REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
30-04-2018	Research	August 2017 - April 2018

4. TITLE AND SUBTITLE
An Organization for Information Warfare in Support of National Security Requirements

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Major Robert W. Woodard

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC School of Advanced Warfighting
Marine Corps University
2044 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

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

12. DISTRIBUTION/AVAILABILITY STATEMENT
Unlimited

13. SUPPLEMENTARY NOTES
N/A

14. ABSTRACT

The United States and its allies have been under increasing technological and psychological attack in cyberspace, a trend that will continue in both quantity and cost as our reliance on connectivity and computers also grows. These competitors will continue to seek advantage through technologies that are becoming increasingly tailored for the cognitive dimension. The 2017 National Security Strategy (NSS) states that, "America's competitors weaponized information to attack the values and institutions that underpin free societies..." The NSS also states that "U.S. efforts to counter the exploitation of information by rivals have been tepid and fragmented. U.S. efforts have lacked a sustained focus and have been hampered by the lack of properly trained professionals." This paper contends that a Combined (Coalition) Interagency Information Warfare Task Force should be stood up to compete in the information environment based on requirements drawn from national values, institutional capabilities and best practices, and competitors' information warfare activities.

15. SUBJECT TERMS
Information Warfare, Information Operations, Influence, Cyber, Internet, Cognitive, Psychological Profile, Persuasive Technology, Freedom of Speech, Global Domain, Intelligence, OSINT, Social Media, Russia, China, Iran, DPRK, Transnational Threat Group

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			MCU/School of Advanced Warfighting
Unclassified	Unclassified	Unclassified		18	19b. TELEPHONE NUMBER *(Include area code)*

United States Marine Corps
School of Advanced Warfighting
Marine Corps University
3070 Moreell Avenue
Marine Corps Combat Development Command
Quantico VA 22134

FUTURE WAR PAPER

An Organization for Information Warfare in Support of National Security Requirements

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF OPERATIONAL STUDIES

Maj Robert Woodard

AY 2017-18

Mentor: Dr. Meyer

Approved: Bradley J. Meyer PhD.

Date: 17 May 2018

Disclaimer

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE SCHOOL OF ADVANCED WARFIGHTING OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

The United States and its allies have been under increasing technological and psychological attack in cyberspace, a trend that will continue in both quantity and cost as our reliance on connectivity and computers also grows. In particular, the 2017 National Security Strategy (NSS) for the United States of America states that, "America's competitors weaponized information to attack the values and institutions that underpin free societies, while shielding themselves from outside information."[1] The NSS also states that "U.S. efforts to counter the exploitation of information by rivals have been tepid and fragmented. U.S. efforts have lacked a sustained focus and have been hampered by the lack of properly trained professionals."[2] In order to compete with these rivals in order to meet the NSS goals of protecting Americans, promoting prosperity, preserving peace, and advancing American influence, the U.S. must deter, disrupt, and potentially defeat the information warfare waged by these competitors. So, what are the capability requirements for information warfare under U.S. strategy? This paper contends that drawing from the best practices and capabilities of the Open Source Enterprise, the National Security Agency, DOJ's National Security Division, the Global Engagement Center, and U.S. Cyber Command, a Combined (Coalition) Interagency Information Warfare Task Force should be stood up to compete in the information environment based on requirements drawn from national values and competitors' information warfare activities.

The focus on information warfare specifically addresses the threat to the psychological or cognitive dimension of the information environment rather than the technological attacks typically associated with cyberspace warfare. Joint Publication 3-13 on Information Operations defines the informational environment as consisting of the

interrelated dimensions of the physical, informational, and cognitive. In this definition the informational dimension "specifies where and how information is collected, processed, stored, disseminated, and protected" whereas the cognitive dimension consists of "the minds of those who transmit, receive, and respond to or act on information."[3] The distinction between cognitive information warfare and technological cyberspace warfare is that while cyberspace warfare can attack the physical and informational dimensions to achieve any number of desired effects, information warfare focuses on achieving effects in the cognitive dimension as an ultimate objective and may not require traditional cyber capabilities.

With that distinction in mind, the future trend in the information environment consists of technologies that take specific aim at the cognitive dimension, increasing the vulnerability of society to malicious actors. From the NSS, "[America's competitors] exploit marketing techniques to target individuals based on their activities, interests, opinions, and values."[4] Commercial companies such as Facebook, Google, and Amazon, create profiles of users to increase advertising or product revenues, tailoring content to the individual consumer. Stanford University's Persuasive Technology Laboratory studies "how computing products – from websites to mobile phone software – can be designed to change what people believe and what they do."[5] In the future, it is probable that all information an individual consumes, whether on the internet, social media, a phone application, or recommendations from smart appliances, will be built around the individual's cognitive profile that has been generated as a marketing strategy by commercial companies. This presents an increasing opportunity for malicious actors engaged in information warfare, such as Russian actors' use of Facebook's, Twitter's,

and Google's algorithms to deliver content prior to the Presidential election in 2016. As reported in the *New York Times*, "Now the companies must grapple with how Russian agents used their technologies exactly as they were meant to be used – but for malevolent purposes."[6] Malicious actors, or competitors, will continue to seek advantage through technologies that are becoming increasingly tailored for the cognitive dimension.

The 2017 NSS identifies three sets of competitor's for political power, each of which employ information warfare distinctly. The first set consists of the powers of Russia and China. Both of these powers aim to control information and information flow, both internally and externally. One primary Russian textbook distinguishes between "information-psychological warfare" and "information-technology warfare", stating that the former is conducted at all times while the latter is used during armed conflict.[7] Further, the strategic leader of Russian doctrine and current Chief of the General Staff, General Valery Gerasminov, wrote that a key feature in modern warfare is "simultaneous effects to the entire depth of enemy territory, in all physical media and in the information domain."[8] Chinese information warfare aims at "the enemy's information detection sources, information channels, and information-processing and decision making systems."[9] Specifically, the information warfare concept adopted in 2003 is called "three warfares" which consists of public opinion warfare, psychological warfare, and legal warfare.[10] The 2014-2015 data breach at the U.S. Office of Personnel Management that resulted in the loss of over 20 million federal employees records was attributed to China, and while the use of those records are a source of speculation, it is certainly possible that they are catalogued for "three warfares" use.

The second set of competitors in the NSS consists of the rogue states of Islamic Republic of Iran and the Democratic People's Republic of Korea. Like the previous powers of Russia and China, they aim for both external and internal control of information, however, they focus less on the external projection of information warfare. Both of these nations have strict internal controls, with a separate intranet and robust content-control. Externally, these rogue states employ information warfare in two distinctive ways. One, in a coercive manner, attempting to establish deterrence by employing destructive cyberspace warfare with no other motive in response to provocations. Examples include Iranian denial-of-service attacks against U.S. banks in 2011-2013, believed to be in retaliation for the 2010 Stuxnet attack against Iranian nuclear centrifuges, and the North Korean 2014 Sony Pictures hack believed to be retaliation for a Sony comedy film about the North Korean regime. The second distinctive method of information warfare employed by these states closely aligns with the Chinese concept of legal warfare. Both nations are aspiring nuclear powers who use diplomacy and international organizations to win concessions and buy time for further development.

The third set of adversaries in the NSS is described as the Transnational Threat Group, which comprises jihadi terror groups and transnational criminal organizations. Jihadi terrorists employ information warfare for radicalization and recruitment, as well as inciting attacks against the U.S. and its allies. In the past few years the terrorist group ISIS has been noted for its professional media production as well as prolific use of social media platforms. Transnational criminal organizations thrive in areas of weak governance and use information warfare to threaten opponents, promote an image of

power, and to recruit by glorifying the cartel lifestyle. One common challenge cited in the NSS for both jihadi groups and the criminal organizations are their reliance on "the dark web to evade detection as they plot, recruit, finance, and execute their operations."[11]

Before discussing the requirements to counter information warfare efforts by these three sets of competitors it is essential to consider principles and values regarding information and the cyber domain. A key national value is American freedom of speech (guaranteed under the First Amendment to the Constitution of the United States) and the associated disdain for censorship. This will require that any effort to counter information warfare should not focus on the information itself but instead focus on identifying foreign actors involved in creating and/or disseminating the information. As an example, the Russian efforts during the 2016 election used Facebook advertisements that appealed to and were meant to inflame various American interest groups but these advertisements were not different from the type of media these interest groups commonly spread themselves. Russian efforts were to amplify this divisive thinking. By focusing in on the foreign actors in the media environment, rather than the media content they generate, their information warfare efforts are countered in a manner keeping with a key national value.

Another key national principle to consider is that the Internet is a global common domain that needs to be open and free.[12] The foremost implication is that no American counter information warfare efforts can restrict the flow of data globally. The second order implication is that our competitors have open and free access to engage in information warfare activities against the United States and its Allies. Lastly, there can be no grand defensive mechanism such as China's "Great Firewall", which would violate

this principle. U.S. counter information warfare activities will need to focus on specific foreign actors.

Now that the focus of effort has been defined with these national values, the capabilities that are required to counter information warfare efforts can be examined. The NSS states, "Protecting American interests requires that we compete continuously within and across these contests, which are being played out in regions around the world."[13] And further, "The United States will deter, defend, and when necessary defeat malicious actors who use cyberspace capabilities against the United States."[14] To meet these strategic objectives the United States will need to both create and strengthen capabilities.

First, the U.S. requires dedicated intelligence support to gain proactive situational awareness in the information environment. As previously stated, the growing threat of adversaries' use of social media and its associated persuasive technologies is at the forefront of the information warfare campaigns. In order to discern a pattern of activity on social media, whether it is Facebook, Twitter, or YouTube for example, analysts will require continuous surveillance across the breadth of those platforms, likely supported by big data algorithms, machine learning, and advanced analytic software. Currently the lead component in the Intelligence Community for Open Source Intelligence (OSINT) is the Open Source Enterprise (OSE), functionally managed under the Central Intelligence Agency (CIA). However, the OSE focuses on enriching classified data for analysis (adding unclassified information to the classified) rather than focusing on OSINT as a stand-alone intelligence discipline as social media analytics would require. Intelligence support to information warfare would require either that a strengthened OSE provide

persistent surveillance across media platforms in order to identify adversary activities, or that an entirely new organization is formed to conduct the required support.

Intelligence support to information warfare would not be solely OSINT. Defined by Joint Publication 2-0, "OSINT is intelligence based on open source information that any member of the public can lawfully obtain by request, purchase, or observation."[15] While an information or disinformation campaign necessarily requires that the content is available to the public, aspects of information warfare is conducted in the surface web, the deep web, and the dark web. The surface web, which includes social media, is defined as that part of the internet that is available to the public and indexed by normal search engines, such as Google, and is estimated to approximate only four percent of the entire internet. By both definitions then OSINT alone only applies to that four percent. Activities that occur on the deep web, which is the other 96 percent, lies behind firewalls or requires login credentials (web forums, private social media, academic sites). The dark web is a portion of the deep web which can only be accessed by specialized internet browsers, the most common being The Onion Router (TOR).

Intelligence support to information warfare then requires authorities to collect beyond the surface web and in particular on the dark web where transnational threat groups conduct operations. Human Intelligence (HUMINT) authorities allow for the creation of cyberspace personas to conduct collection on the internet beyond the surface web. The OSE, functionally managed by the CIA, would have the necessary authorities to support information warfare requirements by virtue of relationship (CIA is the Intelligence Community lead for HUMINT), but still would lack capacity and focus on this new mission. Additionally, the Intelligence Community does not have the authority

to collect on American citizens. An intelligence organization collecting across the breadth of the internet to locate adversary activities would require Department of Justice (DOJ) membership to ensure that the appropriate authorities are available to analyze account activities presumed to be American. Therefore, a new intelligence organization, with all required authorities, to focus on intelligence support to information warfare would most effectively meet the strategic requirement as laid out in the NSS.

The second requirement to effectively meet the NSS strategic objectives is an organization to operationalize the intelligence in three parts. This organization would need to have relationships or liaison officers to share information with the Department of Defense (DOD), the Interagency (particularly the DOJ), our allies, and commercial industry. It would need to have the authorities and capabilities to inform both domestic and foreign publics of adversary information warfare activities. Lastly, it would need the authorities and capabilities to disrupt, defend, or defeat adversary activities if necessary.

In January 2017, the former Director of National Intelligence, in a testimony to the Senate Armed Services Committee about Russian interference in the 2016 elections, said, "...I do think that we could do with having a USIA on steroids... The United States Information Agency [is needed] to fight this information war a lot more aggressively than we're doing right now."[16] The USIA existed from 1953 to 1999 with the mission "to understand, inform, and influence foreign publics in promotion of the national interest, and to broaden the dialogue between Americans and U.S. institutions, and their counterparts abroad."[17] While the testimony does not provide further insight into Director Clapper's recommendation for a "USIA on steroids," from 1981 to 1992 the State Department led the Interagency Active Measures Working Group (IAWG) for a

more robust effort against the Soviet Union's propaganda. (The IAWG effectively ended with the fall of the Berlin Wall in 1989, and the USIA began reporting on Soviet Active Measures in 1988.)[18] Between these two organizations, information warfare activities were effectively analyzed, reported, and publicized.

The final missing part of the requirement is a part of the organization to disrupt, defend, and potentially defeat adversary information warfare activities. Assuming that partnership with DOJ, allies, and industry are unable to counter all information warfare activities, a professional DOD element would be able to project cyberspace power sufficient to deliver the desired effects. This may include disrupting or denying access to the information warfare materials to target audiences in other nations, or potentially disrupting the generation of the activities at the source. This DOD force would likely come from U.S. Cyber Command (USCYBERCOM), which includes in its mission statement that it will "ensure US/allied freedom of action in cyberspace and deny the same to our adversaries."[19]

If the capability requirements for information warfare under U.S. strategy includes robust intelligence support beyond current organizational capability and an operational organization that mainly ceased to exist almost two decades ago, what current means exist that can be strengthened to meet the requirement, or does new capability need to be created? From an intelligence perspective, the National Security Agency (NSA) is likely the best candidate for big data analytics, its foreign signals intelligence (SIGINT) mission, and partnership with industry. However, public opinion and national values will likely oppose an NSA mission that actively monitors all social media regardless of any safeguards used by the Agency.

Operationally, three current organizations currently work aspects of the information warfare fight as discussed: the Global Engagement Center (GEC), USCYBERCOM, and DOJ's National Security Division (NSD). However, the GEC, led by the State Department is only mandated with "coordinating U.S. counterterrorism messaging to foreign audiences."[20] The head of USCYBERCOM, Admiral Michael Rogers, provided testimony to the Senate Armed Services Committee in May 2017 regarding information warfare that, "It right now is not in our defined set of responsibilities per se… I would be the first to admit that [information warfare] is not what our workforce is optimized for… we are certainly not where we need to be."[21] DOJ's NSD is the Department's lead for cyber based threats and has originated indictments for adversary actions in cyberspace. The NSD also runs the Foreign Agent Registration Act (FARA) program that requires registration of foreign propagandist actors. An expansion of FARA requirements (identifying oneself as a foreign actor in any published media) to social media could provide one line of effort in the information warfare struggle, but would likely require massive restructuring to meet the requirements already identified.

With the lack of any one organization that can be simply strengthened to meet the strategic requirement to deter, disrupt, and potentially defeat competitors waging information warfare, an organization needs to be created. Drawing from the best practices and capabilities of the Open Source Enterprise, the National Security Agency, DOJ's National Security Division, the Global Engagement Center, and U.S. Cyber Command, a Combined (Coalition) Interagency Information Warfare Task Force should be stood up to compete in the information environment. The core of the organization

would be comprised of a multi-disciplinary intelligence directorate, a combined and interagency engagement directorate for industry, law enforcement, and allies, an information directorate to inform and publicize information warfare activities to foreign and domestic audiences, and a cyberspace warfare directorate to provide the technological cyber power when required.

The multi-disciplinary intelligence directorate would likely consist of the majority of manpower for the organization due the difficulty of locating, identifying, and attributing information warfare activities across the breadth of the internet. U.S. Code Title 50 establishes the authorities for foreign intelligence, which includes the primary disciplines required --OSINT, HUMINT, and SIGINT-- for surveilling the information environment. U.S Code Title 28 establishes the authorities for the Department of Justice, specifically the Federal Bureau of Investigation, which would be necessary for initial triage of any accounts presumed to be American due to language (English), claimed location, or claimed affiliation with U.S. companies (for example).

The combined and interagency engagement directorate is primarily responsible for information sharing with stakeholders that can take action or are affected by adversary information warfare activities. The DOJ would again be operating with Title 28 authorities, and other participating Interagency partners would likewise derive their authorities from their parent organizations. Many of these information sharing activities are already considered best practices in the cyber security realm.

The information directorate also would have a responsibility for information sharing, but it would be with the general public. U.S. Code Title 22 governs the State Department and provides authorities for disseminating information to foreign audiences.

Domestically, the Department of Justice maintains numerous avenues for sharing threat information with the public. There is also a significant potential for this directorate to enable two-way information sharing, essentially encouraging civilian support to monitoring and identifying suspicious activity. For example, hacktivist groups caused significant disruption to ISIS social media accounts by databasing and reporting tens of thousands of accounts for violations of terms of service.[22] Leveraging a volunteer effort that already exists not only alleviates the burden from solely falling to the intelligence directorate, but also potentially provides localized grassroots sensors in areas that might fall below the threshold of pattern analysis or priority, such as areas for transnational threat group recruitment and activity.

The cyberspace warfare directorate would operate under U.S. Code Title 10 authorities, governing the activities of the military services. Under USCYBERCOM's current model, all cyberspace warfare authorities are centralized at USCYBERCOM and effects must be requested. By providing forces in direct support, with the requisite policy authorities, these forces can quickly support any required effects due to mission focus and familiarity with the cyber terrain.

While referring to the four parts of the proposed Task Force as directorates alludes to a large scale effort, the scalability of each functional area is determined by the amount of work that has to be done. While the intelligence directorate will need persistent collection and analysis, both current technology and anticipated developments in big data analytics and artificial intelligence aids the troop-to-task requirement by alleviating manpower intensive tasking. Notifications to allies, industry, and the public can also be largely automated. Purposefully not included in the proposal is the

requirement for counter-narrative or propaganda generation due to the manpower intensity required. Those efforts are, and should continue to be, the responsibility of the respective Combatant Commanders, informed by the Task Force identification of adversary activities.

An alternative to the proposed Combined Interagency Task Force would be to provide the functional support to Combatant Commanders who have responsibility for competing with Russia, China, Iran, DPRK, and transnational threat groups. Benefits would include a focus on regional stability and better coordination with theater shaping operations. However, there would be a lack of focus on activities against the American homeland as well as a loss in efficiency in analyzing the information environment across multiple commands. Ultimately it would be a less effective course of action, but could gain some effectiveness for local efforts such as against transnational threat groups.

To summarize, the 2017 national Security Strategy requires that the U.S. "deter, defend, and when necessary defeat malicious actors who use cyberspace capabilities against the United States" but also acknowledges that U.S. efforts have lacked focus. Focusing capabilities on the cognitive information warfare aspect of the competitors' activities aligns more closely with how those adversaries behave in the information environment towards the U.S. and our allies, rather than focusing on simply the technological aspect of the threat. The future information environment is trending towards increased vulnerability of individuals due to the use of persuasive technologies and marketing strategies that develop individualized psychological profiles based on preference. Without an organization that has the intelligence and operational capabilities to identify and counter information warfare activities, the U.S. must create one that

includes the functional areas of intelligence, engagement, informing, and if necessary use cyberspace power to disrupt and defeat those activities. Creating a new Combined Interagency Task Force would provide the focus of effort and be most effective to compete in the information environment against information warfare activities.

The United States has not robustly countered information warfare since the fall of the Soviet Union. Standing up a Task Force would message our competitors that the information environment is now contested and that they would no longer enjoy freedom of maneuver in those spaces. Surveillance in the information environment will also provide indications and warning of competitors' activities, such as Russian annexation of Crimea or ISIS's rise in Iraq and Syria. Standing up the Task Force will also raise concerns with the American populace whose national values favor freedom of speech and an open internet. Transparency through engagement and information should alleviate these concerns, while also building deterrence towards our adversaries. In the end, creating a holistic capability to engage our competitors' information warfare activities meets the NSS goals of protecting Americans, promoting prosperity, preserving peace, and advancing American influence.

---

[1] The White House, *National Security Strategy of the United States of* America. (Washington, DC, 2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.
[2] *Ibid.*, 35.
[3] Pentagon. *Information Operations.* Joint Publication 3-13 (Washington, DC: Pentagon, 20 November, 2014), x.
[4] The White House, *National Security Strategy* , 34.
[5] Stanford University, "Stanford Persuasive tech Lab," *Stanford* University, accessed January 2, 2018, https://captology.stanford.edu.

[6] Isaac, Mike and Daisuke Wakabayashi, "Russian Influence Reached 126 Million Through Facebook Alone," *The New York* Times, October 30, 2017, https://www.nytimes.com/2017/10/30/technology/facebook-google-russia.html.
[7] Giles, Keir. *Handbook of Russian Information* Warfare (Rome, Italy: NATO Defense College, 2016), 9.
[8] *Ibid.*, 77.
[9] Wortzel, Larry M. *The Chinese People's Liberation Army and Information* Warfare (Carlisle, PA: U.S. Army War College, Strategic Studies Institute, 2014), 3.
[10] *Ibid.*, 29-30.
[11] The White House, *National Security Strategy* , 10.
[12] *Ibid.*, 40.
[13] *Ibid.*, 26.
[14] *Ibid.*, 31-32.
[15] Pentagon. *Joint Intelligence.* Joint Publication 2-0 (Washington, DC: Pentagon, 22 October, 2013), B-7.
[16] Novak, Matt, "James Clapper Says That America Needs a New Propoganda Agency to Fight Russia," *Gizmodo*, January 5, 2017, https://gizmodo.com/james-clapper-says-that-america-needs-a-new-propaganda-1790801701.
[17] *Wikipedia*, accessed January 2, 2018, https://en.wikipedia.org/wiki/United_States_Information_Agency.
[18] Schoen, Fletcher and Christopher J. Lamb. *Deception, Disinformation, and Strategic Communication.* (Washington D.C.: Institue for National Strategic Studies, Strategic Perspectives, No. 11, 2012).
[19] U.S. Strategic Command, "U.S. Cyber Command," *U.S. Strategic Command*, September 30, 2016, http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/.
[20] U.S. Department of State, "Global Engagement Center," *U.S. Department of State*, last accessed January 2, 2018, https://www.state.gov/r/gec/.
[21] Bing, Chris, "Cyber Command head: We are not prepared to counter info operations," *cyberscoop*, May 9, 2017, https://www.cyberscoop.com/cyber-command-head-not-prepared-counter-info-operations/.
[22] Brooking, E. T., "Anonymous vs. The Islamic State," *Foreign Policy*, last accessed Januray 2, 2018, http://foreignpolicy.com/2015/11/13/anonymous-hackers-islamic-state-isis-chan-online-war/.

Bibliography

Giles, Keir. *Handbook of Russian Information Warfare.* Rome, Italy: NATO Defense College, 2016.

Pentagon. *Joint Intelligence.* Joint Publication 2-0. Washington, DC: Pentagon, 22 October, 2013.

Pentagon. *Information Operations.* Joint Publication 3-13. Washington, DC: Pentagon, 20 November, 2014.

Schoen, Fletcher and Christopher J. Lamb. *Deception, Disinformation, and Strategic Communication: How One Interagency Group Made a Difference.* Washington D.C.: Institue for National Strategic Studies, Strategic Perspectives, No. 11, 2012.

The White House. *The National Security Strategy of the United States of* America. Washington, DC, 2017. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

Wortzel, Larry M. *The Chinese People's Liberation Army and Information Warfare.* Carlisle, PA: U.S. Army War College, Strategic Studies Institute, 2014.