. These sites foster communities of people with similar personal identities, interests, hobbies, or ideologies. These online communities are known as "echo chambers," which have become a hallmark of social media sites. Echo chambers, driven

by algorithmic tailoring, validate and amplify an individual's existing beliefs and opinions to the exclusion of narratives that challenge them. It is now easier than ever to find communities of like-minded people online and to be isolated from differing opinions.

THE CURRENT INFLUENCE OPERATIONS ENVIRONMENT

Social Media

Today, 70 percent of Americans use some form of social media.[17] More than half of all social media users use such sites for news, and one in 10 users relies on social media as their only news source.[18] Social media users can pull content they deem interesting or relevant and share it with others, rather than relying on news organizations and publications to push content to them.[19]

This has sparked a rise in citizen journalism. Users not affiliated with a news organization are able to post pictures and video of an event or spread breaking news, providing valuable eyewitness accounts of events as they happen. News of the 2008 attacks in Mumbai, for example, broke over Twitter, with pictures posted to Flickr, a photograph-sharing site.[20] Video, such as the cellphone videos exposing police brutality and racism,[21] has provided evidence for indictments and criminal cases and reshaped national narratives on police behavior and accountability.

False or misleading information, whether mistakenly shared by citizen journalists or deliberately spread to manipulate others, is often more novel than true information, and presented in a manner meant to provoke outrage, which further entices engagement.[22] Also, interacting with false information can lead users to follow algorithmically generated threads known as "rabbit holes."[23] Since the initial search terms are based on false information or unsupported ideas, the algorithm is likely to generate related threads of polarizing information that can incite calls to action in the real world. Increasingly, what happens online has real-world effects. In the summer of 2018, two dozen people in India were killed by lynch mobs because they were suspected of participating in child-kidnapping rings or plots to harvest organs. The mobs were fueled by unfounded rumors spread on WhatsApp, an encrypted messaging Facebook platform.[24]

Twitter has been used to coordinate disaster response efforts, organize grassroots political campaigns, harass journalists and other public figures, foment revolution, and affect jobs. The #MeToo movement revealed episodes of sexual harassment and assault perpetrated by prominent individuals, and in some cases resulted in criminal investigations and trials. The #MeToo movement also sparked a nationwide discussion of harassment, power dynamics, and appropriate behavior in the workplace.

The IC concluded in 2018 that Russia sponsored a major hacking, disinformation, and political ad campaign to interfere in the 2016 US Presidential election. Special Counsel Robert Mueller, who was assigned to investigate Russian interference in the 2016 Presidential election and

possible links between Russian officials and Trump associates, filed indictments charging 35 individuals related to his investigations.[25],[26] Social media are also prime grounds for terrorist group recruitment and radicalization. The Islamic State of Iraq and al-Sham (ISIS), also known as the Islamic State of Iraq and the Levant (ISIL), ran a sophisticated, multifaceted propaganda campaign to glorify its mission and make life under the caliphate seem like paradise.[27] Recruiters used social media to establish relationships with potential recruits, establishing a sense of intimacy and camaraderie to manipulate recruits into joining.[28]

Some recent lone-wolf terrorist attacks, including the plague of mass shootings terrorizing the US, have roots in online communities and social media sites. Some online communities—echo chambers that validate perceived grievances and advocate violence in response—encourage shootings or other violent acts. Dylann Roof, who shot and killed nine African Americans in the Emanuel African Methodist Episcopal Church in Charleston, South Carolina, in June 2015, self-radicalized using white supremacist and neo-Nazi websites.[29] Google's algorithm led him to sites peddling racist propaganda and falsified statistics about black-on-white crime.[30] Roof immersed himself in these sites before committing mass murder.

The Current Environment Renders the US More Vulnerable to Adversary Influence Operations

The continuously expanding Internet creates an ever-growing and ever-changing attack surface. With more people online and more places for them to communicate come more opportunities to spread fake news or narratives meant to manipulate people[31] while increasing mistrust of fact-based media. Mistrust is largely based on perceived bias in the news or of a powerful publication pushing a particular agenda.[32] Political polarization generates mistrust, no matter a publication's commitment to fact checking and other journalistic standards. Many Internet users find it increasingly difficult to distinguish between the opposing poles of factually real news and factually false news. Instead, they believe that the news lies along a spectrum with real news at one end and fake news at the other.[33] Social media algorithms provide an easy conduit for such information. A search that begins with innocuous content can quickly lead to propaganda or even content espousing hate speech or promoting violence. Algorithms are also increasingly able to target small, specific groups of people. The Russian Internet Research Agency's propaganda campaign in 2016 used algorithmic targeting to identify and obfuscate discussions of current issues, recognizing that exploiting existing divisions is easier than creating new ones.

TECHNOLOGY AND THE EVOLVING THREAT

Technology in Today's Information Environment

The current information environment is marked by the confluence of cyber capabilities and influence operations. Artificial intelligence (AI) makes automated programs (bots) appear more human-like, making it difficult to differentiate between real users and bots. Social engineering

campaigns take advantage of human nature and are based on traditional propaganda methods. Many of these methods have become ubiquitous, and many over time have learned how to identify and ignore the most blatant examples. But the recent revolution in data management has changed this paradigm.

Because of the historical, exponential increase in computer functionality for a given cost, the amount of personal data in the public sphere today is unprecedented (and predicted by Moore's Law).[34] In this interconnected world, where almost everyone has a cell phone and is engaged with social media, where most emails are scanned for content, and where records of electronic financial transactions are vacuumed up, digital footprints can be tracked easily by social media and advertising companies seeking profit. Buying or selling data is a lucrative activity. The expansion of semiconductor-based products (e.g., computers, smartphones, and cars) will most likely continue for the foreseeable future, making collection and analysis of digital footprints even more pervasive than it is now.[35]

Nefarious foreign actors have been using some of these data in social engineering and influence operations efforts against the US; Russia's interference in the 2016 US Presidential election is the most prevalent example.[36] Recent advances in AI, image and video analysis, and data mining, combined with the technology of the coming decade, open up the potential for more powerful influence operations. Advanced computing may well enable targeted advertising messages delivered by email or telephone that are indistinguishable from messages sent by humans, and use detailed psychological profiles to tailor messages to specific targets.

Technology today can be divided into three frameworks: sensing, processing, and acting. Sensing relates to the means for gathering data. Processing is both storing and accessing the data and analyzing those data to discover and extract useful information. Acting relates to how that information is used. Cyberspace is littered with sensors, even to the extent of tracking users as they read. That information is then rapidly processed and added to the users' existing online profiles, which strongly influence what articles and advertisements users are steered toward.

Data collection and analysis can instigate and influence action, such as in boosting security, preventing criminal activity, or tracking disease outbreaks. Data mining and analytics tools such as Palantir[37] collect information from emails, financial documents, phone records, and other sources to search for potential links. Palantir has been used to predict the deployment of improvised explosive devices (IED), detect fraud, conduct criminal investigations, track complex financial transactions, and screen airport travelers. Tools like Palantir have been a boon for security organizations, but they also present risks and challenges, partly because they lack a mechanism to determine the validity of collected information, which may affect the tool's predictions. Incorrect and misleading information collected in Palantir has resulted in mistaken arrests.[38]

The Future Environment

The global trend toward universal surveillance will continue as more technologies track our activity online and offline. Increased networking and data collection expand the potential attack surface. More data mean more information about potential targets and target groups. More online systems mean more access points to exploit. A society's surveillance capability, either government or private sector, could be weaponized and used against it for a cyberattack or influence operations campaign.

It will become increasingly difficult to determine authenticity of information online. Audio and video recordings provide an eyewitness view into events and have corroborated or invalidated witness accounts of what actually happened. Moreover, it is becoming easier to create faked audio and video that are almost indistinguishable from the real thing. Known as *deepfakes*, these audio and video clips enable malicious actors to make it seem like someone did or said something that he or she never did or said, opening up myriad avenues for disinformation.[39] A very common type of deepfake today is the grafting of a celebrity's head onto a porn actor's body. However, it would be an easy transition to deepfakes meant to destroy reputations, rig elections, erode trust in public institutions, and jeopardize national security.

There is no single answer or method for employing defensive measures against the risks of this future environment. Increased connectivity brings greater risk, and each organization or individual accessing networked systems and resources must weigh the desire for convenience against the need for privacy and security. Addressing future risks and opportunities requires both government and private sector participation, and a multi-pronged approach of legislation, regulation, education, and government agency action. Broad regulation is a government responsibility that may require restricting dissemination of online information. Education and media literacy campaigns can arm the public with tools that help flag disinformation and help people think more critically about what they are seeing. Stopping current campaigns and deterring new ones also require further action. A whole-of-government approach to fighting disinformation, coupled with public and private sector collaboration, will focus authorities and resources where they are needed most. DoD has the technical resources to lead such an effort but is limited by policy and law. Partnering with other agencies and private organizations will likely enable the DoD to provide cyber capabilities and expertise when and where needed.

ADDRESSING THE CURRENT THREAT

DoD's Role

The *2018 National Defense Strategy* recognizes that the US military must operate in "an increasingly complex global security environment" and use "areas of competition short of open warfare (e.g., information warfare, ambiguous or denied proxy operations, and subversion)" to achieve our ends.[40] To counter coercion and subversion in competition short of conflict, DoD supports US Government (USG) interagency efforts and works by, with, and through allies and

partners to secure national interests.[41] Such a strategic approach suggests DoD either does not or should not have a leading role in the government's efforts to counter adversary information operations, save for information operations that directly target US forces.

Title 10 and Title 50 Authorities

Titles 10 and 50 of the U.S. Code refer to statutory authorities governing DoD and the IC. Title 10 delineates the functions, duties, and responsibilities of the US military and gives the Secretary of Defense (SECDEF) control over all DoD agencies and commands. It also establishes the combatant commands (COCOM) and gives them statutory authorities, which all report directly to the SECDEF.[42] Title 50 establishes the IC's authorities, and constitutes CIA's authority to conduct intelligence operations and covert actions. Title 50 also establishes Secretary of Defense control over intelligence agencies within DoD, including NSA and the Defense Intelligence Agency (DIA).[43]

While both are subject to Congressional oversight, one difference between Titles 10 and 50 is the need for Congressional notification. Title 10 activities are overseen by the House and Senate Armed Services Committees (HASC and SASC, respectively), and Title 50 activities are subject to oversight by the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI).[44] Nevertheless, Title 50 IC activities require advance notice to Congress, while military activities under Title 10 do not.[45] Another key difference is international protection of sovereignty. Intelligence agencies operating outside the US in covert action status under Title 50 have reasonable claim to international law protection of sovereignty because covert action status carries a statutory obligation to comply with the Constitution and US statutes, but nothing else. Title 10 does not carry the same "implicit statutory shield" against international law objections.[46]

Questions of oversight and responsibility arise when actions could reside under either Title 10 or Title 50. Historically, Congress and executive agencies have viewed Title 10 and Title 50 as separate entities. Yet these Titles themselves, as well as Secretary of Defense authorities under both, suggest otherwise. Some activities fall under either Title, depending on their command and control, funding, and mission intent.[47] IC and DoD both conduct intelligence gathering, generally viewed as falling under Title 50, but intelligence gathering is included under both Title 10 and Title 50. The SECDEF can direct DoD organizations and personnel to execute intelligence activities. Activities meant to fulfill national intelligence requirements fall under Title 50, and if they meet military intelligence requirements, or are used to prepare for an organized conflict, they fall under Title 10. Military intelligence operations in support of taskings from the Director of National Intelligence (DNI) fall under Title 50 and must be reported, but intelligence activities in support of SECDEF taskings are considered Title 10. Furthermore, activities by DoD entities that are also members of the IC fall under both Titles 10 and 50.[48]

In modern operations, particularly in cyberspace operations, convergence of Titles 10 and 50 activities becomes more apparent. Exploiting a network or system to gather information but not to alter, control, or degrade the function of that network or system is generally considered

an intelligence activity, and international law does not consider intelligence activities to be acts of war. On the other hand, exploiting a network or system in order to alter, control, or degrade its function surpasses that threshold and is more likely to be subjected to international law constraints.[49] (In the gray zone, rules of engagement for US cyber operations remain fuzzy and undefined.[50]) Yet, cyber operations often require intelligence gathering to assess a network or system in preparation for an attack. Moving from one activity to another—from Title 50 to Title 10—especially when operating in a foreign country, exposes potential international law issues. Part of the challenge is that cyberspace operations often happen quickly: a fleeting opportunity may arise, that cannot await legal authorization, especially if foreign governments need to consent.

Title 10-Title 50 convergence also raises questions as to who is responsible for intelligence gathering and other cyber operations. The United States Cyber Command (USCYBERCOM), the unified combatant command responsible for cyberspace operations, partners with NSA. The Commander, USCYBERCOM, is also the NSA Director, thereby underscoring the ties between the two organizations. Historically, NSA has been the USG's lead for cyber operations, but USCYBERCOM's responsibility and authority are growing. Convergence is complicated for cyber operations and is even more complicated for information operations.

Current Activities

The 2019 National Defense Authorization Act (NDAA) expanded USCYBERCOM's statutory authorities.[51] The NDAA modifies parts of Title 10 to empower the DoD to conduct cyber operations short of hostilities[52] and in areas where "hostilities are not occurring,"[53] and defines clandestine military activity in cyberspace as "a traditional military activity."[54] The designation of clandestine online activity as traditional military activity removes the oversight required by Title 50. The NDAA also empowers USCYBERCOM to conduct cyber operations that respond to foreign country cyberattacks, but only if those attacks meet two conditions: they constitute "an active, systematic, and ongoing campaign of attacks against the USG or people of the US in cyberspace, including attempting to influence US elections and democratic political processes."[55] Section 1642 of this NDAA restricts this authority to respond to attacks coming from Russia, North Korea, China, or Iran.[56]

USCYBERCOM's actions to protect the 2018 US midterm elections and the 2020 Presidential election, both the subject of repeated foreign adversary attacks, could provide a framework for how the DoD fights disinformation. In each election cycle, USCYBERCOM worked with other combatant commands, such as the Department of Homeland Security (DHS), the Department of the Treasury, and the FBI, and partnered with allied nations to find instances of foreign interference in the election process.[57] To combat 2018 midterm disinformation, USCYBERCOM and NSA created the Russia Small Group task force to deter and protect against Russian disinformation and cyberattacks.[58] On election day, the task force blocked Internet access to the Internet Research Agency in St. Petersburg, long identified as the locus of Russia's disinformation campaign against the US.[59] The task force has since been made permanent.

Creating a Cybersecurity Agency

Another way to counter and deter disinformation would be to create a single government cybersecurity agency. The acknowledgment of cyberspace as a warfighting domain and the intricacies of its related attack surface suggest a need for a new agency focused on this particular threat. Agencies that must fulfill other traditional responsibilities and missions may, with the newer cyber-related missions, be stretched thin. A single, focused, cybersecurity agency that consolidates law enforcement, intelligence activities and the authorities related to cyber activity from both foreign and domestic sources could be more agile and mission-focused, and thereby serve as a hub for top cybersecurity talent. This agency would lead all cyber-focused activities and support other agencies as needed.[60]

Promoting partnerships among existing government cyber resources may advance collaboration among agencies and strengthen existing relationships with the private sector, which has a larger bench of cybersecurity talent and owns the most influential Internet platforms (e.g., Facebook, Twitter, Amazon). This would also facilitate relationships with key government personnel from affected sectors that have no cybersecurity-focused missions. USG cyber expertise today is spread among agencies, with some overlap in mission—for example, intelligence centers such as the Defense Cyber Crime Center (DC3) and the Cyber Threat Intelligence Integration Center, where agency-specific cyber resources can develop specialized skills tailored to specific missions. Increased collaboration among these resources would provide support when and where needed, without the extra cost and upheaval of establishing a new agency.[61] Today, the Authorities that handle domestic or foreign threats are split up among agencies. Combining these authorities into a new agency would mirror the current confusion regarding Title 10 and Title 50 convergence within DoD. The IC and law enforcement agencies separately are dedicated to domestic and foreign activities. Combining these disparate authorities at best would be challenging.

Adopt a Heuristic Construct for Conflict

The onslaught of foreign surveillance into US critical infrastructure and intrusions into social media takes us beyond the question: "How do we deal with these intrusions?" to the question: "Are we at war, and we did not realize it?" Prussian war theorist Carl von Clausewitz argued that the nature of war describes its unchanging essence, and the character of war describes how as a phenomenon it manifests in the real world. War's nature is violent, interactive, and fundamentally political. War's conduct is influenced by technology; law; ethics; culture; methods of social, political, and military organization; and other factors that change across time and place.[62] Understanding the complexity and differences among the various approaches to warfare is critical for understanding adversaries, their methods, and their concepts for victory. US military doctrine so far has successfully evolved to meet the challenges of conventional warfare, irregular warfare, and terrorism. This evolution must continue.

By definition, a hallmark of all gray zones is a blurring of boundaries and responsibilities. The new battle space spans the public and private sectors and encompasses media outlets, social media sites, a range of technologies, and individual citizens. What constitutes a cyberspace attack is yet to be concretely defined (perhaps excepting cyberattacks that cause physical effects). Consequently, it is difficult to determine a response acceptable under international law to incursions into US networks, even when the effects of such incursions have been profound. This new warfare domain does not neatly adhere to current doctrinal definitions. To embrace the changing conduct of war, the US military should adopt a heuristic construct for conflict—as depicted in Figure 2—and abandon any binary peace/war distinction.[63]

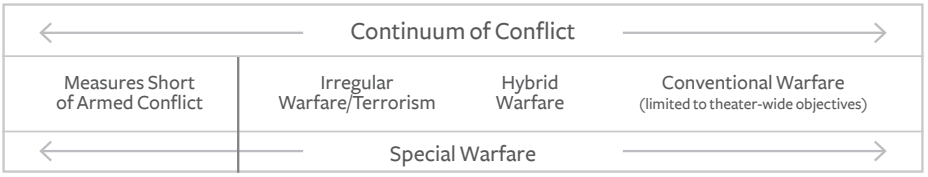

Figure 2. Continuum of Conflict [64]

Given the nebulous nature of the gray zone, it is difficult to define the battle space, much less victory, in the context of influence operations. In fact, the concept of victory might better be stated as maintaining an advantage. Battling influence operations campaigns requires a three-pronged approach of regulation, education, and public-private collaboration. Broad regulation is a government responsibility; that social media companies operating in Europe are already complying with European Union (EU). regulations shows that it is feasible that they can comply with similar US regulations.[65] Education and media literacy campaigns give the public tools to help identify disinformation and think critically about the information they see and interact with online. However, it is not enough to arm the public with the knowledge of these campaigns; we need to stop current campaigns and prevent new ones.

Doing so would require the USG's involvement and a collaborative approach with the private sector. Individual agencies have particular areas of focus and responsibility, and a whole-of-government approach to fighting disinformation would focus agency resources and expertise where they are needed most. DoD has the resources and abilities to take the technical lead but is limited by policy and law. Partnering among DHS, FBI, and other agencies would enable DoD to provide cyber capabilities and expertise where needed, and this must continue and expand. DoD partners with the Department of State's Global Engagement Center, which is charged to "lead, synchronize, and coordinate efforts of the federal government to recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining US national security interests."[66] USCYBERCOM and NSA's Russia Small Group task force, as well as USCYBERCOM's partnerships with allied nations and US government agencies, present a model for future DoD involvement in blunting disinformation. USCYBERCOM's Joint Task Force Ares has partnered with NSA to act as a hub for whole-of-government cyber planning.[67]

USCYBERCOM's pre-authorization to conduct cyber operations against cyberattacks from certain foreign countries defines a proportionate response in specific instances. Establishing that the US can and will respond to an attack is part of an effective deterrent, but defense requires a different approach. Effective defense against influence operations requires the Secretary of Defense to exercise both Title 10 and Title 50 authorities. In the gray zone, questions for DoD are how to operate under these authorities, and when to use them. It may be that finding a means of straddling domestic and foreign activities—like the Coast Guard's jurisdiction covering both domestic and international waters—would be an effective approach, as foreign-led disinformation campaigns, such as Russia's in 2016 and 2018, often spur domestic action online and in the real world.

CONCLUSION

Today we are in a reactive state, scrambling to keep pace with technology and respond to its effects. In the microelectronics arena, new and unforeseen applications of rapidly evolving technology are commonplace. It is not uncommon for new technologies or new applications of existing technologies to create a temporary advantage for innovators and early adopters while defensive technologies, policy, and doctrine adjust.

The limitations and constraints expressed in policy and in DoD's military doctrine make it difficult to incorporate DoD in a whole-of-government response to adversary influence operations in an environment short of war. For DoD, information operations are key to winning the battle of the narrative, which pits adversary attempts to influence the perception of different populations against US efforts to do the same.[68] The battle of the narrative is an integral part of irregular warfare and requires creating a coherent message, working with the host nation or local partner to boost their legitimacy, disseminating the message to the local population and other key audiences, and delegitimizing the adversary's message and goals.[69]

The battle of the narrative, however timeless, is applicable beyond irregular warfare. The emergence of the gray zone and the blurring of what constitutes wartime and peacetime activity have instigated a constant battle to control the narrative and influence the ideas and actions of target populations. To respond to adversary influence operations short of conflict, DoD will need to be imaginative within the bounds of law, policy, and capabilities to integrate information operations and cyberspace capabilities to counter and contest its adversaries globally.[70]

The capability to prevent, contest and prevail in influence operations campaigns needs to become a national priority. Special Counsel Robert Mueller's testimony to the House Judiciary and Intelligence Committees on July 24, 2019 issued a warning about election interference: the 2016 election interference "wasn't a single attempt. They're doing it as we sit here."[71] Election interference and other influence operations campaigns are going to continue to expand in scope and affect our society and way of life.

NOTES

1. Intelligence Community Assessment (ICA), January 6, 2017, "Assessing Russian Activities and Intentions in Recent US Elections," ICA 2017-01D, https://www.dni.gov/files/documents/ICA_2017_01.pdf.
2. The gray zone refers to "employing instruments of power—often asymmetric and ambiguous in character—that are not direct use of acknowledged regular military forces" (International Security Advisory Board (ISAB,) January 3, 2017, *Report on Gray Zone Conflict*, https://www.state.gov/documents/organization/266849.pdf).
3. Z.T. Brown, March 12, 2019, "Unmasking War's Changing Character," Modern War Institute, https://mwi.usma.edu/unmasking-wars-changing-character/.
4. Department of Defense, 2018, *Summary of the 2018 National Defense Strategy of the United States of America*, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.
5. *An information-related capability* (IRC) is a "tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions," Joint Publication 3-13, November 27, 2012, *Information Operations*, incorporating Change 1, November 20, 2014.
6. Ibid.
7. Ibid.
8. Ibid.
9. Ibid.
10. C.A. Theohary, March 5, 2018, CRS Report 7-7500, "Information Warfare: Issues for Congress," Congressional Research Service.
11. Joint Publication 3-12, June 8, 2018, *Cyberspace Operations.*
12. E.V. Larson, et al., 2009, "Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities," RAND, https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG654.pdf.
13. Ibid.
14. Ibid.
15. A. Hern, May 22, 2017, "How social media filter bubbles and algorithms influence the election," *The Guardian*, https://www.theguardian.com/technology/2017/may/22/social-media-election-facebook-filter-bubbles.
16. M. Fischer and A. Taub, April 25, 2018, "How Everyday Social Media Users Become Real-World Extremists," *The New York Times*, https://www.nytimes.com/2018/04/25/world/asia/facebook-extremism.html.
17. A. Perrin and M. Anderson, April 10, 2019, "Share of U.S. adults using social media, including Facebook, is mostly unchanged since 2018," Pew Research Center, https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018/.
18. S. Bradshaw and P.N. Howard, January 29, 2018, "Why Does Junk News Spread So Quickly Across Social Media? Algorithms, Advertising and Exposure in Public Life," *Knight Foundation*, https://kf-site-production.s3.amazonaws.com/media_elements/files/000/000/142/original/Topos_KF_White-Paper_Howard_V1_ado.pdf.
19. Ibid.
20. C. Beaumont, November 27, 2008, "Mumbai attacks: Twitter and Flickr used to break news," T*he Telegraph*, https://www.telegraph.co.uk/news/worldnews/asia/india/3530640/Mumbai-attacks-Twitter-and-Flickr-used-to-break-news-Bombay-India.html.
21. G. Denby, October 18, 2014, "Videos of Deadly Police Encounters Grab the Media Spotlight, but Why?" *NPR*, https://www.npr.org/blogs/codeswitch/2014/10/08/354507430/videos-of-deadly-police-encounters-grab-media-spotlight.
22. S. Vosoughi, D. Roy, and S. Aral, March 9, 2018, "The spread of true and false news online," *Science,* 359, 1146-1151.
23. The term "down the rabbit hole" originated with Lewis Carroll's book *Alice in Wonderland*, in which Alice falls into and down a rabbit hole that eventually leads her to Wonderland. Today, the term "rabbit hole" refers to "a complexly bizarre or difficult state or situation conceived as a hole into which one falls or descends," especially "one in which the pursuit of something (such as an answer or solution) leads to other questions, problems, or pursuits, " "rabbit hole," *Merriam-Webster Dictionary*, https://www.merriam-webster.com/dictionary/rabbit%20hole, accessed October 1, 2019.
24. E. Dwoskin and A. Gowen, July 23, 2018, "On WhatsApp, fake news is fast—and can be fatal," *The Washington Post,* https://www.washingtonpost.com/business/economy/on-whatsapp-fake-news-is-fast--and-can-be-fatal/2018/07/23/a2dd7112-8ebf-11e8-bcd5-9d911c784c38_story.html?noredirect=on&utm_term=.05a5faed4172.

NOTES

25. Department of Justice Office of Public Affairs, February 16, 2018, "Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System," https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere.
26. M. Kahn, July 13, 2018, "Document: Special Counsel Indicts 12 Russian Intelligence Officers for Hacking DNC and Clinton Campaign," *Lawfare*, https://www.lawfareblog.com/document-special-counsel-indicts-12-russian-intelligence-officers-hacking-dnc-and-clinton-campaign.
27. B.I. Koerner, 2016, "Why ISIS Is Winning the Social Media War," *Wired*, https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat/#slide-5.
28. A. Erelle, June 2, 2015, "How One Journalist Found Herself Courted by ISIS," *Vogue,* https://www.vogue.com/article/in-the-skin-of-a-jihadist-isis-recruitment-network-excerpt-anna-erelle.
29. C. Collins, 2017, "The Miseducation of Dylann Roof," *Teaching Tolerance*, https://www.tolerance.org/magazine/fall-2017/the-miseducation-of-dylann-roof.
30. Ibid.
31. J. Anderson and L. Rainie, October 19, 2017, "The Future of Truth and Misinformation Online," Pew Research Center, http://www.pewinternet.org/2017/10/19/the-future-of-truth-and-misinformation-online/.
32. N. Newman and R. Fletcher, 2017, "Bias, Bullshit and Lies: Audience Perspectives on Low Trust in the Media, Digital News Project 2017," Reuters Institute for the Study of Journalism and University of Oxford, https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2017-11/Nic%20Newman%20and%20Richard%20Fletcher%20-%20Bias%2C%20Bullshit%20and%20Lies%20-%20Report.pdf.
33. Ibid.
34. G.E. Moore, April 19, 1965, *Electronics*, Vol. 38, No. 8.
35. There are arguments that the scaling predicted by Moore's Law may be ending in the next decade, but the industry has already begun the research and development into alternate architectures and technology to continue scaling without necessarily continuing to decrease the dimensions of the actual semiconductor.
36. E. Dwoskin, C. Timberg, and A. Entous, October 2, 2017, "Russians took a page from corporate America by using Facebook tool to ID and influence voters," *The Washington Post*, https://www.washingtonpost.com/business/economy/russians-took-a-page-from-corporate-america-by-using-facebook-tool-to-id-and-influence-voters/2017/10/02/681e40d8-a7c5-11e7-850e-2bdd1236be5d_story.html.
37. "Why We're Here," Palantir, https://www.palantir.com/about/.
38. P. Waldman, L.Chapman, and R. Robertson, April 19, 2018, "Palantir Knows Everything About You," *Bloomberg*, https://www.bloomberg.com/features/2018-palantir-peter-thiel/.
39. R. Chesney and D. Citron, 2019, "Deepfakes and the New Disinformation War: The Coming Age in Post-Truth Geopolitics," *Foreign Affairs*, https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war.
40. Summarized from the 2018 National Defense Strategy Summary, 2-3.
41. Summarized from the 2018 National Defense Strategy Summary, 5.
44. 10 U.S.C. §§ 101-18525.
43. 50 U.S.C. §§ 1-2420.
44. A.E. Wall, 2011, "Demystifying the Title 10-Title 50 Debate," *Harvard National Security Journal,* Vol. 3, https://harvardnsj.org/wp-content/uploads/sites/13/2012/01/Vol-3-Wall.pdf.
45. Ibid.
46. R. Chesney, April 12, 2018, "Title 10 and Title 50 Issues When Computer Network Operations Impact Third Countries," *Lawfare*, https://www.lawfareblog.com/title-10-and-title-50-issues-when-computer-network-operations-impact-third-countries.
47. A.E. Wall, 2011, "Demystifying the Title 10-Title 50 Debate," *Harvard National Security Journal*, Vol. 3, https://harvardnsj.org/wp-content/uploads/sites/13/2012/01/Vol-3-Wall.pdf.
48. Ibid.
49. Ibid.

NOTES

50. C. Bing, April 11, 2018, "Command and control: A fight for the future of government hacking," *cyberscoop,* https://www.cyberscoop.com/us-cyber-command-nsa-government-hacking-operations-fight/.
51. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. 115-232 (2018).
52. 10 U.S.C. § 394(b).
53. Ibid.
54. 10 U.S.C. § 394(c).
55. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. 115-232 (2018).
56. Ibid.
57. C.T. Lopez, May 14, 2019, "Persistent Engagement, Partnerships, Top Cybercom's Priorities," Department of Defense, https://www.defense.gov/Newsroom/News/Article/Article/1847823/persistent-engagement-partnerships-top-cybercoms-priorities/.
58. P.M. Nakasone, February 14, 2019, Statement before the Senate Committee on Armed Services.
59. E. Nakashima, February 27, 2019, "U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms," *The Washington Post*, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html?noredirect=on.
60. A. Burt and J.C. Trainor, January 2, 2020, "Our Government's Approach to Cybersecurity Is a Costly Mess. Here's What Would Fix the Problem," Time, https://time.com/5757811/cybersecurity-attacks-agency/.
61. S.C. O'Connell, January 29, 2020, "We don't need a separate cybersecurity agency," Politico, https://www.politico.com/news/agenda/2020/01/29/dont-need-separate-cybersecurity-agency-106631.
62. C. Mewett, January 21, 2014, "Understanding War's Enduring Nature Alongside Its Changing Character," War on the Rocks, https://warontherocks.com/2014/01/understanding-wars-enduring-nature-alongside-its-changing-character/.
63. F.G. Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," *Prism 7,* No 4, https://cco.ndu.edu/News/Article/1680696/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges/.
64. Adapted from reference 61.
65. P.M. Lefkowitz, June 25, 2019, "Why America Needs a Thoughtful Federal Privacy Law," *The New York Times*, https://www.nytimes.com/2019/06/25/opinion/congress-privacy-law.html?searchResultPosition=2.
66. National Defense Authorization Act (NDAA) for Fiscal Year 2017, Pub. L. 114-328 § 1287(a)(2).
67. P.M. Nakasone, February 14, 2019, Statement before the Senate Committee on Armed Services.
68. Department of Defense, May 17, 2010, *Irregular Warfare: Countering Irregular Threats Joint Operating Concept Version 2.0*, http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_iw_v2.pdf?ver=2017-12-28-162021-510.
69. Ibid.
70. How the Department of Defense will need to respond was taken from the USCYBERCOM 2018 *Cyberspace Strategy Symposium Proceedings*, p. 2.
71. Davis J. Hirshfeld Davis and M. Mazzetti, July 24, 2019, "Highlights of Robert Mueller's Testimony to Congress," *The New York Times*, https://www.nytimes.com/2019/07/24/us/politics/mueller-testimony.html?action=click&module=RelatedLinks&pgtype=Article.