REPORT DOCUMENTATION PAGE

FORM APPROVED - - - OMB NO. 0704-0188

1. AGENCY USE ONLY (LEAVE BLANK)

2. REPORT DATE (DD-MM-YYYY)

07-04-2016

3. REPORT TYPE AND DATES COVERED

Master of Military Studies Sep 2015-Apr 2016

4. TITLE AND SUBTITLE

Tor: What It Is and How It Can Support DoD Information Operations

5. FUNDING NUMBERS

N/A

6. AUTHOR(S)

McPhee, Weston S, Major, USMC

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

USMC COMMAND AND STAFF COLLEGE
2076 SOUTH STREET, MCCDC, QUANTICO, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER

NONE

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

SAME AS #7.

10. SPONSORING/MONITORING AGENCY REPORT NUMBER:

NONE

11. SUPPLEMENTARY NOTES

NONE

12A. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release, distribution unlimited

12B. DISTRIBUTION CODE

N/A

ABSTRACT (MAXIMUM 200 WORDS)

Tor is an open source anonymizing application which operates on the physical infrastructure of the standard internet through the use of non-standard protocols. It functions by routing its traffic encased in multiple layers of encryption through a series of privately controlled nodes. The layered encryption provides the user complete anonymity—no outside observer can determine the source, destination, or content of the information traversing the network. Utilizing Tor, users can collaborate with others, browse the Internet, or access “hidden services” within the Tor network itself without compromising their identity. The anonymity provided by Tor makes it a popular tool for individuals who wish to hide their online activities, and is widely used by dissidents in repressive regimes and members of extremist organizations at odds with the United States. Because of this, Tor is an exceptional platform for intelligence-gathering, gaining effects through messaging to populations, and as a vector for the delivery of cyber weapons. Using Tor, the DoD can conduct real-time messaging and collaboration with dissident populations inside adversarial nations, more efficiently gather intelligence during Phase 0 (Shaping) and Phase 1 (Deterrence) operations, and effectively deliver cyber weapons which provide an asymmetric advantage to US forces.

14. SUBJECT TERMS (KEY WORDS ON WHICH TO PERFORM SEARCH)

The Dark Net; The Onion Router; Tor; Hidden Services; Information Operations; Cyber Warfare

15. NUMBER OF PAGES:
32

16. PRICE CODE: N/A

17. SECURITY CLASSIFICATION OF REPORT:

UNCLASSIFIED

18. SECURITY CLASSIFICATION OF THIS PAGE:

UNCLASSIFIED

19. SECURITY CLASSIFICATION OF ABSTRACT

UNCLASSIFIED

20. LIMITATION OF ABSTRACT

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE:

TOR: WHAT IT IS AND HOW IT CAN SUPPORT DOD INFORMATION OPERATIONS

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

AUTHOR: Major Weston S. McPhee

AY 15-16

Mentor and Oral Defense Committee Member: Gary D Brown
Approved: GARY D BROWN
Date: 6 Apr 16

Oral Defense Committee Member: MATTHEW FLYNN
Approved:
Date: 4/6/16

LtCol Edward S. Debish
4/6/16

J.W. Gordon
4/6/16

DISCLAIMER

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

QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

Executive Summary

Title: Tor: What It Is and How It Can Support DoD Information Operations

Author: Major Weston McPhee, United States Marine Corps

Thesis: The DoD needs to include Tor as a tool to facilitate the achievement of Information Operation objectives to maximize its effectiveness in the contemporary information environment.

Discussion: Tor is an open source anonymizing application which operates on the physical infrastructure of the standard internet through the use of non-standard protocols. It functions by routing its traffic encased in multiple layers of encryption through a series of privately controlled nodes. The layered encryption provides the user complete anonymity—no outside observer can determine the source, destination, or content of the information traversing the network. Utilizing Tor, users can collaborate with others, browse the Internet, or access "hidden services" within the Tor network itself without compromising their identity. The anonymity provided by Tor makes it a popular tool for individuals who wish to hide their online activities, and is widely used by dissidents in repressive regimes and members of extremist organizations at odds with the United States. Because of this, Tor is an exceptional platform for intelligence-gathering, gaining effects through messaging to populations, and as a vector for the delivery of cyber weapons.

Conclusion: Using Tor, the DoD can conduct real-time messaging and collaboration with dissident populations inside adversarial nations, more efficiently gather intelligence during Phase 0 (Shaping) and Phase 1 (Deterrence) operations, and effectively deliver cyber weapons which provide an asymmetric advantage to US forces. Ultimately, the use of Tor can provide the DoD with a greater means to shape emerging conflict areas and cultivate desired changes within them—potentially without having to use force.

Table of Contents

Page

DISCLAIMER i

EXECUTIVE SUMMARY ii

INTRODUCTION 1

REVIEW OF LITERATURE 3

INFORMATION OPERATIONS...5

INTERNET BASICS 7

TOR AND THE DARK NET 9

PUTTING IT TOGETHER: TOR'S USE IN INFORMATION OPERATIONS 13

Tor as a Messaging Platform 13

Tor as an Intelligence-Gathering Platform 17

Tor as a Vector for Cyber-Weapons...19

MANAGING TOR'S USE 24

CONCLUSION..26

ENDNOTES 27

BIBLIOGRAPHY 30

INTRODUCTION

When two geographically separated computers first communicated across a digital network in 1969, cyberspace was born. This new network, created by scientists from the Advanced Research Projects Agency (ARPA), developed into what is known today as the "Internet". It also became a new domain of warfare. As distributed computers became increasingly utilized to exchange and store sensitive information, they also became lucrative targets for adversaries to exploit. As technology advanced over the years, so too did the level of sophistication within cyber operations. As early as the late 1980s, the Soviet Union exploited vulnerabilities in the newly created internet to gain access to sensitive data repositories and exfiltrate secret US documents.[1] Today, new methods of exploitation have been created to gain access to sensitive information for intelligence-gathering purposes, code has been developed to commandeer an adversary's system without his knowledge, and cyber weapons capable of causing physical destruction have been created. Moreover, cyberspace has developed into an arena in which the human element is extensive; there are estimated to be over 3.2 billion internet users in the world today.[2] Because of this, cyberspace has become another realm in which human cognition—the key driver of behavior—can be influenced.

Within the sphere of cyberspace is the concept of the "dark net", a hidden network operating across the physical infrastructure used by the internet. The dark net is, in essence, a parallel electronic universe accessed through non-standard software and protocols which go undetected by those used to enable applications of the standard internet. Its operation is enabled primarily through the use of the protocol "Tor", which is an acronym for "The Onion Router". Tor functions by routing network traffic wrapped in multiple layers of encryption through a series of privately controlled nodes. This layering of encryption provides the user complete anonymity—

no outside observer can determine the source, destination, or content of the information. Utilizing Tor, users can anonymously collaborate with others, browse the Internet, or access "hidden services" within the Tor network itself.

Tor has recently been a subject of much trepidation within many agencies of the national defense apparatus, including the Department of Defense (DoD). This is primarily due to actions of individuals such as Bradley Manning and Edward Snowden who used Tor to anonymously leak reams of sensitive national security information. However; while Tor does provide a means for malicious insiders to secretly release sensitive information, it can also serve as a very beneficial tool for military information operations (IO). Through deeper examination, it becomes evident that Tor is an exceptional platform for gaining effects through messaging to populations, intelligence-gathering, and serves as an excellent vector for the delivery of cyber weapons. These enhanced capabilities facilitated by Tor could provide the DoD with a greater means to shape emerging conflict areas and cultivate desired changes within them—potentially without the use of force. Because of this, Tor should be embraced by the DoD and included as a tool to facilitate the achievement of its IO objectives.

Throughout the course of this paper, the applicable literature regarding Tor and cyber warfare will be reviewed, the concept of IO as it relates to Tor will be discussed, and the basic history and function of Tor will be examined. Finally, Tor's utility in DoD IO will be discussed in depth. This in-depth discussion will illustrate how Tor can serve as an advantageous platform for intelligence-gathering, messaging to populations, and as a vector for the delivery of cyber weapons.

REVIEW OF LITERATURE

At the time the topic of this paper was being researched there were very few published sources with a focus on Tor. Due to this, the literature review for this paper is done in three tiers. The first tier consists of three books focused on Tor and the concept of the dark net, the materials published on the TorProject, Inc. website, and scholarly papers written on Tor. The second tier consists of other works which are directly relevant to the topic, but not specifically focused on it. These works include books on cybersecurity, cyberwarfare, and the DoD doctrinal publication on IO. The third tier consists of items which provide ancillary supporting information such as statistics and historical examples.

Of but three books available on Tor, two are self-published works by the same author (Lance Henderson). Henderson's work *Tor and the Dark Art of Anonymity* provides a comprehensive understanding of what Tor is and how it functions. His work *Darknet: A Beginner's Guide to Staying Anonymous Online* describes Tor at a more basic level, but also serves as a "how-to" guide for using Tor. Both publications provide best practices for using Tor to maintain anonymity online, as well as highlight areas which can be exploited to compromise anonymity if not understood. The underlying thesis in both of these books is that the use of the open internet exposes users to possible identity exploitation in many forms and that the only way to protect against exploitation is to utilize an online anonymizing tool such as Tor.

The third book, *The Dark Net* by Jamie Bartlett, is published by a commercial publishing house and is a casual sociological/anthropological study of the sub-culture and content of Tor's dark net. The purpose of Bartlett's endeavor appears to be to better understand how online anonymity influences human behavior. In this book, Bartlett provides anecdotes of his first-hand observations and interactions with users of the dark net. While this work does not provide a technical understanding of the functioning of Tor or the dark net, it does provide a very good understanding of what content is resident within Tor “hidden services”, and it also underscores how effective the anonymity provided by Tor is.

The scholarly papers reviewed generally focus either on the technical aspects of Tor, or the criminal conduct it enables. The most relevant scholarly paper for the topic at hand is Richard B. Yetter’s Master’s Thesis entitled “Darknets, Cybercrime, & The Onion Router: Anonymity & Security in Cyberspace”. In it, Yetter argues that although Tor enables a significant amount of criminal activity, it is simply a tool for privacy and is no more a criminal platform than any other online application. In discussing this, he provides an excellent synopsis of Tor’s use in criminal activities and the challenges Tor creates for law enforcement and government agencies, especially regarding the implications of privacy rights with its use. Additionally, Yetter includes multiple Tor screenshots that illustrate the myriad of goods and services which can be accessed through Tor’s “hidden services”. This corroborates Bartlett’s accounts and further illuminates the effectiveness of Tor’s protection of anonymity.

The books reviewed regarding cybersecurity and cyberwarfare all essentially shared the view that the advent of computer networks has incredibly enhanced humanity’s ability to exchange information, but has also opened a new domain which can be exploited for various purposes due to its complexity and permeation into many facets of everyday life. Beyond the technical descriptions of the various methods of cyber exploitations and attacks which were contained in each work reviewed, Jeffrey Carr’s *Inside Cyber Warfare* was most applicable to the study at hand. Carr provided a comprehensive description of how individuals, organizations, and states utilize cyber operations to achieve political, informational, economic, and/or military advantages. Carr’s assessment went beyond the discussion of subjects like malware and distributed denial of service attacks which typically dominate cyberwarfare/cybersecurity conversations, and delved into the use of social media as a means to achieve a desired end. Furthermore, he examined a spectrum of actors from cyber criminals to hacktivists to state-sponsored actors to illustrate how they utilize cyberspace to achieve their desired effects.

Unfortunately, very few works specifically regarding Tor have been published, and no works are presently available which discuss in depth Tor's utility to the DoD through influencing dissident populations in repressive regimes, as a tool for intelligence gathering, or as a vector for the delivery of cyber weapons. This is the gap that this paper will attempt to fill, or at least lay the foundation for others to develop further.

INFORMATION OPERATIONS

To understand how Tor can aid the accomplishment of the DoD's IO objectives, one must first understand what the essence of IO in the modern digital era is. The convergence of computer technology and human factors in cyberspace has led to the awareness that cyberspace is not simply a network of interconnected machines, but instead an integral part of an "information environment" entailing three sub-dimensions: the physical which consists of the equipment and people who use it, the informational which is focused on how information is collected, stored, and disseminated, and the cognitive which is oriented on the mental and emotional aspects of the people who interact with the information.[3] This understanding of three information sub-domains has given rise to the concept of "information operations"—a line of operations in a military campaign which strives to integrate information-related capabilities with other lines of operations to gain an advantage over an adversary.[4]

The key aspect of IO is its focus on persuading or coercing a target audience (i.e. people) to behave in a way which achieves a desired effect or gives the presenter an advantage. The concept is not a new one. Methods of influencing the enemy's behavior through providing information and misinformation has been around since ancient times. In the 5th century BCE, Sun Tzu wrote, "All warfare is based on deception. Therefore, when capable, feign incapacity; when active, inactivity. When near, make it appear that you are far away; when far away, that you are near. Offer the enemy a bait to lure him; feign disorder and strike him."[5]

Today, the objective of IO is still to control the information the enemy is presented to influence his behavior. Although IO is people-centric—because it is people who are to be influenced—it is heavily reliant upon contemporary technology to accomplish its desired effects. Unlike in Sun Tzu's time, IO today incorporates cyberspace. This makes maneuver in the contemporary information environment much more complex than in previous epochs. Within this modern virtual-physical hybrid operating environment, the physical, informational, and cognitive subdomains converge. Modern military commanders rely heavily on digital systems to collect, view, and exchange information critical to their decision-making cycles, and their orders are often conveyed to subordinates across computer networks. These digital networks allow information to be relayed nearly instantaneously. This gives commanders unprecedented situational awareness of what is occurring in every area of the battlefield, and provides them a means to coordinate actions to influence it. However, corruption of digital data makes information unusable, interrupting or slowing the decision cycle. Inhibiting access to digital-borne information blinds decision-makers, precluding them from fully understanding a situation for what it is and preventing them from influencing action. And cyberspace allows adversaries to instantaneously influence one another through the delivery of targeted messages, such as with execution videos posted to online social media sites by the violent extremist organization (VEO) Daesh[6] to intimidate adversaries. It has become apparent that he who controls the information controls the situation. Following this model, Tor can serve as an integral tool to achieve desired IO effects.

INTERNET BASICS

To understand the functionality of Tor and the dark net, one must first have a fundamental understanding of internet protocol (IP) routing and how the internet works. In the late 1960s, ARPA computer scientists and mathematicians set about to create an extended distance network which was more efficient for computer-to-computer communications than the circuit-switched telephone communications network. To achieve this, they began improving upon the concept of the packet-switched network which was originally conceptualized in the mid-1960s by Paul Baran of the RAND Corporation and Donald Davies, a British computer scientist.[7] Unlike with circuit switching communications, a packet-switched network does not require a dedicated circuit between communicating devices. Instead, information is broken into small portions of data called packets. These packets are transmitted via paths which may be shared by multiple simultaneous communication sessions of other devices. Additionally, packets can be routed via multiple paths between the source and destination, increasing network efficiency.

However, without a dedicated circuit being established between communicating devices, a protocol is needed to ensure proper routing and sequencing of the packets. Within internet protocol (IP) routing, this is provided in the structure of the packet itself. Each IP packet consists of a payload and a header. The payload contains a small portion of the data which makes up the whole message being transmitted between end points. The header is the portion of the packet which contains all of the necessary “overhead” to allow the packet to be correctly routed and sequenced at the destination. Most notably, the header contains both a source IP address and a destination IP address.

Each IP address is unique to a device connected to the internet. It identifies the specific IP sub-network upon which the device resides, as well as its specific host position on the sub-network. When a user wants to connect their device to the internet, they must have a valid public IP address. Attempting to run a device with an invalid IP address will either result in an inability to connect to the internet, or cause connectivity to be intermittent and unreliable due to an IP conflict with another device on the network. This construct allows the packets to route through the network independent of a dedicated communication circuit being established directly between end devices.

Public IP addresses are globally managed by the Internet Assigned Numbers Authority (IANA). The IANA delegates assignment of IP addresses to five regional internet registries. These regional registries then allocate IP address to local-level internet service providers (ISPs) who, in turn, assign IP addresses to individual subscribers. Because of this, it is possible to trace a valid public IP address to the physical location it is being used. This can then be used to correlate the identity of the specific user.

Furthermore, when a user browses the internet, their device’s web browser—a software application which allows viewing and interacting with web sites (e.g. Internet Explorer or FireFox)—shares data with the web server from which content is being browsed. This data includes information such as the user’s public IP address. Additionally, many computer programs run various applications in the background that send information to parent servers via the internet connection. This information may be diagnostic data such as current software version and last update, or feedback on a program's use to allow targeted advertisement of additional functionalities. For example, Adobe is a program which provides a parent server information about the user's habits.[8] Whatever the case, these applications are sharing unique identification characteristics of the user's device—namely its public IP address—which can allow the user's online actions to be tracked and their location to be determined.

Moreover, standard packets traversing the internet can be intercepted en-route, allowing their source and destination IP addresses to be revealed. If unencrypted, the contents of the payload can also be determined, allowing electronic eavesdroppers to discern the nature of the user's communications. For anyone wanting to remain anonymous, this system of information exchange creates an unacceptable electronic fingerprint of their activities and online presence. What Tor offers these users is complete online anonymity through ensuring that the true public source and destination IP addresses are concealed, and that the contents of the payload are undecipherable to electronic eavesdroppers.

TOR AND THE DARK NET

The Tor concept was developed in 1995 by the US Naval Research Laboratory.[9] The purpose of the project was to find an affordable way to protect the transmission of US intelligence communications using the public internet infrastructure.[10] In 1997, DARPA became involved with the project and developed it into a usable application.[11] Then, in 2004, the US Government released Tor for world-wide use under a free license. It is speculated that this was intended to generate sufficient nodes and user traffic to dilute intelligence traffic.[12] Tor is now available for free download from a number of sites and organizations, most notably The Tor Project, Inc., which is a nonprofit organization that currently maintains Tor's coding.

Tor is essentially an "overlay network" which utilizes the internet's physical topography, but provides its own virtual structure.[13] It provides anonymity primarily through concealing the user's true public IP address. To do this, Tor relies on volunteers to offer their devices as relays on the Tor network. There are currently over 7,000 active Tor relays worldwide.[14] Each time a user goes online with Tor, their device is assigned a new, random Tor IP address.[15] When the user sends data via Tor, their device assesses the active Tor relays available and determines a random path to the destination via a random number of these relays. The user's device then encapsulates each packet with one layer of encryption for each hop between relays to the final destination in the Tor network. As the packet traverses the Tor network, one layer of encryption is stripped away at each relay along the path. At the final relay, the last layer of encryption is removed and the packet is routed to its intended destination. The layering of encryption in this manner is analogous to the layers of an onion and is why Tor was originally called "The Onion Router".

Since the packet is wrapped in multiple layers of encryption that conceal the original source and destination IP addresses, no intermediate device in the network can determine the source or destination of the packet more than one hop back or one hop forward. Hence, if a packet is intercepted and examined, the identity of the user remains anonymous, and the contents of their packet's payload remains undecipherable due to the layered encryption. For an outsider to trace a packet back to a source would require that they monitor nearly all Tor traffic simultaneously because of the random routing of packets through the Tor network; a feature which further anonymizes the user.

Through the use of exit nodes, Tor users are able to anonymously browse the standard public internet. Exit nodes are volunteers' relays which connect the Tor network with the standard public internet. The exit node serves as the last relay in the Tor network and routes the user's packets into the public internet.[16] Due to the randomness of Tor routing, the exit node utilized is unlikely to be located near a user's physical location. For instance, a Tor user in the United States may utilize an exit node in Australia to view internet web sites during one session, but during the next session, an exit node in Switzerland may be utilized. This further serves to protect the user's anonymity.

Shortly after Tor was released to the general public for use under a free license, its use began to morph into something more than just anonymous routing of IP traffic; "hidden services" began to be established within the Tor network. Hidden services, also commonly referred to as "onion sites", are services provided on servers which reside within the virtual bounds of the Tor network. These servers utilize Tor-assigned IP addresses and are configured to accept inbound traffic only from the Tor network. This conceals each server's network location—and thus its physical location, as well. Since these servers can only be accessed through the Tor network, they are invisible to devices operating on the standard internet.[17] They function by acting as sites within a pseudo-top level domain with the suffix ".onion". Since .onion is not a valid domain name system (DNS) root, servers established within Tor are configured to act as DNS servers and translate .onion addresses to the appropriate Tor IP address so that they can be accessed more easily. Collectively, these hidden servers make up what is often referred to as the "dark net".

Servers on the dark net provide anonymous use of services such as chat rooms, email, and file sharing. However, the Tor-enabled dark net is also ripe with sites that facilitate illegal activities such as the sale of drugs, child pornography, and fraudulently acquired bank account information. One site, known as “The Assassination Market”, even facilitates murder-for-hire.[18] These illicit sites exist for two reasons: first, there is a demand for the services they provide, and second—and more important—it is nearly impossible to track down the servers’ locations to shut them down and arrest the administrators running them due to the anonymity provided by Tor. The scale of such nefarious activity occurring so blatantly is a true testament to the protection provided by the use Tor.

The anonymity provided by Tor appeals to many groups of people, not just those purely criminal in nature. Among them are whistle-blowers, journalists, law enforcement officials, and activists. For whistle-blowers, the anonymity provided by Tor conceals their identity and helps protect them from reprisals by the highlighted party. For journalists, Tor allows anonymous communication with sources regarding sensitive subjects they are researching, allowing them to receive leads that they otherwise would not have. Journalists residing in repressive regimes also use Tor to publish stories with media organizations outside of state control.[19] Law enforcement officials use Tor to investigate internet crimes and search suspicious online content without exposing an IP address linked to their department’s official network, thus protecting their investigations from compromise. Finally, activists use Tor to anonymously express their views and further calls for social change. Tor’s anonymity is especially appealing to activists whose speech is illegal, such as those who are members of VEOs plotting terror attacks or those who reside in oppressive regimes which outlaw dissention against the government. These are the individuals that the DoD can most effectively influence using Tor.

PUTTING IT TOGETHER: TOR'S USES IN INFORMATION OPERATIONS

Tor is applicable to DoD IO in three distinct ways: as a medium for messaging to dissidents residing in adversary nations, as an intelligence-gathering platform, and as a vector for the delivery of cyber weapons. Each application of Tor's use is able to facilitate unique effects through targeting various aspects of the three IO sub-domains (physical, informational, and cognitive). When employed with other aspects of IO and military actions, the effects are synergistic and create a substantial advantage for US forces.

Tor as a Messaging Platform

Many of the countries that the United States identifies as potential adversaries are those with authoritarian governments that suppress basic civil liberties. Among the liberties often suppressed is unregulated access to information. Examples of such repressive countries include North Korea, Iran, and China. For these regimes, controlling information serves as a method of population control. The regimes of countries such as these have specific narratives that they want their populations to adopt and believe as true. To ensure the desired narrative is internalized by the people, the government permits access only to state-approved information which reinforces the desired narrative. Repressive regimes often enact laws to ban the voicing of dissenting opinions, outlaw private meetings to debate politics, and prohibit the importation of foreign media such as news publications, books, and movies. In the era prior to the proliferation of the internet, the prohibition of foreign information was accomplished largely through physical means; no unapproved foreign publications were allowed through the customs process. The only way for the illegal information to be introduced was through physically smuggling it in.

However, being discovered with contraband information items such as a foreign newspaper or book often results in severe penalties. For example, in North Korea, all DVDs and

CDs must have a stamp of approval by the government[20]. The punishment for possession or distribution of contraband information items ranges from five years in a “labour re-education centre” for minor offenses to execution for offenses deemed serious due to “decadent, carnal or foul contents” within the media.[21] Having to covertly transport and conceal relatively conspicuous items such as these, at the risk of harsh punishments, likely dissuaded many from becoming involved and accomplished the regime’s censorship goals.

In an attempt to circumvent the physical impediments emplaced by repressive regimes, outside organizations eager to break information blockades and counter adversaries’ narratives began using radio broadcasts. For example, during the Cold War the United States utilized “Radio Free Europe”, a collection of shortwave radio stations which broadcast western news stories, to influence the populations in Soviet-controlled Eastern Europe. As a counter, the Soviets attempted to jam Radio Free Europe frequencies[22] and enacted laws requiring components facilitating reception of the frequency band used by Radio Free Europe be removed from radios[23]. While these counteractions did not exterminate the effectiveness of Radio Free Europe, they did serve to degrade it.

While the effectiveness of smuggling items containing information and the broadcasting of outside perspectives over the radio waves can be debated, it cannot be contested that these methods lacked a key component necessary to mobilize a population toward action; they did not provide a venue for collaboration amongst dissidents who were in receipt of outside information or a method for outsiders to collaborate directly with the dissidents themselves. With the advent of personal computers and the internet, it became possible for dissidents to not only receive uncensored outside information, but to hold secret virtual discussions about it through the use of chat rooms and instant messaging. However, repressive regimes quickly enacted measures to block unapproved access to outside information. With internet traffic, this control is accomplished virtually vice physically, and is primarily done through filtering traffic at a firewall along the country's virtual border. This functions the same way as with a corporation that blocks access to Facebook to decrease workplace distractions and increase employee productivity. The Chinese government's firewall is so effective at blocking unapproved outside content that it is often jestingly referred to as "The Great Firewall of China," a pun referring to the nation's enormous physical barrier constructed centuries ago to keep the Mongols out.

However, Tor's design allows residents of repressive regimes to traverse the firewall restrictions implemented by their governments. Then, using Tor exit nodes located outside of the repressive regime, they are able to access uncensored information on the internet. Unlike packets using standard internet protocols, the content of Tor packets is safe from observation. The multiple-layered encryption obscures the source and destination IP addresses, protecting both the anonymity of the dissident user, as well as what web site(s) is being accessed. Tor's layered encryption also ensures that the contents of the packet cannot be discerned by state-sponsored network eavesdroppers. This protects the dissidents and keeps them safe from state reprisal.

Attaining access to uncensored information from sources outside of the repressive regime builds awareness in people that they are indeed oppressed, and may awaken a sense of grievance within them. If this sense of grievance is substantial enough, it may motivate them to action against their repressors. In support of the DoD's IO goals, Tor offers a means to influence the cognitive domain of individuals in these repressed populations, and guide dissident action to a much greater degree than the smuggling of foreign media or broadcasting of radio messages ever could. This is because Tor can facilitate real-time interaction with individuals living inside repressive regimes. This is a critical capability which can enhance Phase 0 (Shaping) operations.

Utilizing Tor as a platform for instant messaging or chat, military information support operations (MISO) specialists such can deliver custom-designed messages to specific dissidents or groups. These messages can be used to develop members of target audiences as sources of intelligence, provide them with the desire to rally other dissidents to action, and/or to guide them in achieving specific effects within their country. These effects could be physical, such the destruction of infrastructure critical to the regime, or social, such as organizing demonstrations and protests at a time and place of the DoD's choosing. Feedback regarding the effectiveness of these messages on targeted individuals can be assessed almost immediately withthe real-time connectivity enabled through Tor. And again, the correspondence is hidden from prying eyes on the network because of Tor's layered encryption. Utilizing Tor in this manner can allow the DoD to "shape the battlespace" prior to a bomb being dropped or a troop setting foot on the ground. Essentially, this would foster a desired change in a developing conflict area without the use of force.

Repressive regimes are aware of the danger that Tor poses to their ability to conduct population control. Given that the nature of IO is not one sided, but rather involves counteraction by the adversary, these repressive regimes allocate a great deal of resources in attempting to prevent Tor traffic from travelling in and out of their countries. However, each time a method is developed to reduce the effectiveness of Tor, Tor programmers counter it. For instance, China recently determined a way to block a substantial portion of Tor traffic based on the Transmission Control Protocol used in its routing methodology. In response, Tor Project, Inc. released an update which allowed Tor traffic to piggyback on User Datagram Protocol (UDP) applications.[24] These UDP applications are typically associated with real-time voice and video services such as Skype. Essentially, this creates a situation where the only way to fully block Tor users from accessing content on the internet is to cut off all internet connectivity traversing the country's virtual boundary.

However, this is not feasible—even for repressive, isolationist regimes. Even those regimes need to maintain some level of performance-based legitimacy with their populations to preserve authority. Their performance-based legitimacy is often predicated on the ability to conduct commerce with parties outside of the country to obtain necessary commodities such as shipments of food and oil. In the digital age, this requires transnational network connectivity to conduct efficiently. Severing this connectivity would indeed prevent Tor users from accessing external information and interacting with outsiders, but it would also hinder the regime's ability to conduct commerce to provide many basic needs for its people. This, in turn, would severely erode the performance-based legitimacy of the government—likely putting it in a precarious position with the people. Hence, to these regimes, the less immediate threat is to allow at least some level of connectivity to the outside world. Because of this, it is almost certain that Tor will provide DoD officials with a continuous asymmetric advantage through real-time access to dissidents within repressive adversary nations.

Tor as an Intelligence-Gathering Platform

With respect to the informational sub-domain of IO, having the ability to garner real-time information from within an adversary nation's borders provides a substantial advantage. In this regard, the same characteristics that make Tor an excellent messaging platform also make it an excellent intelligence-gathering platform. Utilizing Tor, intelligence officers can not only message to dissidents, they can also receive valuable feedback directly from them as well. This feedback may be in the form of sensitive government information which is immediately of great value (such as classified documents), or something more benign which can be aggregated and analyzed with other information to form an accurate intelligence assessment (such as pieces of information which provide the indication of an imminent mechanized operation in a particular area).

Furthermore, Tor can be used by covertly-inserted reconnaissance elements during Phase 0 (Shaping) and Phase 1 (Deterrence) operations to provide intelligence reports back to their headquarters. Instead of utilizing conspicuous, sensitive communications equipment to provide encrypted satellite or radio communications which can easily be jammed or traced to an origin through radio direction finding, the reconnaissance element can simply utilize an inexpensive laptop (or other mobile electronic device) to communicate via Tor from any accessible network. Options include an unsecure Wi-Fi network, a hotel network, or even a local internet café. In this respect, the reconnaissance element would essentially be delivering intelligence information in plain sight, yet undetected. If the reconnaissance operation becomes compromised, the laptop or mobile device being utilized could be discarded, wiped, or physically destroyed; there is no sophisticated government communications equipment, cryptographic fill devices, or classified encryption keys present which may fall into an adversary's hands for exploitation.

Additionally, Tor can facilitate intelligence-gathering through allowing intelligence personnel to monitor chat rooms hosted on .onion sites. These sites are often utilized by VEOs such as Daesh.[25] Through monitoring the conversations in these Tor hidden service discussions, DoD intelligence officials can gather critical insight into the composition, disposition, capabilities, intentions, and potential weaknesses of the organizations they are surveilling. Moreover, through incognito participation in the discussion boards used by such organizations, DoD intelligence and MISO officials may be able to manipulate participants into providing various pieces of information which seem benign, but can be correlated to expose their true identities, thus stripping them of anonymity provided by Tor and allowing them to be targeted outside the virtual world.

Tor also has utility as an intelligence-gathering platform within counterinsurgency (COIN) operations. Within COIN operations, information offered by informants can provide a critical advantage to the counterinsurgency force. However, in an environment where insurgents utilize brutal intimidation tactics such as torture, mutilation, and murder to discourage cooperation of the civilian populace with counterinsurgency forces, many civilians are reluctant to come forward with information. Providing a method with the assurance of complete anonymity may be the only way to motivate many members of the civilian populace who desire to provide information but are paralyzed by fear. Utilizing Tor, intelligence officers could establish anonymous tip lines to solicit local informants' comments. Using Tor in this manner is a technique being used successfully by many law enforcement agencies, and provides proof of the method's validity.[26]

Tor as a Vector for Cyber-Weapons

On the modern battlefield, advanced militaries and unsophisticated adversaries alike have become increasingly dependent upon computer technology to function efficiently and effectively. Computer-enabled technologies have permeated command and control (C2) systems, surveillance and reconnaissance platforms, integrated air defense systems (IADS), logistics techniques, and even basic information exchange methods. Because of the proliferation of computer-enabled network technologies within military applications, and the subsequent dependency upon them, a critical facet of IO capabilities is the ability to conduct cyber-attacks on an adversary to exploit, destroy, degrade, or deny the use of his systems. To achieve these desired effects, various "cyber-weapons" have been developed. These cyber-weapons range from a basic key logger application to a "rootkit"[27] to very complex programs like the Stuxnet worm which can cause physical destruction to infrastructure. However, no matter how simple or complex the type of cyber-weapon to be employed, each requires a delivery method to reach its intended target. In this regard, Tor provides utility as a vector for cyber-weapons.

Perhaps most vulnerable to attack through the use of Tor as a vector are non-state sponsored VEOs. This is because these organizations typically do not possess the resources to acquire and employ technologically advanced reconnaissance capabilities. Instead, they rely heavily on unsophisticated intelligence-gathering methods such as open-source information. In this vein, a VEO developing a plan to conduct an attack will likely look to the internet to acquire intelligence information on possible targets. As they settle on a specific target, they will have the need to gain sufficient detail of the target to plan a successful attack. Some specific items required to refine their plans—such as imagery inside a secure location or building design blueprints—may not be available on the public internet due to their sensitive nature. This will require the VEO to employ other capabilities to obtain the necessary information. Given their anonymity, the use of Tor chat rooms and hidden services are attractive resources and a logical next-step for fulfilling these outstanding requirements. This can be exploited by DoD not only to uncover plans for impending attacks, but also to employ cyber-weapons against the VEO planning the attack.

Through anonymously monitoring Tor chat rooms frequently utilized by VEOs, DoD intelligence officials can ascertain what the potential targets are, and what information the malicious organization still requires to complete their intelligence preparation. Through the use of Tor hidden services, the required items can be "marketed" to the VEO planners. Unbeknownst to them, the file they purchase would contain embedded malware hidden through the process of electronic steganography.[28] The code concealed within the file would in fact be a cyber-weapon chosen to achieve a desired effect.

As an illustration of the potential effectiveness of this methodology, take a VEO such as Daesh that is eager to conduct an attack on a US military base in Turkey. While Daesh is able to ascertain much information about their target from open-sources, such as satellite imagery from Google Earth, they are missing key information regarding the interior design of the command post building. After exhausting resources available on the open internet, they begin scouring Tor hidden services and reaching out on Tor chat rooms for contacts who can supply the needed information. They are directed to a hidden service site (by an incognito DoD official) where they purchase blueprints for the building from an individual identified as a former engineer from the construction project who is looking to make a quick $5,000. Unaware that the file contains a remote access tool (RAT) concealed within it, they download the file. The embedded malware, similar to the "gh0st RAT" program developed by the Chinese, infects each machine the file is loaded to and allows the DoD to remotely operate the microphone and web camera, log keystrokes, exfiltrate files on the hard drive, and activate the Wi-Fi.[29]

Using these capabilities, DoD intelligence officials would be able to map the human network of the planning cell, eavesdrop on conversations through their devices' microphones, photograph members of the planning cell with their own web cameras, and ascertain exact locations of each individual through the geotagging[30] information embedded in the web camera photographs. Knowing what the key personnel look like and where they are located could then allow a capture operation to be conducted effectively. Finally, if it is desired that a key member of the cell be eliminated, activating that individual's Wi-Fi could serve as a guidance method for a precision-guided weapon adapted to track the discrete Wi-Fi signal, allowing the VEO member to be targeted in the physical world with a kinetic weapon. The possibilities are practically endless, and can be facilitated through using Tor as a delivery vehicle for cyber-weapons.

Sophisticated militaries with advanced network security strategies are also vulnerable to cyber weapons delivered through the use of Tor. Since modern militaries have become reliant upon digital technology to maintain command and control, tempo, and effectiveness, undermining their digital abilities can give the DoD a tremendous advantage in all phases of a military operation. Using Tor, the DoD can deliver cyber weapons which allow US military forces to disable an adversary's IADS prior to conducting an air strike, degrade C2 capabilities, or disrupt logistics processes.

To protect against this, many contemporary militaries utilize commercial anti-virus, employ "air gaps"[31], and conduct user verification for network access. However, these tactics are not sufficient. First, even the most sophisticated anti-virus cannot detect a zero day exploit. This is because anti-virus programs are signature-based, which means that they are designed to look for specific digital signatures that belong to *known* malware programs. A zero day exploit is a malware program which has either never been employed, or has been previously employed but has not yet been discovered.[32] As such, a custom-crafted exploit renders the anti-virus software useless and facilitates the achievement of desired effects on a specific target.

Second, air gaps have been proven ineffective against preventing malware from infecting isolated sensitive networks. The National Cybersecurity and Communications Integration Center (NCCIC) recently conducted hundreds of vulnerability assessments on US businesses which employ air gaps to safeguard sensitive information and found that not a single one successfully isolated the sensitive network from the business' other enterprise networks.[33] For proof of this same vulnerability existing with sensitive military or government networks, there are two excellent examples: Agent.btz and Stuxnet. In the case of Agent.btz, exfiltration malware infected US military classified networks in 2008 through the use of an unauthorized thumb drive[34]. The Stuxnet worm, discovered in 2010, was introduced into one of Iran's isolated uranium centrifuge control networks by a scientist's thumb drive and caused substantial physical damage to nearly 1,000 centrifuges.[35]

In both the Agent.btz and Stuxnet scenarios, malicious code was introduced to the air-gapped network by a trusted user with legitimate access. Thus, the greatest threat to a network is an insider—even an insider who does not desire to do harm but is simply complacent or negligent. Because of this, a critical component to delivering cyber-weapons to an air-gapped network is through exploiting the human element. This is where Tor can once again lend utility. Through various methods, intelligence and MISO professionals can profile which adversary personnel with access to their military's sensitive network likely utilize Tor, and for what purpose. The types of content that these individuals view and download using Tor could then be contaminated with a cyber-weapon.

After infecting their device, the NCCIC study shows that it is only a matter of time before the code is migrated over to the sensitive network. Like the Stuxnet worm, once inside, the cyber-weapon would seek out its target system undetected. The cyber weapon, delivered using Tor, could attack any or all of the three IO sub-domains. It could create physical destruction to hardware, it could corrupt digital information repositories to slow decision-making cycles, or it could provide the adversary false information to gain a cognitive advantage and affect their actions and behaviors.

MANAGING TOR'S USE

At this point, it is clear that Tor is an excellent tool that the DoD should include in its IO toolbox. However, due to its ability to affect all three IO sub-domains in substantial ways, Tor must be used in a manner in which it does not adversely affect other ongoing campaigns. Since military action is not the only instrument of national power, it must be kept in mind that other national-level IO campaigns may be occurring where the DoD desires to employ Tor. For this reason, it is essential that Tor's use be centralized and controlled to ensure that its employment compliments the activities of those other IO campaigns.

Given that Tor is a hybrid instrument which can facilitate offensive cyber operations as well as serve as a MISO platform requires that a determination be made as to where the responsibility for its management should reside within the DoD. In determining where Tor's management should be assigned, two critical factors need to be addressed. The first is the requirement for unity of effort with regard to national-level strategic IO campaigns to ensure cyber operations are appropriately coordinated, and that there is consistent US government messaging. The second critical factor is the requirement for responsiveness in the employment of Tor to support military operations, especially those of a time-sensitive nature.

Since Tor is a cyber application, the first instinct may be to assign its responsibility to US Cyber Command (Cybercom), a sub-unified command under US Strategic Command. This would seem logical since *Joint Publication 3-12* (Cyberspace Operations) identifies US Strategic Command as the command overall responsible for conducting full-spectrum military cyber operations.[36] However, this is not the wisest method to control Tor's use effectively.

Maintaining approval authority for the use of Tor at the US Stratcom or Cybercom level would indeed ensure that its use is tightly controlled and integrated within the greater IO campaign, but it would also likely add too many layers to the approval chain and slow responsiveness. *Joint Publication 3-12* attempts to address issues like this by requiring US Stratcom to provide supported Geographic Combatant Commands (GCC) with Cyber Support Elements (CSE) to be integrated within the GCC's planning staffs to assist in cyber operations planning and synchronization.[37] However, in this construct, US Stratcom retains operational control of the CSEs, and Stratcom (via Cybercom) is still the approving authority for the employment of cyber operations (which would include the use of Tor). This does nothing to solve the problem of unnecessary layers in the approval chain, and only serves to slow the responsiveness of employing Tor in support of military operations. The result would likely be Tor not being considered for use in many time-sensitive cases where it would otherwise provide desired results.

Conversely, assigning the responsibility for managing and approving Tor's use at a much lower level—such as a regiment or battalion—would certainly increase operational responsiveness, but it would also increase the likelihood that Tor's employment would not sufficiently complement the larger, strategic IO campaign. This could result in inconsistent messaging between US military units within the same theater of operations, as well as between the DoD at large and various other US government agencies. A disparity of this nature could result in significant negative consequences to US strategic IO objectives and undermine previous successful efforts made to achieve them.

The best solution is to assign the responsibility for the approval and management of Tor's use directly to the six geographic combatant commands. From the messaging standpoint, the GCC is already responsible for integrating and coordinating strategic messaging through the use of MISO.[38] From the cyber operations standpoint, a structure similar to the CSE—capable of coordinating and synchronizing efforts with US Cybercom/Stratcom—could be permanently established within each GCC staff. However, unlike the CSE, the geographic Combatant Commander would retain operational control of it, and would be able to assign it to support subordinate Joint Task Forces if required. This would eliminate multiple unnecessary layers in the approval chain while still allowing reach-back to US Stratcom and synchronization with other strategic cyber operations.

Managing Tor's employment in this way would allow a balance between the need for responsiveness and the potential risk to the greater, strategic IO campaign. This is because the Combatant Commander and his/her staff work closely with the ambassador and Department of State country teams for each nation within the command's geographic area of responsibility. These civil-military relationships help to ensure that the staff of each GCC has greater awareness of the strategic IO campaign for their specific regions than would the staff of US Strategic Command or US Cyber Command who is supporting operations around the world. This translates into the ability of the GCC staff to discern the regional consequences of Tor's use more rapidly, and would facilitate a faster approval process for Tor requests. Ultimately, this would allow the most effective and efficient use of the capabilities that Tor provides and would maximize its usefulness with the least amount of risk to other IO campaigns.

CONCLUSION

Computer-enabled network technologies have permeated human society and led to a reliance on cyberspace in everyday life. Individuals and groups around the world now rely on the internet to acquire information and communicate with one another. Modern militaries and militant organizations alike have also become dependent upon computer-enabled network technologies to collect, view, store, and exchange information critical to their operations. Due to this hybrid virtual/physical information environment which has arisen, information operations are now more reliant than ever upon computer technology to achieve desired effects. The information environment facilitated through the use of computer networks is available to all who connect, and as such, gives an asymmetric advantage only to those who exploit its capabilities to the maximum extent possible. Because of this, the DoD must find ways to leverage cyber technology to maintain an advantage over potential adversaries.

In this context, it is clear that Tor provides a means for the DoD to capitalize on a tremendous opportunity in the contemporary information environment because it provides multiple methods to exploit aspects of the informational, cognitive, and physical sub-domains of IO. Tor is an exceptional platform for intelligence gathering during Phase 0 and Phase 1 operations where it can facilitate real-time information updates from individuals present on the ground, it can facilitate effects through providing a means to collaborate with dissident elements within repressive adversary nations, and it is an excellent vector for the delivery of cyber-weapons. Ultimately, the use of Tor can provide the DoD with a greater means to shape emerging conflict areas and cultivate desired changes within them—potentially without having to use force. However, failing to exploit its capabilities cedes an asymmetric advantage to adversaries of the United States. The DoD would be remiss if it did not employ Tor to achieve its IO objectives.

NOTES

[1] Steve Winterville and Jason Andress, *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice* (Boston MA: Elsevier, 2013), 1.

[2] "Internet Users," *Internet Live Stats*, accessed January, 18 2016 http://www.internetlivestats.com/internet-users/.

[3] Joint Chiefs of Staff. *Information Operations*. Joint Publication 3-13 (Washington DC, November 20, 2014) I-2—I-3.

[4] Joint Chiefs of Staff. *Information Operations*. ix.

[5] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press, 1963), 66.

[6] "Daesh" refers to the so-called "Islamic State of Iraq and the Levant". It is an acronym for the Arabic phrase al-Dawla al-Islamiya al-Iraq al-Sham which means Islamic State of Iraq and the Levant, but the acronym's pronunciation is similar to the Arabic word "Daes" which translates to "one who sows discord". To refer to them as the "Islamic State" would give credibility to their organization.

[7] Dr. Lawrence G. Roberts, "The Evolution of Packet Switching." http://www.packet.cc/files/ev-packet-sw.html (November 1978). Accessed December 30, 2015.

[8] Lance Henderson, *Darknet: A Beginner's guide to Staying Anonymous Online* (Middleton DE: Amazon Books, 2012), Ch 2. (Note: This book does not contain page numbers)

[9] Joseph Babatunde Fagoyinbo, *The Armed Forces: Instrument of Peace, Strength, Development and Prosperity* (Bloomington IN: Author House, 2013), 262.

[10] David Leigh and Luke Harding, *Wikileaks: Inside Julian Assange's War on Secrecy* (New York: Public Affairs, 2011), 76.

[11] Fagoyinbo, *The Armed Forces: Instrument of Peace, Strength, Development and Prosperity*, 262.

[12] "Almost Everyone Involved In Developing Tor Was (or Is) Funded By the US Government," *Pando,* July 16, 2014. Yasha Levine, retrieved December 31, 2015. https://pando.com/2014/07/16/tor-spooks/.

[13] P.W. Singer and Allen Friedman, *Cybersecurity and Cyberwar: What Everyone Needs To Know* (New York: Oxford University Press, 2014), 109.

[14] "Tor Network Status," Joseph B. Kowalski, retrieved December 31, 2015. http://torstatus.blutmagie.de/.

[15] Henderson, *Darknet: A Beginner's guide to Staying Anonymous Online*, Ch 2.

[16] Since the exit node is the last Tor relay, it removes the final layer of encryption from the user's packets. Unless safeguarded by the user's device with an end-to-end encryption (such as a 256 bit Advanced Encryption Standard) prior to receiving its layered Tor encryption, the packet's contents may be read if intercepted, possibly compromising the user's anonymity.

[17] Henderson, *Darknet: A Beginner's guide to Staying Anonymous Online*, Ch 3

[18] Jamie Bartlett, *The Dark Net: Inside the Digital Underworld* (Brooklyn NY: Melville House, 2014), 3-4.

[19] The Tor Project, Inc., retrieved December 30, 2015. http://www.torproject.org.

[20] United Nations Human Rights Council, *Report of the Detailed Findings of the Commission on Human Rights in the Democratic People's Republic of North Korea-A/HRC/25/CRP.1* (New York: United Nations Human Rights Council, February 7, 2014), 59.

[21] United Nations Human Rights Council, *Report of the Detailed Findings of the Commission on Human Rights in the Democratic People's Republic of North Korea-A/HRC/25/CRP.1*, 59-60.

[22] Arch Puddington, *Broadcasting Freedom: The Cold War Triumph of Radio Free Europe and Radio Liberty* (Lexington KY: University Press of Kentucky, 2003), 214.

[23] Simo Mikkonen. "Stealing the Monopoly of Knowledge?: Soviet Reactions to US Cold War Broadcasting." *Kritika: Explorations in Russian and Eurasian History* vol 11, issue 4 (November 2010): 781.

[24] The Tor Project, Inc., retrieved December 30, 2015. http://www.torproject.org

[25] Barbara Starr and Jamie Crawford, "Pentagon Hunts For ISIS on the Secret Internet," *CNN.com,* May 12, 2015, http://cnn.com/2015/05/12/politics/pentagon-isis-dark-web-google-internet.

[26] The Tor Project, Inc., retrieved December 30, 2015. http://www.torproject.org.

[27] A Rootkit is a program which takes control of an operating system and gives full access to the attacker while hiding its presence and operation from the system's owner.

[28] Steganography is derived from the Greek words meaning "concealed" and "writing". Electronic steganography is the process of concealing electronic code such as a file, message, image, or video within another electronic file.

[29] Jeffrey Carr, *Inside Cyber Warfare*, 2nd ed. (Sebastopol CA: O'Reilly, 2012), 146.

[30] Geotagging is the process of adding geographical identification metadata to electronic media such as a photograph or video recording.

[31] An "air gap" is a method to increase cybersecurity through ensuring a physical separation exists between a classified or sensitive network and an unclassified network which interfaces with the public internet.

[32] Carr, *Inside Cyber Warfare*, 151-152.

[33] P.W. Singer and Allen Friedman, *Cybersecurity and Cyberwar: What Everyone Needs To Know*, 63-64.

[34] P.W. Singer and Allen Friedman, *Cybersecurity and Cyberwar: What Everyone Needs To Know*, 64.

[35] P.W. Singer and Allen Friedman, *Cybersecurity and Cyberwar: What Everyone Needs To Know*, 116-117.

[36] Joint Chiefs of Staff. *Cyberspace Operations*. Joint Publication 3-12 (Washington DC, February 5, 2013) III-6.

[37] Joint Chiefs of Staff. *Cyberspace Operations*. III-6.

[38] Joint Chiefs of Staff. *Information Operations*. III-2.

BIBLIOGRAPHY

Andress, Jason, and Steve Winterfield. *Cyber Warfare: Techniques, Tactics, and Tools for Security Practitioners*. New York: Elsevier, 2011.

Andress, Jason, and Steve Winterfield. *The Basics of Cyber Warfare: Understanding the Fundamentals in Theory and Practice.* Boston, MA: Elsevier, 2013.

Bartlett, Jamie. *The Dark Net: Inside the Digital Underworld.* Brooklyn, NY: Melville House, 2014.

Carr, Jeffrey. *Cyber Warfare: Mapping the Cyber Underworld*. 2nd ed. Sebastopol CA: O'Reilly Media, 2012.

Carr, Jeffrey. *Inside Cyber Warfare,* 2nd ed. Sebastopol CA: O'Reilly, 2012.

Chertoff, Michael, and Tobby Simon. *The Impact of the Dark Web on Internet Governance and Cyber Security.* Paper Series no. 6. Global Commission on Internet Governance. London: Chatham House, February, 2015.

Darnton, Geoffrey. *Cyberwar, Netwar, and the Revolution in Military Affairs.* Edited by Edward Halpin, Philippa Trevorrow, David Webb, and Steve Wright. New York: Palgrave MacMillan, 2006. https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf.

Dingledine, Roger, Nick Matthewson, and Paul Syverson. "Tor: The Second-Generation Onion Router." US Naval Research Laboratory Report, 2004. http://www.dtic.mil/get-tr-doc/pdf?Location=U2&doc=GetTRDoc.pdf&AD=ADA465464.

Executive Order 12333 of December 4, 1981, United States Intelligence Activities. Code of Federal Regulations, title 3 (1981): 46 FR 59941. http://www.archives.gov/federal-register/codification/executive-order/12333.html

Fagoyinbo, Joseph Babatunde. *The Armed Forces: Instrument of Peace, Strength, Development and Prosperity.* Bloomington, IN: Author House, 2013.

Foreign Intelligence Surveillance Act of 1978. US Code. Title 50. Chapter 36. As amended June 2, 2015. http://legcounsel.house.gov/Comps/Foreign%20Intelligence%20Surveillance%20Act%20Of%201978.pdf.

Goldschlag, David, Michael reed, and Paul Syverson. "Onion Routing for Anonymous and Private Internet Connections." US Naval Research Laboratory Report, 1999. http://www.dtic.mil/dtic/tr/fulltext/u2/a465075.pdf.

Henderson, Lance. *Darknet: A Beginner's Guide to Staying Anonymous Online*. Middletown, DE: Amazon Books, 2012.

Henderson, Lance. *Tor and the Dark Art of Anonymity*. Middletown, DE: Amazon Books, 2015.

Janczewski, Lech J. and Andrew M. Colarik. *Cyber Warfare and Cyber Terrorism.* Hershey NY: Information Science Reference, 2008.

Kirby, Michael Donald, Sonja Biserko, and Marzuki Darusman. *Report of the Detailed Findings of the Commission on Human Rights in the Democratic People's Republic of Korea-A/HRC/25/CRP.1*. Report to the United Nations. New York: United Nations Human Rights Council, February 7, 2014.

Leigh, David, and Luke Harding. *WikiLeaks: Inside Julian Assange's War on Secrecy*. New York: Public Affairs, 2011.

Mikkonen, Simo. "Stealing the Monopoly of Knowledge?: Soviet Reactions to U.S. Cold War Broadcasting." Kritika. *Explorations in Russian and Eurasian History* vol 87, no. 4 (November 2010).

Navy.com. *Information Warfare Officer.* http://www.navy.com/careers/information-and-technology/information-warfare.html#ft-key-responsibilities. Retrieved December 21, 2015.

Puddington, Arch. *Broadcasting Freedom: The Cold War Triumph of Radio Free Europe and Radio Liberty.* Lexington, KY: University Press of Kentucky, 2003.

Roberts, Lawrence G. Ph.D., "The Evolution of Packet Switching." http://www.packet.cc/files/ev-packet-sw.html (November 1978). Accessed December 30, 2015.

Singer, P.W., and Allen Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* New York: Oxford University Press, 2014.

Tucker, Patrick. *How the Military Will Fight ISIS on the Dark Web.* Defense One. February 24, 2015. http://defenseone.com/technolohy/2015/02/how-military-will-fight-isis-dark-web/105948/.

US Department of Defense, *Joint Publication 3-12.* Cyberspace Operations. Washington, DC: US Department of Defense, February 5, 2013.

US Department of Defense, *Joint Publication 3-13.* Information Operations. Washington, DC: US Department of Defense, November 20, 2014.

US Department of Defense, *The Department of Defense Cyber Strategy.* Washington, DC: US Department of Defense, April 2015.

US Department of the Navy. *Naval Administrative Message 316/09*. Establishment of the Deputy Chief of Naval Operations for Information Dominance (N2/N6). Washington, DC: US Department of the Navy, October 29, 2009. http://www.public.navy.mil/bupers-npc/reference/messages/Documents/NAVADMINS/NAV2009/NAV09316.txt.

Yetter, Richard B. "Darknets, Cybercrime, & The Onion Router: Anonymity & Security in Cyberspace." Master's Thesis, Utica College, 2015. http://media.proquest.com/media/pq/classic/doc/3670197591/fmt/ai/rep/NPDF?_s=AGGy%2FFQcuZcfwVoUH4ccbYPkLok%3D.

Zetter, Kim. "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History." *Wired.com* (July 11, 2011): http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.