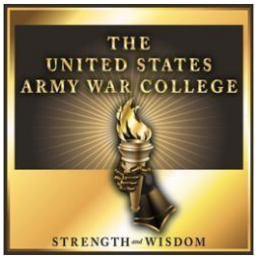
Strategy Research Project

Necessary Influence: Military Messaging to Counter the Virtual Caliphate

by

Lieutenant Colonel Jeremy S. Mushtare
United States Army

Under the Direction of:
Dr. Frank Jones



United States Army War College
Class of 2018

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
01-04-2018	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Necessary Influence: Military Messaging to Counter the Virtual Caliphate

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel Jeremy S. Mushtare
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Dr. Frank Jones

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.
I understand this document will be included in a research database and available to the public. Author: ☒

13. SUPPLEMENTARY NOTES
Word Count: 6258

14. ABSTRACT

The Islamic State of Iraq and Syria (ISIS) is on the verge of having its physical "caliphate" in Iraq and Syria destroyed. However, ISIS's online activities will likely allow it to persist as a dangerous threat—a virtual caliphate. This paper analyzes U.S. government technical and psychological activities in cyberspace to target ISIS extremists and reduce online radicalization that provides recruits, supporters, and inspires homegrown violent extremists. The U.S. tends to focus on the technical activities, while its psychological activities are largely split between State Department public diplomacy and Department of Defense military information support operations (MISO). Current activities are misaligned between those two departments are misaligned. Also, the Defense Department is overly restrictive in its adherence to the Smith-Mundt Act, lacks organic capabilities to conduct non-attributed messaging, and is overly reliant on contractors for current capabilities. This paper ends by positing prescriptive actions for better synergy and effectiveness against the virtual caliphate.

15. SUBJECT TERMS
Virtual Caliphate, ISIS, ISIL, Psychological Operations, PSYOP, Military Information Support Operations, MISO

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(w/ area code)*
UU	UU	UU	UU	36	

Necessary Influence: Military Messaging to Counter the Virtual Caliphate

(6258 words)

Abstract

The Islamic State of Iraq and Syria (ISIS) is on the verge of having its physical "caliphate" in Iraq and Syria destroyed. However, ISIS's online activities will likely allow it to persist as a dangerous threat—a virtual caliphate. This paper analyzes U.S. government technical and psychological activities in cyberspace to target ISIS extremists and reduce online radicalization that provides recruits, supporters, and inspires homegrown violent extremists. The U.S. tends to focus on the technical activities, while its psychological activities are largely split between State Department public diplomacy and Department of Defense military information support operations (MISO). Current activities are misaligned between those two departments are misaligned. Also, the Defense Department is overly restrictive in its adherence to the Smith-Mundt Act, lacks organic capabilities to conduct non-attributed messaging, and is overly reliant on contractors for current capabilities. This paper ends by positing prescriptive actions for better synergy and effectiveness against the virtual caliphate.

Necessary Influence: Military Messaging to Counter the Virtual Caliphate

> ISIL's virtual caliphate has progressed beyond strictly propaganda or recruitment efforts. It is about more than the proliferation of ideas; it is about the proliferation of action and of violence.
>
> —General Joseph L. Votel, et al[1]

The Islamic State of Iraq and Syria (ISIS) is on the verge of having its physical "caliphate" in Iraq and Syria destroyed.[2] The prevailing thought among senior national security professionals is that ISIS's extensive foothold in cyberspace, enabled by its organizational resilience and propaganda appeal, will allow it to persist as a dangerous threat—a *virtual caliphate*. That threat is generated through the radicalization process, stages where individuals consume propaganda and participate in online interactions with extremists. These interactions produce recruits, online supporters who amplify the propaganda fight, and homegrown violent extremists who ISIS inspires.

To combat these threats, the U.S. government has several ongoing activities, using both technical and psychological means, but is heavily reliant on the technical side. However, the virtual caliphate is not susceptible to targeting solely through technical means. There are two primary U.S. government mechanisms for addressing the psychological component. The first is State Department public diplomacy and the second is Department of Defense military information support operations. The Global Engagement Center was recently codified in law by Congress in the fiscal year 2017 National Defense Authorization Act, but under the control of the Department of State, to conduct counterterrorism messaging. In doing so, Congress has essentially "militarized" public diplomacy extending the State Department's original Title 22 statutory responsibilities and its existing capabilities. Meanwhile, the Department of Defense has

the requisite authorities to target the virtual caliphate, but self-imposed policies, misalignment of capabilities, and overreliance on contractors hinder these efforts.

To examine these concepts, this paper will describe the rise of ISIS and the emergence of the virtual caliphate. It will then explain the dangers of radicalization, the radicalization process, and its enablers. From that perspective, the paper recounts current U.S. government activities to contest the cyberspace domain against ISIS through both technical and psychological activities. Within the Department of Defense specifically, it will examine current activities, against the backdrop of extant authorities and capabilities, in order to determine alignment of U.S. efforts. Finally, the paper makes recommendations based on what have been determined to be the misalignment of U.S. government activities against the virtual caliphate.

Emergence of ISIS

The United States withdrew the last its military forces from Iraq at the end of 2011, through what was dubbed the “responsible drawdown of forces” (RDOF). The RDOF inadvertently led to a power vacuum in Iraq as security and governance deteriorated. During that same timeframe, political unrest in Syria, tied to the “Arab Spring” movement, devolved into a bloody Syrian civil war that continues to this day. Exploiting first on the chaos in Syria to build strength, and then on the power vacuum in Iraq, the group known as the Islamic State of Iraq (formerly al-Qaeda in Iraq) amassed a powerful following and acquired significant resources.[3] In April 2013, to capitalize on its expanding influence, the organization changed its title to the Islamic State of Iraq and Syria (ISIS).[4] In 2014, ISIS conducted a full-fledged invasion of northern and western Iraq, including seizure of major cities, resulting in stunning battlefield victories.[5] The Iraqi security forces were badly defeated with the Government Accountability Office (GAO)

estimating combined Iraqi casualties and desertions at approximately 74,000—almost half of Iraq's standing army strength.[6] Thus, ISIS suddenly found itself on the international stage.

Through the almost serendipitous confluence of battlefield successes, dominant control of populations and territory, and a new international audience, ISIS was presented with advantages that it immediately exploited. Most notably, ISIS declared itself as a caliphate, rebranded under the new title of the "Islamic State," in June 2014.[7] The caliphate represented something new, a state-like organization controlling populations, significant resources, an army, and land, while welding together "historical, philosophical and theological" concepts into an ideology more comprehensive than those of its predecessors.[8] The "caliphate brand" soon developed into an all-out, global franchise, opening branches in other countries (Afghanistan, Pakistan, Yemen, North Africa, and the Philippines, among others), while other terrorist groups, such as Boko Haram in Nigeria, voluntarily aligned with ISIS.[9]

As part of ISIS's rise to power, it brilliantly incorporated emergent internet and communications technologies, particularly social media platforms and mobile devices, into their propaganda campaign. Increased access to the internet in the early 2000s was rapidly followed by extensive development and proliferation of better, faster, and more internet-capable mobile devices. A rapid boom in the development of social media sites and applications, under what was termed Web 2.0, changed the paradigm of individuals' internet experiences and activities.[10] Gone were the days where internet users could only consume posted content passively. Now they could dynamically participate, en masse, through interactive "*social-networking and user-generated*

content" (emphasis in the original).[11] Naturally, violent extremist organizations, particularly al-Qaeda, were quick to employ these new technologies and inexpensive platforms both to increase messaging speed and extend reach, thereby gaining access to wider, global audiences.[12] New internet capabilities allowed terrorists to operate "chat rooms, dedicated servers and websites, and social networking tools." Such capabilities now routinely serve as an integral component of ISIS's terrorist operations.[13] Although ISIS has an advanced propaganda arm including audio, video, and print products, it is the group's extensive, networked online presence that has led it to become identified as a separate and distinct threat—the virtual caliphate.[14]

The Virtual Caliphate

Among terrorist groups, ISIS was unique because its military victories and seizure of territory allowed it to assume the trappings of "sovereignty" and "statehood," thereby creating an aura of legitimacy that magnified its appeal through skilled propaganda campaign. Few took notice until 2014, when ISIS consolidated its gains and occupied a position that posed an existential threat to Iraq and the broader Middle East. That summer, the Barack Obama administration reintroduced U.S. military forces into Iraq to assist Iraqi security forces in retaking territory and stabilizing the country.[15] Less than three years later, General Joseph Votel, commander of U.S. Central Command (USCENTCOM), discussed the growing dangers of the virtual caliphate: "Ready access to the Internet, social media, and other messaging platforms has enabled a new generation of extremists to spread their radical Islamist views, incite widespread violence, and recruit new followers to their cause."[16] There is now widespread belief that the threat posed by the virtual caliphate can outlive the eventual demise of ISIS in Iraq and Syria. Furthermore, the GAO states, in concert with

prevailing opinion, when the physical caliphate recedes, it is more likely that ISIS will use online propaganda to further incite attacks around the world.[17] Indeed, the virtual caliphate's primary propaganda objectives are to "intimidate the global population, recruit followers, promote its violent extremist ideology, and encourage terrorist attacks."[18] However, there is debate about the potential viability of the virtual caliphate to survive and pose a continued threat. Some critics offer the opinion that once ISIS loses all of its physical territory, and therefore its "sovereignty" as a state, its ideology will be undermined and its propaganda will no longer have appeal.[19] In concert with that thought, it is true that battlefield defeats and significant loss of territory have degraded ISIS's propaganda efforts, including having to "walk back its utopian promise."[20] Nevertheless, it is probable that, given its widespread network of online affiliates and supporters, the virtual caliphate will persist as a threat.

Radicalization

General Votel highlighted the danger of the virtual caliphate as imbued in its "proliferation of action and of violence."[21] To this end, radicalization is the chief online threat of the virtual caliphate because it is the catalyzing process that produces extremists committed to conducting violent acts and generates a host of online supporters. Radicalized individuals may become active recruits, but there are also individuals, including many homegrown violent extremists (HVEs), who are "inspired" by ISIS to carry out attacks, though they are not officially members of the group. Furthermore, it has been recognized that, "Propaganda is an accelerant on the process of radicalization."[22] While there is a correlation between those individuals who seek out propaganda and radicalization, the messaging itself is merely a contributor to the individual's radicalization process, not the sole cause.[23] What we know is that the

influence ISIS wields in social media is dangerous and unquestionably stimulates radicalization and fear. Although the exact degree to which propaganda contributes is ultimately unknowable, efforts must be made to contest virtual spaces against those threats.

ISIS's propaganda machine has demonstrated prowess in its recruiting efforts drawing an estimated 40,000 foreign fighters into its active fight in the Middle East.[24] While the majority of these individuals were from within the Middle East and North Africa, there were a notable amount coming from Western nations as well, including the United Kingdom, France, Germany, and up to approximately 100 from the United States.[25] Though the most radical of the extremists flock to the ISIS banner to fight or commit acts of violence against soft targets, many other radicalized individuals choose instead to provide support from relative safety, joining the virtual caliphate to promulgate ISIS propaganda materials.[26] Through its social media activities in particular, ISIS has created a followership of thousands.[27]

One reason radicalization has received much attention over the last few years is because of the violent acts committed by HVEs within the United States and the role that access to online extremist propaganda may have played in facilitating those crimes. In addition to the potential that a surviving virtual caliphate will continue to radicalize and recruit followers who try to reestablish an "Islamic State," there is also the likelihood that the number of HVEs will continue to grow within the United States. Terrorism expert Peter Neumann notes that there is wide agreement within U.S. government agencies that terrorist use of the internet is "the single most significant innovation to have affected homegrown radicalization since the 11 September attacks in 2001."[28] In 2015, FBI

Director James Comey stated that there were more than “900 active investigations into homegrown violent extremism across all 50 states.”[29] Law enforcement agencies have arrested numerous terrorist group affiliated persons over the last few years and subsequent investigations have shown some degree of relationship between propaganda consumption and radicalization. Moreover, virtual caliphate propaganda has been noted as a potential contributor to the radicalization of the HVEs that committed the mass shooting and attempted bombing in San Bernardino, California, in 2015.[30] Since 2014, U.S. authorities have identified twelve ISIS-inspired attacks within United States territory that resulted in a total of eighty-two deaths.[31] Regardless of the differing paths individuals take to become recruits, inspired extremists, or online supporters, there are similarities in the online radicalization process.

Online Radicalization Process

Online radicalization, focusing on ISIS in particular, has been described as entailing three phases.[32] The first phase is pre-radicalization and self-identification—where individuals initially seek out extremist materials out of curiosity or accidental exposure.[33] The second phase, indoctrination, is when, after repeated exposure to materials, individuals have bought into the fundamental precepts of the group and stand ready to take action on behalf of the group.[34] In the third phase, “jihadization,” individuals are recruited and interact with ISIS members with the goal of identifying and executing terrorist acts.[35] ISIS’s recruiting strategy has been known to differ from al Qaeda’s because individuals who are recruited are somewhat radicalized already, rather than recruiting first and then indoctrinating members.[36] The process toward active recruitment, what one may view as part of the jihadization phase, has been described as entailing four steps for ISIS: (1) initiating first contact; (2) creating a micro-community

of believers; (3) shifting to private communications; and (4) identifying an ISIS approved target and encouragement to action it.[37] While ISIS uses more popular online sites to cast a wide net and identify potential recruits, its true recruiting efforts are actually handled through more restrictive communications.[38] During the "shift to private communications" step, ISIS operators typically draw the recruits into encrypted platforms (such as Telegram, WhatsApp, Kik, and Surespot) to plan operations.[39] Among those individuals who are radicalized, there is no definitive way to know when one may make the leap from online support for ISIS to willingly committing violence on its behalf.[40]

Radicalization Enablers

There are two main enablers that contribute to ISIS's ability to radicalize individuals online: its persistent, resilient presence in social media and its appeal through an overarching narrative with supporting themes. First, to achieve multiple objectives, ISIS adeptly messages through popular, accessible internet-based communications platforms, including social media that provide speed and international reach. However, despite attempts to disrupt ISIS online propaganda, the group has demonstrated resilience through their flexibility, shifting operations to alternative communications sites and platforms while continuing to saturate virtual spaces with content. Second, ISIS's narrative and supporting themes are expertly developed to target, and in some cases, appeal to multiple audiences to achieve different objectives.

Resilience of the Virtual Caliphate

ISIS is resilient online for two main reasons. The first is its ability to displace to other sites and still operate, and the second, its extensive follower base that conducts decentralized propaganda dissemination. Wisely, ISIS has taken advantage of the

openness of several popular social media sites such as YouTube, Diaspora, Twitter, and Facebook.[41] Social networking sites were initially slow to respond to extremist posts, but eventually some did begin to take action. However, ISIS remains resilient despite being challenged by social media gatekeepers who delete content or employ algorithms that automatically redirect users to alternative sites. The trend has been for ISIS to maintain operations by shifting to other social media platforms that facilitate more anonymity and protection—such as Telegram.[42] The group has also entered into activities on the dark web, that is, "a portion of the Internet requiring anonymous web browsing, not accessible through regular browsers like Google Chrome, Mozilla, or Internet Explorer."[43] Furthermore, ISIS has demonstrated the use of advanced software such as the employment of "Twitter bots" that can automatically mass-spam users by posting and re-posting content.[44]

Aside from the official propagandists, active online supporters also present an unofficial dissemination arm. These individuals and cells produce user-generated ISIS propaganda themselves and also provide a decentralized capability for translating ISIS products into native languages.[45] This methodology has been described as the "outsourcing" of ISIS's propaganda efforts to "fans" of the organization.[46] These individuals, the so-called "keyboard jihadists," enable ISIS to create market saturation of its propaganda and compound its efforts and effects.[47]

Virtual Caliphate Narrative and Themes

To address, and many cases, appeal to, varying audiences, ISIS uses an overarching narrative, comprising several themes. First and foremost, ISIS attempts to market its legitimacy and status as a "functioning, expanding caliphate" by blending information about actual circumstances with hyperbole reflecting its utopian vision.[48]

ISIS also displays a diversity in product development and dissemination, including "daily radio and text bulletins, photographic essays and videos—all meticulously branded—depicting executions, excerpts from daily life, religious training and military operations."[49]

Terrorism researcher Charlie Winter describes six central themes to ISIS products (1) brutality; (2) utopianism; (3) victimhood; (4) war; (5) belonging; and (6) mercy.[50] The two most important aspects are brutality and utopianism. First, the theme of brutality is likely what comes to mind most to those who envision terrorist propaganda. Gruesome visions of executions, beheadings, and suicide bomber attacks are frightening imagery designed to maximize ISIS's shock value. Most people logically would expect brutality to be ISIS's dominant theme, but counterintuitively others posit that it is actually utopianism because it serves as a better recruiting tool.[51] Former Under Secretary of State for Public Diplomacy and Public Affairs Richard Stengel noted that about eighty percent of ISIS propaganda is characterized by utopian themes.[52] The most important aspect of that utopian messaging is the legitimacy ISIS weaves in by capitalizing on its state-like caliphate structure and advanced media operations.[53] Some analysts have confirmed that more than fifty percent of ISIS propaganda releases focus on issues broader than the war, addressing such issues as governance, theology, and beneficial day-to-day life under ISIS rule.[54]

Aside from the online threat of ISIS itself, there is another important aspect for why U.S. forces must examine and counter virtual caliphate operations—ISIS is not the only violent extremist organization utilizing the cyberspace domain. Other terrorist groups, including al-Qaeda and Hamas, continue to engage audiences online for similar

objectives as ISIS.[55] Furthermore, these and other terrorist groups are following ISIS's trail-blazing example, evolving propaganda products and techniques in order to improve messaging effectiveness.[56] Therefore, there is importance in not only stemming the tide of ISIS radicalization, but in applying successful techniques to counter other online violent extremists as well. To counter these threats, the U.S. government currently has several ongoing activities.

U.S. Government Activities to Counter the Virtual Caliphate:

At present, U.S. government efforts targeting ISIS propaganda can be described as involving both technical and psychological activities. The technical activities generally consist of efforts that disrupt terrorists' abilities to access sites or post content, or divert users away from accessing the propaganda. The psychological activities are often described as employing counter-narratives or counter-messaging.[57] Charlie Winter describes ISIS propaganda as intricate and requiring an equally intricate campaign to compete with all aspects of it.[58] He also contrasts ISIS propaganda with opposing efforts of its adversaries stating, "The quantity, quality and variation of Islamic State propaganda in just one month far outweighs the quantity, quality and variation of any attempts, state or non-state, to challenge the group."[59] However, the preponderance of the U.S. government's efforts does not rise to that level of complexity, relying more on technical activities, without the commensurate emphasis on the psychological component.

Technical Activities

The two major types of technical activities conducted to target ISIS propaganda are disruption and diversion. Disruption efforts are ways to block terrorists from posting content through methods such as account suspensions, finding and deleting posted

content, taking down websites, and corrupting the data of the posted content.[60] Diversion efforts include activities that redirect users away from extremist materials, often toward materials with anti-extremist themes.[61]

Through U.S. government engagement, social networking sites and search engines have been encouraged to self-censor content to prevent proliferation and accessibility of ISIS materials. Some of the major social networking companies, such as Facebook, YouTube, Twitter, and Google, have complied and have experienced some degrees of success.[62] These companies typically employ redirection (diversion) and account suspensions (disruption). For example, YouTube utilizes redirection where attempts to search for certain extremist propaganda will "lead users to videos that rebut violent narratives."[63] Other social media sites suspend accounts when individuals violate the user agreement for terms of service by posting violent content or advocating for terrorism.[64] ISIS Twitter activity was driven down significantly, due largely to account suspensions, affecting some 235,000 ISIS and extremist affiliated accounts by 2016.[65] Unfortunately, while Twitter may block certain handles (usernames), individuals who have been suspended are able to reenter the discussion with only a slight modification to the handle. Many of the propagandists are resilient, changing their usernames and resurfacing time and again with little disruption to their activities.[66] In addition, "Twitter neither suspends nor blocks" hashtag names, which easily can direct individuals to extremist content.[67]

There are also other technical efforts the U.S. government is undertaking, though largely not discussed in open-source media. These tools involve closely guarded offensive cyberspace operations (OCO).[68] In 2016, U.S. Strategic Command tasked

U.S. Cyber Command to establish Joint Task Force (JTF) Ares, collocated at Fort Meade with U.S. Cyber Command (USCYBERCOM) and the National Security Agency.[69] Its mission is "to deny ISIL's use of the cyberspace domain through a multipronged approach."[70] Though the specifics of that approach are not publicly available, it has been described as "destroying or disrupting computer networks used by the militant group to recruit fighters and communicate inside the organization [ISIS]…."[71] Open source reporting describes that as part of one operation, JTF Ares "obtained the passwords to a number of Islamic State administrator accounts and then used them to access the accounts, change the passwords and delete content such as battlefield video. It also shut the group's propaganda specialists out of their accounts...."[72] USCYBERCOM and the Department of Defense touted the success of these operations, but other intelligence analysists have stated that even these effects were only temporary because ISIS was still able to recover from these setbacks by re-posting content or moving its hosting services to alternate servers.[73] While these technical efforts are effective only partially, they do make it more restrictive for the virtual caliphate to engage audiences through cyberspace activities.[74] However, in the face of such technical efforts, ISIS is resilient in maintaining access and operations. Technical activities are not a panacea against online extremism and are incomplete without a complementary psychological approach.

Psychological Activities

Psychological activities to challenge ISIS propaganda online largely consist of counter-messaging, often with the purpose of undermining or discrediting the propaganda or the propagandist. The United States government conducts such online messaging predominantly through the Department of State and the Department of

Defense.[75] Within the activities of these two departments there are four major areas of concern. First, Department of State public diplomacy is ill-suited to conduct anti-ISIS messaging because of its Title 22 mandate and legal limits that only authorize dissemination of products attributable to the U.S. government. Second, Department of State efforts that build partner capacity (BPC) with other nations to conduct online messaging against ISIS are misaligned because public diplomacy personnel lack requisite skills and knowledge on these activities to conduct them. Third, the Department of Defense has requisite authorities to counter the virtual caliphate, however, its internal policy observing the Smith-Mundt Act, a law that prohibits the Department of State from disseminating materials intended for foreign audiences within the United States, is an overly stringent Cold War relic. Fourth, Department of Defense capabilities to conduct non-attributed engagements online are limited in quantity, organizationally misaligned, and too dependent upon the use of contracting.

Department of State Activities

The Department of State conducts public diplomacy through its embassies around the world to influence foreign audiences.[76] Public diplomacy products are openly attributed to the U.S. government, without a legal basis to conduct non-attributed activities.[77] Under Title 22 U.S. Code, the mandate for public diplomacy is to target

> …developed and developing countries and select and general audiences, using appropriate media *to properly explain the foreign policy of the United States* [emphasis added] to the governments and populations of such countries, with the objectives of increasing support for United States policies and providing news and information. The Secretary [of State] shall, through the most effective mechanisms, counter misinformation and propaganda concerning the United States.[78]

Therefore, it is a responsibility for public diplomacy to “counter misinformation and propaganda concerning the United States” only insofar as it relates to explaining U.S. foreign policy abroad.

Despite recent debate as to its applicability, the existing post-9/11 Authorization for Use of Military Force (AUMF) has continued to serve as the legal basis for conducting operations against al-Qaeda and its affiliates.[79] Consequently, the AUMF places ISIS in the category of national security threats and therefore, under the general purview of the Department of Defense. However, in 2016, President Barack Obama signed an executive order establishing the Global Engagement Center (GEC) under the Department of State, to “lead the coordination, integration, and synchronization of Government-wide communications activities directed at foreign audiences abroad in order to counter the messaging and diminish the influence of international terrorist organizations, including the Islamic State of Iraq and the Levant (ISIL), al Qa'ida, and other violent extremists abroad….”[80] Yet, in actuality, the GEC’s activities entail more than just synchronization as it employs an operational arm known as the Digital Outreach Team (DOT).[81] In doing so, the GEC’s activities are not consistent with previous law (Title 22) or the traditional role of the Department of Defense relative to the AUMF. It is a stretch in statutory interpretation to describe activities aimed at countering ISIS ideology and propaganda as equated with conveying U.S. foreign policy in accordance with the statute. In short, Global Engagement Center activities, under the auspices of the Department of State, which target AUMF applicable extremists have essentially militarized public diplomacy.

In a shift, with growing concerns over the extent of Russia's influence campaign during the 2016 U.S. election season, Congress formally established the Global Engagement Center in the Fiscal Year 2017 National Defense Authorization Act (NDAA).[82] The GEC's purpose was expanded also to include the task to "counter foreign state and non-state propaganda and disinformation efforts."[83] This new focus is in concert with traditional public diplomacy efforts because it focuses on explaining U.S. foreign policy and countering misinformation that undermines those policies. However, the GEC still maintains a significant focus on terrorism and ISIS in particular.[84]

The GEC is also challenged in how it conducts operations to target extremists – through activities attributed to the U.S. government.[85] House Foreign Affairs Committee hearings described the ineffectiveness of GEC counter-messaging as a direct result of the reliance on U.S. attribution.[86] Ambassador Alberto Fernandez, who once headed the GEC's forerunner, stated "Everything we did had the State Department label on it, and that was a liability."[87] Fernandez's claim have led many experts to wonder openly "whether the U.S. government should be involved in overt messaging at all."[88]

Another key aspect of the State Department's counterterrorism messaging has been through building partner capacity efforts.[89] In 2015, as a broader initiative to counter ISIS and extremist ideology within the Middle East, the Department of State and the United Arab Emirates established the Sawab Center, the "first-ever multinational online messaging and engagement program."[90] Based out of Abu Dhabi, the Sawab Center's methodology is to use social media to "amplify those many moderate voices that too often get drowned out by the noise of the extremists."[91] Sawab also has been criticized for disseminating "violent — videos, made by Muslims to scare Muslims away

from extremist content and to promote anti-terrorist sentiment online."[92] While security assistance programs like this are within the purview of the State Department, the personnel who manage them lack training and expertise in areas specific to targeting audience vulnerabilities. This specialization is not within the realm of public diplomacy. Nevertheless, the State Department's favorable view of the Sawab Center led it to plan for similar centers in other locations (Jordan, Nigeria, and Malaysia).[93]

The Department of State's U.S. attributed public diplomacy activities serve an important function as an arm of U.S. foreign policy, particularly as employed by U.S. embassies around the world. However, programs that target terrorists and supporters, those threats that are targetable under the authorities of the AUMF, go beyond State Department public diplomacy roles, training, or capabilities. While the Department of Defense is better suited to conduct operations against the virtual caliphate, there are challenges with those efforts as well.

Department of Defense Activities

The Department of Defense is actively conducting operations to counter the virtual caliphate through technical means, as previously discussed, and psychological activities. Psychological operations (PSYOP) forces perform these activities, known as military information support operations (MISO), to influence foreign target audiences.[94] Unlike public diplomacy, MISO are not explicitly defined in U.S. law and can only be conducted under the authority of an approved program.[95] Furthermore, whereas public diplomacy is generally focused on themes that promote shared values, MISO specifically target vulnerabilities in select audiences. While there are generally sufficient authorities to conduct MISO against the virtual caliphate, there are restraints imposed

by current Department of Defense policy, along with challenges from misaligned or deficient capabilities and overreliance on contractor personnel.

Unlike the Department of State, under specific conditions, the Department of Defense can conduct disseminate products that are non-attributed, meaning "there is no intention to ever acknowledge the source of the message or action."[96] Non-attributed products are only authorized if the operations constitute an exception to the covert action statute (Title 50 United States Code §3093).[97] One such exception is if the activity is deemed a traditional military activity (TMA).[98] In order to be defined as a TMA, the activity must be conducted "by military personnel under the direction and control of a United States military commander… preceding and related to hostilities which are either anticipated…[or] ongoing, and, where the fact of the U.S. role in the overall operation is apparent or to be acknowledged publicly."[99] Therefore, when meeting the criteria of TMA, non-attributed MISO products may be permissible, for instance, in areas such as Iraq or Afghanistan that are clearly related to ongoing, publicly acknowledged activities under command and control of a military commander.

While PSYOP forces employ military information support teams (MISTs) to support U.S. embassy's in several countries around the world, the majority of online operations to target extremism have been conducted at the combatant command level and not at the local or host nation level. In 2007, the Department of Defense established two overarching policies for military influence operations on the internet and in social media.[100] The first, known as the Trans-Regional Web Initiative (TRWI) referred to static posts on websites owned and managed by the combatant commands.[101] The second,

the Interactive Internet Activities (IIA) policy, allowed for interactive messaging through a variety means, sites, or applications.[102]

Under TRWI, U.S. Special Operations Command (USSOCOM) employed contractors to create and manage up to ten websites for the geographic combatant commanders.[103] The purpose of TRWI was to provide the combatant commanders with an online news-based platform to message and influence foreign target audiences in their respective languages. However, TRWI came under considerable congressional and public scrutiny after the Government Accountability Office raised questions about costs (up to $22 million per year), effectiveness, and lack of coordination with Department of State and relevant U.S. embassies.[104] It was also noted that TRWI was potentially too involved in the realm of public diplomacy and "duplicated capabilities which already existed in Voice of America and Radio Free Europe/Radio Liberty."[105] This scrutiny, along with tightening budgets after sequestration in 2013, ultimately led Congress to defund TRWI in the fiscal year 2014 NDAA.[106]

Under the IIA policy, the Department of Defense authorized Combatant Commands to expand their MISO activities online through interactive methods, including social media, to communicate with select audiences.[107] United States Central Command had the greater need for these activities, where the primary threats were originally al-Qaeda and affiliates. To conduct messaging against these targets, USCENTCOM established a web operations (WebOps) cell to execute activities under its version of IIA, titled the Regional Web Interaction Program (RWIP).[108] The main objectives for RWIP are "to counter violent extremist ideology and enemy propaganda," and "to amplify messages of credible individuals over the internet."[109] Along with

messaging to contest social media spaces against extremists, the WebOps team supported technical activities by reporting terrorist usernames to have accounts suspended.[110] Open source materials from 2016 show that USCENTCOM believed its WebOps, along with other activities (both physical and virtual), were eroding ISIS's online efforts.[111] Differentiated from the issues of the now defunct TRWI program, General James Mattis, then Commander of USCENTCOM, noted in his 2012 posture statement that these operations "do not address the American public nor are they a Public Diplomacy tool to increase popular support for any U.S. policy."[112] Finally, as ISIS is considered targetable due to the extant AUMF, non-attributable targeting of virtual caliphate propagandists and propaganda may be authorized. However, doing so online is complicated by Department of Defense adherence to the Smith-Mundt Act.

As mentioned earlier, one of the main challenges to conducting contemporary influence operations online is the U.S. Information and Educational Act of 1948 (known as the Smith-Mundt Act). Smith-Mundt prohibited the Department of State from disseminating propaganda-type materials domestically, where U.S. citizens could be influenced by it.[113] While this law technically does not apply to the military, the Department of Defense has traditionally observed it through a self-imposed policy restriction. This practice has been complicated by technology, characterized by ubiquity of internet access, proliferation of communications, and terrorist freedom of movement through cyberspace. The difficulty is that individual users create online personas and therefore Americans may be on sites that extremists frequent. It can be very difficult to identify if the individuals are American or not. These sites, typically in languages such as Arabic or Urdu, may even include Americans who are the keyboard jihadists

disseminating propaganda. Therefore, compliance with Smith-Mundt slows or prevents the ability of military forces to engage. However, Smith-Mundt is a Cold War relic created during a time when government messaging abroad was not likely to be obtained by U.S. audiences. The security environment has changed with the expansion of global communication platforms and increased access to information.

Another challenge is that Department of Defense online MISO activities are characterized by misalignment of current capabilities, lack of organic messaging capabilities, and overreliance on contractor personnel. Military information support operations are an element of special operations, but, USCENTCOM's RWIP activities are administered from within the combatant command headquarters staff and are not under the authority or direction of a special operations commander. While the program is run by MISO staff officers, its WebOps team consists of about one-hundred twenty contracted personnel.[114] As evidenced by the history of TRWI and its information operations programs in the wake of the 2013 sequester, congressional and public scrutiny remains high on overuse of government contracts.[115] RWIP itself has been subject to some recent public interest due potential issues with this multimillion-dollar contract.[116] However, the reason why USCENTCOM must rely on a contract vehicle to provide these capabilities is because the special operations community, in conjunction with the Army, have not developed or fielded appropriate deployable or static RWIP-like systems. Not all combatant commands even have the contracted capability to conduct online MISO activities, therefore, presenting a capability gap. This should be of concern as competitors and adversaries are heavily investing both in cyberspace and online information warfare capabilities.

Issues and Recommendations

Overall, there is misalignment of U.S. government activities against the virtual caliphate. There are four recommendations that would create better synergy and effectiveness. First, the State Department's role in messaging against the virtual caliphate, particularly through the Global Engagement Center, is outside of its original mandate and public diplomacy role. However, the GEC has functional capability, increased funding, and a new purpose—to counter "foreign state and non-state propaganda and disinformation efforts."[117] These activities should be focused, as a subset of public diplomacy in accordance with Title 22, on Russian and other adversarial states' or non-state actor disinformation activities abroad where they misinterpret or mischaracterize U.S. foreign policies.

Second, the Sawab Center, and others like it, are a good concept for building partner capacity to counter extremist ideology online. However, these particular endeavors are more akin to the role of military information support operations and require a degree of training and expertise that public diplomacy personnel do not have, such as skills in targeting audience vulnerabilities and counterpropaganda operations. These efforts are consistent with special operations activities that build partner capacity to combat terrorism. General Votel noted that the credible voices with the legitimacy, influence, and ability to oppose the ISIS ideology come from within the region itself.[118] Therefore, Theater Special Operations Commands (TSOCs) should partner with relevant host nation militaries to establish national information warfare centers that combine technical and psychological activities to counter online radicalization. This should be explored under the authorities provided in Title 10 §127e. "Support of U.S. Special Operations to Foreign Forces to Combat Terrorism."[119] Increased United States

assistance to partner nations in combating the virtual caliphate is an important, viable option that “will yield far better results than trying to manage an information or counter-messaging campaign from Washington.”[120]

Third, the Department of Defense should reexamine its self-imposed adherence to the Smith-Mundt Act in an era so very different from the dynamics of the Cold War. In the modern world, pervaded by disinformation from state and non-state actors, there is minimal risk to an American who views U.S. military messages online designed to undermine ISIS extremism. Furthermore, if an American is an active supporter of the virtual caliphate, operating on sites that facilitate recruitment and radicalization for ISIS, exposure to messaging that dissuades that individual from further support is a desirable outcome. Therefore, the long-held stigma attached to messaging and counter-messaging should give way to current understanding of the operational environment and contemporary threats. Virtual spaces must be contested through technological and psychological activities, and the potential adverse effects on unintended audiences or HVEs online are ultimately low risk.

Fourth, USSOCOM and the Army should develop organic messaging platforms to conduct non-attributed interactive internet activities and abandon overreliance on contracts. Since MISO are defined by Title 10 as part of special operations, those capabilities logically should be assigned to the TSOCs. This will enable messaging capability, including non-attribution, to each geographic combatant command. Furthermore, by residing at the TSOCs, these capabilities would be at the interface between tactical and operational levels and under the appropriate direction of a special

operations commander, and not subordinate to a staff as in USCENTCOM's current model.

Conclusion

There is no panacea to counter online radicalization by ISIS or any other extremist organization. Violent extremist propaganda cannot be eliminated from the internet, but the space must be contested through a variety of means to undermine, discredit, and degrade virtual caliphate propaganda operations and break the online radicalization process. The virtual caliphate's operations have been sophisticated accounting for both psychological and technological aspects. The United States should be doing likewise. However, challenges remain to the methods and capabilities that the U.S. government is employing to contest the cyberspace domain. The Department of State has a role in explaining U.S. policies and countering propaganda designed to undermine those policies, but, when it comes to active, dangerous threats to the United States, military messaging remains a necessary influence.

Endnotes

[1]Joseph L. Votel et al, "#Virtual Caliphate: Defeating ISIL on the Physical Battlefield is Not Enough," January 12, 2017, linked from *the Center for a New American Security Home Page*, https://www.cnas.org/publications/reports/virtual-caliphate (accessed December 29, 2017).

[2] The term Islamic State of Iraq and Syria (ISIS) is used because it is incorporated into the most recent National Security Strategy. For purposes of this project, This term is synonymous with selected quotes and citations that use the terms Islamic State (IS), Islamic State of Iraq and the Levant (ISIL), Islamic State of Iraq and al-Sham, and *Daesh* (the transliterated Arabic acronym for ISIS). Donald J. Trump, *National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (accessed December 20, 2017).

[3] Joby Warrick, *Black Flags: The Rise of ISIS* (New York, NY: Anchor Books, 2016), 244.

[4] U.S. Government Accountability Office, *Countering ISIS and its Effects: Key Issues for Oversight*, GAO-17-687SP (Washington, DC: U.S. Government Accountability Office, July 2017), 3, https://www.gao.gov/assets/690/685908.pdf (accessed December 29, 2017).

[5] Ibid., 4.

[6] Ibid.

[7] Charlie Winter, *The Virtual "Caliphate": Understanding Islamic State's Propaganda Strategy* (London: The Quilliam Foundation, 2015), 6.

[8] Amarnath Amarasingam and J. M. Berger, "With the Destruction of the Caliphate, the Islamic State has Lost far more than Territory," *Washington Post Online*, October 31, 2017, https://www.washingtonpost.com/news/monkey-cage/wp/2017/10/31/the-caliphate-that-was/?utm_term=.7d47c2ffad52 (accessed January 1, 2018).

[9] U.S. Government Accountability Office, *Countering ISIS and its Effects*, 7.

[10] Peter R. Neumann, "Options and Strategies for Countering Online Radicalization in the United States," *Studies in Conflict & Terrorism* 36, no. 6 (May 2013): 434-435.

[11] Ibid.

[12] Ibid.

[13] Catherine A. Theohary and John Rollins, *Terrorist Use of the Internet: Information Operations in Cyberspace* (Washington, DC: U.S. Library of Congress, Congressional Research Service, March 8, 2011), 2, https://fas.org/sgp/crs/terror/R41674.pdf (accessed January 5, 2018).

[14] Anne Aly et al., "Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization," *Studies in Conflict & Terrorism* 40, no. 1 (April 2016): 3.

[15] Barack Obama, "Transcript: President Obama's June 19 Remarks on Iraq," *Washington Post Online*, June 19, 2014, https://www.washingtonpost.com/politics/transcript-obamas-june-19-statement-on-iraq/2014/06/19/91380028-f7cc-11e3-a3a5-42be35962a52_story.html?utm_term=.33dcfb734ee9 (accessed February 10, 2018).

[16] Joseph L. Votel, *The Posture of U.S. Central Command*, Posture Statement presented to the 115th Cong., 1st sess. (Washington, DC: U.S. Central Command, March 9, 2017), 4-5, http://www.centcom.mil/Portals/6/Documents/Votel_03-09-17.pdf (accessed December 27, 2017).

[17] U.S. Government Accountability Office, *Countering ISIS and its Effects*, 2-3.

[18] Ibid.

[19] Haroro J. Ingram and Craig Whiteside, "In Search of the Virtual Caliphate: Convenient Fallacy, Dangerous Distraction," *War on the Rocks*, September 27, 2017, https://warontherocks.com/2017/09/in-search-of-the-virtual-caliphate-convenient-fallacy-dangerous-distraction/ (accessed January 3, 2018).

[20] Colin Clarke and Charlie Winter, "The Islamic State may be Failing, but its Strategic Communications Legacy is Here to Stay," *War on the Rocks,* August 17, 2017,

https://warontherocks.com/2017/08/the-islamic-state-may-be-failing-but-its-strategic-communications-legacy-is-here-to-stay/ (accessed January 1, 2018).

[21] Votel et al., "#Virtual Caliphate."

[22] Jeremy Bash, *The Plan to Defeat ISIS: Key Decisions and Considerations*, Statement before the Senate Foreign Relations Committee, 115th Cong., 1st sess., February 27, 2017, 4, https://www.hsdl.org/?view&did=799867 (accessed February 15, 2018).

[23] Winter, *The Virtual "Caliphate*," 8.

[24] U.S. Government Accountability Office, *Countering ISIS and its Effects*, 7.

[25] Aly et al., "Terrorist Online Propaganda and Radicalization," 5.

[26] J. M. Berger, "Tailored Online Interventions: The Islamic State's Recruitment Strategy," *CTC Sentinel* 8, no. 10 (October 2015): 23, https://ctc.usma.edu/tailored-online-interventions-the-islamic-states-recruitment-strategy/ (accessed January 1, 2018).

[27] U.S. Government Accountability Office, *Countering ISIS and its Effects*, 32.

[28] Neumann, "Options and Strategies for Countering Online Radicalization," 432.

[29] Seamus Hughes, C*ountering the Virtual Caliphate*, Statement before the House Foreign Affairs Committee, 114th Cong. 2nd sess., June 23, 2016, 1, https://extremism.gwu.edu/sites/extremism.gwu.edu/files/downloads/Hughes%20HFAC%20Testimony.pdf (accessed December 29, 2017).

[30] U.S. Government Accountability Office, *Countering ISIS and its Effects*, 7.

[31] John Haltiwanger, "ISIS in America: How Many Times has the Islamic State Attacked the U.S.?" *Newsweek Online*, December 11, 2017, http://www.newsweek.com/islamic-state-america-attacks-744497 (accessed February 22, 2017).

[32] Peter Neumann goes into greater detail about the psychological processes that underpin the reasons why individuals become radicalized through online exposure to propaganda. "In recent years, experts have identified (at least) six processes and dynamics that explain online radicalization – that is, how the Internet promotes extremist beliefs and/or violent methods. The first two of these processes [Mortality Salience and Sense of Moral Outrage] deal with the consequences of being exposed to extremist content…in most cases, radicalization results from individuals being immersed in extremist content for extended periods of time, the amplified effects of graphic images and video, and the resulting emotional desensitization…. The third and fourth explanations of online radicalization [Criminogenic Environments and Online Disinhibition] emphasize the social environment in which people are exposed on the Internet…. The fifth process [Mobilization through Role-Playing]…is an offshoot of explanations that emphasize the social and interactive nature of the Internet….The sixth explanation [Links into Terrorist Structures] [is based on] connecting people with similar interests, even across great distances and with no prior interaction." Neumann, "Options and Strategies for Countering Online Radicalization," 436-437.

[33] Aly et al., "Terrorist Online Propaganda and Radicalization," 4.

[34] Ibid.

[35] Ibid.

[36] Ibid., 5.

[37] Berger, "Tailored Online Interventions," 19.

[38] Charlie Winter, *Documenting the Virtual Caliphate* (London: The Quilliam Foundation, 2015), 11.

[39] Berger, "Tailored Online Interventions," 21.

[40] Ibid., 23.

[41] Aly et al., "Terrorist Online Propaganda and Radicalization," 2.

[42] "Daniel Milton, *Communication Breakdown: Unraveling the Islamic State's Media Efforts* (West Point, NY: United States Military Academy, Combating Terrorism Center, October 2016), 51, https://ctc.usma.edu/app/uploads/2016/10/ISMedia_Online.pdf (accessed December 20, 2017).

[43] Karen J. Greenberg, "Counter-Radicalization via the Internet," *The Annals of The American Academy of Political and Social Science* 668, no. 1 (November 2016): 168.

[44] Winter, *The Virtual "Caliphate*,*"* 36.

[45] Milton, *Communication Breakdown*, 46.

[46] Winter, *The Virtual "Caliphate*,*"* 36.

[47] Daniel Wagner, "The Islamic State: From Physical Caliphate to Virtual Jihad," *Huffington Post*, November 7, 2017, https://www.huffingtonpost.com/entry/the-islamic-state-from-physical-caliphate-to-virtual_us_5a022455e4b02f3ab3377dd6 (accessed February 15, 2018): Winter, *The Virtual "Caliphate*,*"* 37.

[48] Milton, *Communication Breakdown,* 50.

[49] Winter, *The Virtual "Caliphate*,*"* 18.

[50] Aly et al., "Terrorist Online Propaganda and Radicalization," 4. Milton differed in approach during his analysis by grouping ISIS propaganda into five thematic categories: Commercial, Military, Religious, Governance, Lifestyle, and Other. Milton, *Communication Breakdown*, 23.

[51] Winter, *The Virtual "Caliphate*,*"* 6.

[52] House Committee on Foreign Affairs, *Countering the Virtual Caliphate: The State Department's Performance*, 114th Cong., 2nd sess., 2016, 22, https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg20744/pdf/CHRG-114hhrg20744.pdf (accessed February 19, 2018).

[53] Winter, *Documenting the Virtual Caliphate*, 30.

[54] "…of the more than 9,000 Islamic State visual media releases coded for this project, more than 50 percent focus on themes outside of the battlefield, such as governance, justice, the importance of religious practices, and life in the caliphate. Moreover, only a small percentage of releases, approximately nine percent, specifically show the commission or aftermath of executions or battlefield killings." Milton, *Communication Breakdown*, iv.

[55] Kathleen Ann Ruane, *The Advocacy of Terrorism on the Internet: Freedom of Speech Issues and the Material Support Statutes* (Washington, DC: U.S. Library of Congress, Congressional Research Service, September 8, 2016), 1, https://fas.org/sgp/crs/terror/R44626.pdf (accessed December 9, 2017).

[56] Clarke and Winter, "The Islamic State may be Failing."

[57] Greenberg, "Counter-Radicalization via the Internet," 167.

[58] Winter, *Documenting the Virtual Caliphate*, 39.

[59] Ibid., 7.

[60] Greenberg, "Counter-Radicalization via the Internet," 167.

[61] Ibid., 170-171.

[62] Berger, "Tailored Online Interventions," 20.

[63] Peter Holley, "YouTube Battles ISIS with a Redirect Strategy," *Washington Post*, July 25, 2017.

[64] Ruane, *The Advocacy of Terrorism on the Internet,* 2.

[65] Greenberg, "Counter-Radicalization via the Internet," 167.

[66] Milton, *Communication Breakdown*, 45.

[67] Winter, *Documenting the Virtual Caliphate*, 11.

[68] Offensive Cyberspace Operations are defined as, "operations intended to project power by the application of force in or through cyberspace." U.S. Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication 3-12 (Washington, DC: U.S. Joint Chiefs of Staff, February 5, 2013), GL-4, http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf (accessed February 18, 2018).

[69] U.S. Strategic Command, "FRAGORD 01 to TASKORD 16-0063 to Establish Joint Task Force (JTF) – Ares to Counter the Islamic State of Iraq and the Levant (ISIL) in Cyberspace," May 5, 2016, http://www.stratcom.mil/Portals/8/Documents/FOIA/FOIA%2017-023,%2017-033,%2017-064%20-%20USCYBERCOM%20Joint%20Task%20Force%20Areas.pdf?ver=2017-04-19-111941-797 (accessed February 8, 2018).

[70] Ibid.

[71] Dan Lamothe, "How the Pentagon's Cyber Offensive Against ISIS Could Shape the Future for Elite U.S. Forces," *Washington Post Online*, December 16, 2017, https://www.washingtonpost.com/news/checkpoint/wp/2017/12/16/how-the-pentagons-cyber-offensive-against-isis-could-shape-the-future-for-elite-u-s-forces/?utm_term=.a331b2ef7c91 (accessed February 18, 2018).

[72] Ellen Nakashima, "U.S. Military Cyber Operation to Attack ISIS Last Year Sparked Heated Debate Over Alerting Allies," *Washington Post Online*, May 9, 2017, https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html?utm_term=.1eb0bffbfed8 (accessed February 18, 2018).

[73] Ibid.

[74] Milton, *Communication Breakdown,* 46.

[75] U.S. Government Accountability Office, *Countering ISIS and its Effects*, 32.

[76] Here the focus is on public diplomacy because several departments and agencies of the U.S. government have public affairs offices and personnel whose responsibility it is to inform publics. However, public diplomacy is also charged with influencing foreign publics. "The mission of American public diplomacy is to support the achievement of U.S. foreign policy goals and objectives, advance national interests, and enhance national security by informing and influencing foreign publics and by expanding and strengthening the relationship between the people and Government of the United States and citizens of the rest of the world." U.S. Department of State, Under Secretary for Public Diplomacy and Public Affairs, https://www.state.gov/r/ (accessed February 18, 2018).

[77] "An attribution method is the stance the USG [U.S. Government] takes in acknowledging responsibility for messages and actions." Department of the Army, *Military Information Support Operations*, Field Manual 3-53 (Washington, DC: Department of the Army, January 2013), 2-4.

[78] Title 22 United States Code § 2732 (c), "Public Diplomacy Responsibilities of the Department of State," https://www.law.cornell.edu/uscode/text/22/2732 (accessed February 19, 2018).

[79] "In response to the 9/11 terrorist attacks, Congress enacted the AUMF authorizing the President to use military force against 'those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons....' Although the Islamic State does not appear to fall within that language, it is possible that the executive branch regards it as one of the 'associated forces' fighting alongside Al Qaeda and the Taliban that it asserts are also targetable under the 2001 AUMF." Matthew C. Weed, *A New Authorization for Use of Military Force Against the Islamic State: Issues and Current Proposals* (Washington, DC: U.S. Library of Congress, Congressional Research Service, February 21, 2017), 2, https://fas.org/sgp/crs/natsec/R43760.pdf (accessed February 24, 2018).

[80] Barack Obama, "Developing an Integrated Global Engagement Center to Support Government-wide Counterterrorism Communications Activities Directed Abroad and Revoking Executive Order 13584," Executive Order 13721 (Washington, DC: The White House, March 14, 2016), https://www.federalregister.gov/documents/2016/03/17/2016-06250/developing-an-

integrated-global-engagement-center-to-support-government-wide-counterterrorism (accessed February 24, 2018).

[81] David Patrikarakos, *War in 140 Characters: How Social Media is Reshaping Conflict in the Twenty-First Century* (New York, NY: Basic Books, 2017), 234-235.

[82] Matthew C. Weed, *Global Engagement Center: Background and Issues* (Washington, DC: U.S. Library of Congress, Congressional Research Service, August 4, 2017), 2, https://fas.org/sgp/crs/row/IN10744.pdf (accessed January 1, 2018).

[83] Ibid.

[84] Ibid.

[85] "Most experts agree that government is not the most effective conveyor of these messages [challenges to the violent extremists' ideology and to their political and/or religious claims]. It has a role to play in dispelling rumors and false claims that relate to its own actions, but – for the most part – its involvement in countermessaging is thought to be most effective when limited to acting as enabler, supporting mainstream community groups and the victims of terrorism to become more effective at telling their stories and reaching the audiences that are potentially vulnerable to becoming radicalized." Neumann, "Options and Strategies for Countering Online Radicalization," 447.

[86] House, *Countering the Virtual Caliphate*, 1-2.

[87] Patrikarakos, *War in 140 Characters*, 243.

[88] Greg Miller, "Panel Casts Doubt on U.S. Propaganda Efforts Against ISIS," *Washington Post Online*, December 2, 2015, https://www.washingtonpost.com/world/national-security/panel-casts-doubt-on-us-propaganda-efforts-against-isis/2015/12/02/ab7f9a14-9851-11e5-94f0-9eeaff906ef3_story.html?utm_term=.b759db285d8e (accessed February 19, 2018).

[89] "'BPC' refers to a broad set of missions, programs, activities, and authorities intended to improve the ability of other nations to achieve security-oriented goals shared with the United States and encompasses, among other things, DOD security cooperation and State security assistance efforts funded with U.S. government appropriations." U.S. Government Accountability Office, *Building Partner Capacity: Inventory of Department of Defense Security Cooperation and Department of State Security Assistance Efforts*, GAO-17-255R (Washington, DC: U.S. Government Accountability Office, March 24, 2017), 3, https://www.gao.gov/assets/690/683682.pdf (accessed February 24, 2018).

[90] U.S. Government Accountability Office, *Countering ISIS and its Effects*, 33. See also: U.S. Department of State, "Launch of the Sawab Center," July 8, 2015, https://2009-2017.state.gov/r/pa/prs/ps/2015/07/244709.htm (accessed February 19, 2018).

[91] "The Arabic word Sawab is often translated into English as 'doing the right thing' or being on the 'right path'. Sawab seeks to do just that by giving a voice to the millions of Muslims and others around the world that stand united against the terrorism and falsehood propagated by DAESH. Sawab will use online communication and social media tools to put things in the right perspective and to amplify those many moderate voices that too often get drowned out by the noise of the extremists." Sawab, http://80.227.220.174/ (accessed February 19, 2018).

[92] Guy Taylor, "Muslim-Run Messaging Center Wages Cyberwar on Islamic State," *Washington Times Online*, October 19, 2017, https://www.washingtontimes.com/news/2017/oct/19/sawab-center-muslim-run-messaging-center-wages-cyb/ (accessed February 19, 2018).

[93] Richard Stengel, "Statement of Richard A. Stengel," 2.

[94] Within the Department of Defense, MISO is defined as "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 in a manner favorable to the originators objectives." U.S. Chairman of the Joint Chiefs of Staff, *Military Information Support Operations Supplement to the Joint Strategic Capabilities Plan*, Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3110.05F, (Washington, DC: U.S. Chairman of the Joint Chiefs of Staff, April 7, 2017), 2.

[95] Along with several other activities, active duty MISO are organized within United States Code Title 10 §167, as a special operations activity, falling under the purview of U.S. Special Operations Command (USSOCOM). Title 10 United States Code §167, http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title10-section167&num=0&edition=prelim (accessed February 19, 2018).

[96] There are three major categories for attributing U.S. military products: U.S. government attributed, partner attributed, and non-attributed. For products attributed to the U.S. government, they can either utilize immediate or delayed attribution (authorized in certain circumstances such as for operations security). Partner attribution can be utilized in operations where the partner (usually nation or security forces) concurs – often utilized in security assistance or counter-insurgency operations. Department of the Army, *Military Information Support Operations*, Field Manual 3-53, 2-5.

[97] Defined as "an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but does not include: (1) activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities; (2) traditional diplomatic or military activities or routine support to such activities; (3) traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or (4) activities to provide routine support to the overt activities (other than activities described in paragraph (1), (2) or (3)) of other United States Government agencies abroad." *National Security Act of 1947*, Public Law No. 235, 80th Congress (July 26, 1947), as amended by Public Law 102-88 (August 14, 1991) §503(e) [Title 50, United States Code, §3093].

[98] Another exception is "routine support to such activities:" "The committee considers as 'routine support' unilateral U.S. activities to provide or arrange for logistical or other support for U.S. military forces in the event of a military operation that is to be publicly acknowledged. Examples include caching communications equipment or weapons, the lease or purchase from unwitting sources of residential or commercial property to support an aspect of an operation, or obtaining currency or documentation for possible operational uses, if the operation as a whole is to be publicly acknowledged." Marshall Curtis Erwin, *Covert Action: Legislative Background and Possible Policy Questions* (Washington, DC: U.S. Library of Congress, Congressional Research

Service, April 10, 2013), 8, https://fas.org/sgp/crs/intel/RL33715.pdf (accessed January 2, 2018).

[99] "It is the intent of the conferees that 'traditional military activities' include activities by military personnel under the direction and control of a United States military commander (whether or not the U.S. sponsorship of such activities is apparent or later to be acknowledged) preceding and related to hostilities which are either anticipated (meaning approval has been given by the National Command Authorities for the activities and or operational planning for hostilities) to involve U.S. military forces, or where such hostilities involving United States military forces are ongoing, and, where the fact of the U.S. role in the overall operation is apparent or to be acknowledged publicly. In this regard, the conferees intend to draw a line between activities that are and are not under the direction and control of the military commander. Activities that are not under the direction and control of a military commander should not be considered as 'traditional military activities.'" Erwin, *Covert Action*, 7.

[100] Daniel Silverberg and Joseph Heimann, "An Ever-Expanding War: Legal Aspects of Online Strategic Communication," *Parameters* 39, no. 2 (Summer 2009): 77-78, 81.

[101] Ibid., 82.

[102] Ibid.

[103] Sharon Weinberger, "Special Operations Command's Trans-Regional Web Initiative," January 18, 2008, https://www.wired.com/2008/01/special-operati/ (accessed February 20, 2018). See also Tom Vanden Brook, "House Fails to Kill Pentagon's Foreign Websites," *USA Today Online*, July 24, 2013, https://www.usatoday.com/story/news/politics/2013/07/24/military-propaganda-information-operations-gao/2583837/ (accessed February 20, 2018).

[104] Vanden Brook, "House Fails to Kill Pentagon's Foreign Websites." See also Peter Cary, *The Pentagon and Independent Media – An Update* (Washington, DC: Center for International Media Assistance, November 2015), 8, http://www.cima.ned.org/wp-content/uploads/2015/11/CIMA-The-Pentagon-and-International-Media-Update.pdf (accessed February 20, 2018).

[105] Matthew Wallin, *Military Public Diplomacy: How the Military Influences Foreign Audiences* (Washington, DC: American Security Project, February 2015), 11, https://www.americansecurityproject.org/wp-content/uploads/2015/02/Ref-0185-Military-Public-Diplomacy.pdf (accessed February 20, 2018).

[106] Theohary and Rollins, "*Terrorist Use of the Internet*," 2.

[107] Memorandum from the Deputy Secretary of Defense, "Policy for Department of Defense (DoD) Interactive Internet Activities," June 8, 2007; Department of Defense Inspector General, *DoD Effectively Planned and Executed Military Information Support Operations for Operation Inherent Resolve but Needs to Develop Formal Processes and Procedures for Web-Based Operations*, Report No. DODIG-2016-111 (Washington, DC: U.S. Department of Defense, July 20, 2016), 9, https://media.defense.gov/2017/Aug/09/2001790494/-1/-1/1/DODIG-2016-111%20(U)%20%5bREDACTED%5d.PDF (accessed February 20, 2018).

[108] James N. Mattis, A *Statement on the Posture of U.S. Central Command*, Posture Statement presented to the Senate Armed Services Committee, 113th Cong., 1st sess. (Tampa,

FL: U.S. Central Command, March 5, 2013), 26, https://fas.org/irp/congress/2013_hr/030513mattis.pdf (accessed February 20, 2018).

[109] Department of Defense Inspector General, "DoD Effectively Planned and Executed Military Information Support Operations," 3.

[110] Karen Parrish, "CENTCOM Counters ISIL Propaganda," *U.S. Department of Defense News Online*, July 6, 2016, https://www.defense.gov/News/Article/Article/827761/centcom-counters-isil-propaganda/ (accessed February 20, 2018).

[111] Ibid.

[112] Mattis, "Statement of General James N. Mattis," 25.

[113] "The Smith-Mundt Act regulates foreign dissemination of information to audiences outside the United States, and prohibits the targeting of U.S. citizens for influence." Department of the Army, *Military Information Support Operations*, Appendix-5. See also Title 22 United States Code § 1461-1a, https://www.law.cornell.edu/uscode/text/22/1461%E2%80%931a (accessed February 19, 2018).

[114] Parrish, "CENTCOM Counters ISIL Propaganda."

[115] Silverberg and Heimann, "An Ever-Expanding War," 88.

[116] Associated Press, "Congress Probes Islamic State Counterpropaganda Operations," *ABC News Online*, March 10, 2017, http://abcnews.go.com/amp/Politics/wireStory/congress-probes-islamic-state-counter-propaganda-operations-46036905 (accessed February 25, 2018).

[117] Weed, *Global Engagement Center: Background and Issues*, 2. Along with that new mandate came increases in funding, with the GEC's budget doubled. In fiscal year (FY) 2016 the GEC received a budget of $16 million, which then increased to approximately $32 million in FY 2017. The NDAA also included language that would enable the Secretary of Defense to transfer up to $60 million to the GEC. As of February 2018, Defense Department may be looking to transfer approximately $40 million in FY18 funds to the GEC, on top of the $35 million ($19.8 million to focus against ISIS) already budgeted for the GEC. See Oren Dorell, "State Department's Answer to Russian Meddling is about to be Funded," *USA Today* Online, February 13, 2018, https://www.usatoday.com/story/news/world/2018/02/13/state-department-answer-russian-meddling-funded/322992002/ (accessed February 19, 2018).

[118] Votel, "The Posture of U.S. Central Command," 4-5.

[119] Now codified in public law as Title 10, U.S. Code §127e; "Support of Special Operations to Combat Terrorism," https://www.law.cornell.edu/uscode/text/10/127e (accessed February 25, 2018).

[120] Aaron R. Lobel, "Countering the Virtual Caliphate," Congressional Record (June 23, 2016), 2-3, http://docs.house.gov/meetings/FA/FA00/20160623/105128/HHRG-114-FA00-Wstate-LobelA-20160623.pdf (accessed December 29, 2017).