AU/ACSC/2017

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

AFOSI CYBER THREAT PURSUIT: THE AIR FORCE'S 'OUTSIDE THE BOX' RESPONSE TO CYBER EXPLOITATION

by

Daron M Hartvigsen, DAFC

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor(s): Dr. Gregory F. Intoccia and Dr. Greg Williams

Maxwell Air Force Base, Alabama

February 2017

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the U.S. government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

TABLE OF CONTENTS

Page

LIST OF FIGURES

ABSTRACT

The purpose of this research paper is to encourage Air Force leaders to enhance the Air Force Office of Special Investigations' (AFOSI) unique cyber threat pursuit capabilities to achieve effects on adversaries and offer an important alternative to military operations. The problem/solution framework is used to study the extent, if at all, the Air Force has overlooked AFOSI cyber threat pursuit and disruption capabilities. The paper argues the case for Air Force decision makers to allocate more resources toward AFOSI's ability to act where traditional Air Force cyber capabilities cannot.

One key finding of this research is Air Force Cyber (AFCYBER), United States Cyber Command (USCYBERCOM), National Security Agency (NSA), and Department of Defense (DoD) network defense capabilities are not adequately enabled by policy or law to actively target cyber threat actors throughout the spectrum of conflict. An additional finding is AFOSI is enabled by law and policy to investigate, target, and counter cyber threats, during peacetime and war, whether criminal actors or nation-state entities.

Some key recommendations include the idea current Air Force decision-makers should: further enable AFOSI by updating policy, supplying additional resources, and increasing AFOSI's cyber investigative manpower allocations so the Air Force can better exploit the full spectrum of cyberspace through AFOSI's mission and legal enablers.

ABBREVIATIONS

AFCYBER	Air Force Cyber Command
AFIN	Air Force Information Network
AFOSI	Air Force Office of Special Investigations
AFPD	Air Force Policy Directive
ARCYBER	Army Cyber Command
CI	Counterintelligence
CIA	Central Intelligence Agency
CID	Army's Criminal Investigations Division
CIO	Chief Information Officer
CNE	Computer Network Exploitation
CNO	Computer Network Operations
CSS	Central Security Service
DCIO	Defense Criminal Investigative Organizations
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDIN	Department of Defense Information Network
E.O.	Executive Order
FAR	Federal Acquisition Regulation
FISA	Foreign Intelligence Surveillance Act
FLTCYBER	Fleet Cyber Command
IA	Information Assurance

IC	Intelligence Community
JPL	Jet Propulsion Laboratory
MARFORCYBER	Marine Forces Cyber Command
NDAA	National Defense Authorization Act
OPSEC	Operations Security
OSD	Office of the Secretary of Defense
NAF	Numbered Air Force
NASA	National Aeronautics and Space Association
NCIX	National Counterintelligence Executive
NDAA	National Defense Authorization Act
NSA	National Security Agency
NSD	National Security Directive
USCYBERCOM	United States Cyber Command
USSTRATCOM	United States Strategic Command
SECAF	Secretary of the Air Force
SIGINT	Signals Intelligence
USC	United States Code

SECTION 1: INTRODUCTION

The Air Force Office of Special Investigations (AFOSI) has fewer than 100 Special Agents trained to conduct cybercrime investigations and cyber counterintelligence operations. Air Force Cyber Command (AFCYBER) and its numbered Air Force host, 24th Air Force (AF), list its cyber force as 5400 members strong.[1] By virtue of Executive Order (E.O.) 12333 and Public Law, AFOSI agents are authorized to pursue and counter cyber threat actors throughout the spectrum of conflict. Currently, as a practical matter the only two Air Force entities specifically provisioned to conduct activities in cyberspace are 24th AF, which conducts cyber defensive activities, and AFCYBER, which conducts military operations.[2] Given AFOSI's broad charge to conduct activities in cyberspace, yet the virtually nonexistent resources to do so, the question must be asked: To what extent, if at all, do Air Force leaders overlook Air Force Office of Special Investigations' cyber threat pursuit and disruption mission as they seek to counter cyber threats across the spectrum of conflict? Air Force leadership has largely bypassed AFOSI's cyber threat pursuit capabilities due an all too common false assumptions that US intelligence agencies are the sole entities who should pursue and identify cyber threats; and AFCYBER warfighters are the sole AF entity who can conduct activities against those identified cyber threats.

Evidence of the Air Force bypassing AFOSI while building its cyber forces can be found by looking at the results of where the Air Force expended resources. Benefactors included the 24th AF, AFCYBER, and more recently, the 25th AF. AFOSI did not receive any additional funding or manpower from the Air Force as the Air Force ramped up its cyber portfolio. Not doing so has resulted in AFCYBER being limited to defensive activity and to a narrow military operations mission. First, the 24th AF is a military force designed to execute military operations. Military operations by design focus on an adversary's armed forces to achieve some effect on the

adversary's government.[3] AFCYBER's military operations mission means 24 AF generally cannot overtly exploit enemy vulnerabilities, attack systems or otherwise perform active actions to degrade threats until directed by the Secretary of Defense, through United States Strategic Command (USSTRATCOM).[4] The direction to execute military operations against another military, to affect an adversary's government is usually reserved for a time of active hostility or war and assumes positive identification of an adversary. Until AFCYBER's warfare capabilities are called on, AFCYBER and 24th AF largely perform peacetime activities to operate and defend Air Force networks "inside the wire." AFCYBER is very limited on what cyber activity they can do to impact threats outside of Air Force networks. Since AFCYBER is limited to military operations during hostilities, and internal Air Force networks during peacetime,[5] AFOSI is the only AF agency enabled to pursue and actively counter cyber threats, regardless of the stage of conflict.

Agencies who are missioned to execute criminal and counterintelligence investigative functions can act when AFCYBER, USCYBERCOM, and the Intelligence Community (IC) are unable. AFOSI is enabled by law and policy to be the bridge between the "walls" of defense, "spies" of the intelligence community, and the "warriors" who will theoretically spring into action once hostilities are declared.

Foreign spies represent a significant cyber threat to the United States and the U.S. Air Force.[6] Attributing foreign intelligence Computer Network Exploitation (CNE) to an actual entity is very difficult and often not possible.[7] Attribution to criminal hackers is also very difficult for many of the same reasons it is difficult to identify nation-state intelligence activity. Even if USCYBER or AFCYBER could attribute a hostile cyber action to a nation-state intelligence actor or criminal hacker, unleashing a military operation against either is not likely since neither are normally subject to a military response. Recent assertions in the news that

Russia and China are infiltrating and exploiting U.S. interests have yet to garner a United States "military operation" response using USCYBERCOM capabilities. Nonetheless, the United States is currently organizing the bulk of its cyber efforts around such military capabilities when responses by law enforcement or counterintelligence entities might be more appropriate.

Currently, the specter of cybercrime and espionage against U.S. interests is growing even in the face of the United States building better cyber "spies, bombs, and bullets." USCYBERCOM and the National Security Agency (NSA) seem to have had little effect on adversary exploitation of the United States. A 2015 Time.com article highlights how Chinese cyber intelligence was so successful at cyber theft that President Obama was left with no choice but to meet with China's president in November of 2015. Obama's message to China signaled China's continuing theft of United States' intellectual property needed to be stopped.[8]

Unfortunately, after years of investment into AFCYBER, USCYBERCOM, NSA, and others, all have largely failed to stop nation-state exploitation of the United States. This lack of effectiveness forced the President, who did not have any other option, to ask China to cease its hacking of U.S. interests. This fact is reason enough for the United States to explore other courses of action beyond building cyber walls (network defense), spies (NSA), warriors, bombs, and bullets (USCYBERCOM).

Given these developments, to what extent, if at all, do Air Force leaders overlook the need to fully use and exploit Air Force Office of Special Investigations' cyber threat pursuit and disruption mission as they seek to counter cyber threats? Air Force leadership is overlooking the Air Force Office of Special Investigations' cyber threat pursuit capability due to the common but ill-advised assumptions: (1) U.S. intelligence agencies are the sole entity who should pursue and identify cyber threats;[9] and (2) the nation must rely on war fighting capabilities to take some action to counter those threats.[10]

The Department of Defense (DoD) is experiencing a capabilities gap because USCYBERCOM and NSA are not able to counter ambiguous threat actors when those actors operate outside of the parameters warranting a military operations response. The DoD invested heavily in a cyber war fighting entity (USCYBERCOM) and an intelligence gathering function (NSA) to satisfy much of the nation's cyber security needs. Unfortunately, neither capability is sufficient. The Air Force requires an in-house capability able to operate against cyber threats even when attribution is ambiguous, and when military operations are not an option. AFOSI is enabled by law and policy to be the bridge between the "walls" of defense, "spies" of the intelligence community, and the "warriors" of AFCYBER.

The framework used for this project is the problem/solution model since it is most appropriate for exploring the legal and procedural factors influencing Air Force leaders who seem to overlook AFOSI's cyber counter-threat capabilities. The problem/solution framework helps highlight the unique authorities and policy AFOSI can exploit as it works to degrade threat actors and defend the Air Force.

The problem/solution framework guides a cyber threat review while allowing for an exploration of DoD's response to those threats. This paper will review how the United States directed resources to a war fighting command as well as an intelligence function in order to address the evolving requirements cyberspace was exposing. The problem/solution framework helps analyze the policy foundations leading to current United States cyber strategy and enables a discussion of the factors leading to AFOSI being largely bypassed when it came time to allocate resources to DoD cyber security functions.

Section Two describes the evolution of cyberspace from a security perspective and highlights some of the ways the Air Force and DoD began to respond to cyber's evolution. The cyber domain evolution was a difficult problem and the choices DoD leadership made resulted in

a very military centric end state.

Section Three reviews the missions of AFCYBER, USCYBER, NSA, and AFOSI. These entities are DoD capabilities with a stake in the identification and mitigation of cyber threats. The mission analysis will describe each organization's focus and their stated "lanes in the road."

Section Four reviews selected law and policy driving the missions of AFCYBER, USCYBER, NSA, and AFOSI. The authorities defining what entity can act is very important to understand when pursuing and countering cyber threat actors. These laws and policies describe which organization(s) should be operating against cyber threat actors, in any given circumstance.

Section Five summarizes the results of the mission analysis and policy review. It details the overarching finding that AFOSI's broad ability to challenge and counter cyber threats has not yet resonated with Air Force leadership. Section Five also highlights the gaps between AFOSI's cyber mission and current policy, AFOSI's need for additional funds, and additional manpower allocations.

Section Six synthesizes the previous sections into recommendations. It includes a suggestion for the Air Force to establish a Tiger Team tasked with investigating the benefits of relying more on AFOSI's capabilities within the Air Force's cyberspace portfolio. The Air Force should then create a plan to fund and resource AFOSI to better integrate and scale up the capabilities the Tiger Team finds are of most value.

Section Seven solidifies and summarizes resulting conclusions derived from the project's review of U.S. law, DoD policies, and agency missions. The primary conclusions include the fact our Air Force and DoD have many of the tools it needs to effectively pursue and counter cyber threats throughout the spectrum of conflict. Section Seven suggests the DoD would be more effective if it enabled those tools by building additional capacity outside of traditional military operations.

SECTION 2: BACKGROUND

Over the last few decades, hackers and their hacking activities shaped how the U.S. government responded to threats targeting its computer systems. The interlinking of computers and networks was initially an experiment by academics intended to share information, not keep it secure. The history surrounding network security and cyber threats has been explored often, however there is a perspective of cyber threat evolution not yet detailed much; the perspective shared by some DoD Law Enforcement and Counterintelligence agents.

External cyber threats in the late 1990s and early 2000s often originated from malicious kids who explored the rapidly evolving Internet by hacking into companies, government systems, and military networks.[11] One example was investigated by AFOSI and other Federal agencies from 2003 through 2005; the investigation linked numerous computer intrusions to a 16-year-old boy from Sweden. This boy went by the Internet handle "Stakkato."[12] Stakkato was wildly successful and his exploits eventually were publicized as the U.S. and Sweden worked to prosecute him. The publicity of his arrest included allegations he stole F-18 plans, accessed the National Aeronautics and Space Association's (NASA) Jet Propulsion Laboratory (JPL), and other Military systems.[13] Publicizing this information likely sent a message to other would-be hackers of repercussions if caught, while also signaling to foreign intelligence entities that computer theft is a viable way to satisfy their information needs.

The Air Force was quick to recognize the need to move against the looming cyber threat and had already began to organize against it when Lieutenant General (Lt Gen) Gen Bob Elder declared in October of 2006 he was standing up a "Cyber Command." [14] As the Air Force moved out to what many interpreted to be an effort to become the Executive Agent (EA)[15] for cyberspace, it did so during a time when the U.S. government was not yet able to define roles or

organizational expectations for those entities who were building cyberspace capacity. The lack of a synchronized effort was highlighted when in 2007 the USSTRATCOM commander described U.S. cyber strategy as "dysfunctional."[16] Without specific leadership the services within the DoD began building separate cyber functions.

Lt Gen Elder, as the 8th AF commander was in charge of the AF's strategic nuclear bomber fleet, as well as the AF's global network operations. Lt Gen Elder was responsible for the defense and operation of the Air Force's global information network and had first hand knowledge of foreign threats conducting CNE inside AF systems. In 2005 and 2006 there were a number of significant intrusions into AF systems and it became clear to all that more needed to be done. Lt Gen Elder, after support from the Secretary of the Air Force (SECAF), began the processes needed to build a "Cyber Command."[17] This effort faced immediate resistance from other DoD services and the NSA. Many in oppositon did not believe the Air Force should own DoD's posture in cyberspace and quickly organized to counter the idea the Air Force would serve as the EA for Cyberspace.[18] Consequently, the Air Force was forced to focus on Air Force equities and to name its new function in accordance with the emerging joint cyber community; the new command was coined "AFCYBER."[19]

AFCYBER began as a provisional command and much of the initial work to stand it up became the responsibility of a newly minted Numbered Air Force (NAF). The 24th Air Force was designated as the new NAF with the mission to "establish, maintain, operate, and defend Air Force cyberspace components; exploit adversary vulnerabilities; attack adversary systems; and provide command and control for assigned and attached cyberspace forces."[20]

As its subordinate, AFCYBER provides Air Force forces to United States Cyber Command (USCYBERCOM). USCYBERCOM and AFCYBER are responsible for defending the Department of Defense Information Network (DoDIN), providing support to combatant

commanders, and strengthening the nation's ability to withstand cyber-attacks.[21] Thus, both are focused principally on cyber defense and warfare. The factors influencing how AFCYBER was built and what it does are derived from USCYBERCOM's evolution. Therefore, both are irrevocably linked to each other and to their shared mission to conduct military operations.[22]

It was not long before the counterintelligence community observed a shift away from the criminal hacker to an organized and determined nation-state sponsored foe. This shift was finally publicly acknowledged in a very detailed report put out by the nation's focal point for counterintelligence, the National Counterintelligence Executive (NCIX).[23] The 2011 NCIX report highlighted sophisticated Russian and Chinese threats had exploited the United States since before 2009 and warned those threats were continuing to exploit U.S. interests, through cyberspace, in 2011.[24]

The 2011 NCIX report predicted cyber exploitation would continue and that prediction was correct; the United States has been working to counter nation-state cyber exploitation and theft ever since. Access, exploitation, and theft, however, has more recently evolved to nation-states using cyber activity to manipulate and influence other nations. Ironically, Russia acknowledged the evolution of cyber-attacks enabling "foreign influence" when it updated a Kremlin plan to defend against information-psychological methods by foreign intelligence agencies intent on influencing Russia's population using cyberspace activities.[25] The recent compromises and information leaks during the 2016 U.S. Presidential election confirms the 2011 NCIX report's assertion that cyber-attacks can be a tool for outsiders to further their goals against the United States. Recent events highlight a shift where covert theft has taken a back seat to overt actions. These overt actions are possible because it is difficult to attribute events in cyberspace to the originator. Attribution is not only needed to prosecute hackers in a court of law but is also a key component for USCYBERCOM engagement using military operations.

The evolution of cyber threats from curious teenagers to sophisticated strategic threats has forced the U.S. Government and the DoD to change. The United States responded to the ever-increasing sophistication of hackers by building cyber bombs and enhancing its cyber spies. The early days of building DoD and AF cyber capabilities did not include a correct assessment of emerging threats and how laws and authorities would enable DoD action. The result is an inordinate amount of emphasis for consolidation of effort into military operations and intelligence collections while ignoring law enforcement and counterintelligence capabilities.

SECTION 3: MISSION ANALYSIS

Air Force Cyber Command (AFCYBER)

The U.S. Air Force's primary cyber operations entity is the 24th AF headquartered at Joint Base San Antonio (JBSA). The 24th AF is a warfighting organization that "establishes, operates, maintains and defends Air Force networks to ensure warfighters can maintain the information advantage as U.S. forces prosecute military operations around the world."[26] As such the 24th is organized, trained, and equipped to support and execute military operations during peacetime and in war.

The 24th Air Force provides Air Force forces to USCYBERCOM to enable USCYBERCOM to conduct military operations in and through cyberspace. When performing missions under tasking from USCYBERCOM the 24th AF serves in its war fighting capacity as "Air Forces Cyber." AFCYBER's stated mission is "American Airmen delivering full-spectrum, global cyberspace capabilities and effects for our Service, the Joint Force, and our Nation."[27] AFCYBER commands and controls a global workforce operating and maintaining global cyber capabilities, a daunting task considering both must also be defended from a myriad of cyber threats. AFCYBER is comprised of 5,400 members, of which approximately 3,500 are military,

800 are civilian, and 900 are contractor personnel.[28] AFCYBER's cyber capabilities enable and ensure the success of Air Force and Joint operations throughout the globe. AFCYBER's fact sheet lists AFCYBER operations as six Lines of Effort (LOE). The listed LOE's are: Build, Operate, Secure and Defend the Air Force Information Network (AFIN) and directed mission critical cyber terrain, Extend cyber capabilities to the tactical edge of the modern battlefield, and Engage the adversary in support of combatant and air component commanders.[29] These LOEs re-enforce the idea that AFCYBER's role is to focus on the AFIN and engage the adversary only in support of "combatant and air component commanders."

United States Cyber Command (USCYBERCOM)

USCYBERCOM is the United States' principle cyber war fighting entity. USCYBERCOM's mission, as listed on its website, is: "plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."[30]

Like AFCYBER, USCYBERCOM is responsible to protect DoD networks while supporting combatant commander's requirements. These responsibilities are specifically called out in USSTRATCOM's web page under USCYBER's fact sheet. The fact sheet describes those responsibilities as defending the DoDIN, providing support to combatant commanders for execution of their missions around the world, and strengthening the United States' ability to withstand and respond to cyber attack.[31]

USCYBERCOM is entrusted by the SECDEF and enabled by DoD to unify all of DoD's cyberspace operations and is tasked with building and strengthening DoD cyberspace

capabilities. USCYBERCOM is also expected to operate resilient, reliable information and communication networks, counter cyberspace threats, and assure access to cyberspace.[32] Further, USCYBERCOM is responsible for conceptualizing and implementing the organizational, training, and certification standards for all the services supplying forces to USCYBERCOM's mission.[33]

Currently, USCYBERCOM in not a full combatant command, but rather is a sub-unified combatant command and it is still subordinate to USSTRATCOM. USCYBERCOM acquires its workforce from all military departments and is supported by: Army Cyber Command (ARCYBER), Fleet Cyber Command (FLTCYBER), AFCYBER, and Marine Forces Cyber Command (MARFORCYBER).[34]

National Security Agency (NSA)

The National Security Agency/Central Security Service (NSA/CSS) has a broad mission portfolio including Signals Intelligence (SIGINT) and support to military operations. NSA/CSS is responsible for the U.S. Government's cryptology needs while presumably using its expertise to execute intelligence collections, or SIGINT. NSA activities are designed to collect information about threats and security concerns to our nation. One result of NSA activities is the production of cyber threat indicators and warnings for community consumption. Often these indicators and warnings culminate in Information Assurance (IA) products and services[35] for DoD and U.S. Government customers to help those entities defend their networks. NSA also executes Computer Network Operations (CNO) in an effort to provide advantage for National decision makers.[36]

NSA describes its SIGINT role as activities intended to provide national and military leaders with information identifying the nation's adversaries, their location, plans, capabilities

and intentions.[37] Other customers include members of the intelligence community, law enforcement, and national policy makers such as Congress. As powerful as SIGINT can be for national leaders, it creates unique challenges when dissemination of the data is required. The methods and sources used to collect SIGINT are often a closely held secret. Dissemination controls for SIGINT information can stymie sharing of the data thus limiting the potential impact of the collected information. Acting on SIGINT harvests may even compromise the collection; therefore using SIGINT derived information to go after cyber threat actors creates Operations Security (OPSEC) challenges for NSA. NSA may in fact know who and where a threat actor is, but if it takes some action against that actor, it risks exposing its sources and methods.

NSA also has an IA mission in addition to its other better-known roles. NSA IA efforts serve the government and the nation in a way no other DoD or U.S. Government entity does. NSA's website highlights this national interaction by stating: "National Security Directive (NSD) 42 authorizes NSA to secure National Security Systems, which includes systems processing classified information or are otherwise critical to military or intelligence activities. IA has a pivotal leadership role in performing this responsibility, and partners with government, industry, and academia to execute the IA mission." [38] This mission statement suggests NSA defends classified and critical systems by partnering with external agencies, but any partnership is limited by the practicality of sharing SIGINT information and the OPSEC impact of doing so.

Air Force Office of Special Investigations (AFOSI)

The Air Force Office of Special Investigations was established 1 August of 1948 to investigate major crimes affecting the Air Force and has been the Air Force's primary force for investigation of felony level crime, since inception.[39] When AFOSI was established it was organized under the Secretary of the Air Force's Inspector General in an effort to prevent local

command influence from its activities. Today, AFOSI supports all Air Force activities with professional investigations and counterintelligence activities. As such, AFOSI's primary responsibilities to the Air Force are executing criminal investigations and counterintelligence services.[40]

AFOSI is a global force similar to NSA, USCYBER, and AFCYBER. AFOSI has 2,738 active-duty, reserve and civilian personnel[41] spread throughout the world working with various Law Enforcement and counterintelligence partners. Included in that global workforce are 2,029 federally credentialed Special Agents who are responsible for protecting critical technologies and information, detecting and mitigating threats, providing global specialized services, conducting major criminal investigations, and engaging foreign adversaries and threats offensively.[42]

AFOSI's mission statement as listed on its website is as follows: Identify, exploit and neutralize criminal, terrorist, and intelligence threats to the Air Force, Department of Defense and U.S. Government.[43] Since AFOSI is a federal law enforcement and investigative agency and its agents are recognized federal investigators, AFOSI can investigate throughout the domestic United States as well as overseas. Additionally, AFOSI agents are also credentialed counterintelligence officers and conduct counterintelligence activities globally, to include the domestic United States. This scope is unique in the DoD where other operational entities are confined to specific domains, in specific theaters. AFOSI can and does operate throughout the full spectrum of military conflict, in and through any domain, including cyberspace.[44]

SECTION 4: POLICY

There are generally five national capabilities the United States has at its disposal to defend against and counter cyber threat actors. The cyber security capabilities the United States relies on now were built in response to emerging requirements as the cyber domain evolved. As

criminal hackers hacked, law was updated to describe acceptable and unacceptable activity. The United States' vulnerability to cyber threats has been significant for more than 13 years and of course the threat remains real from a variety of sources. The U.S. response to cyber threats has been slow in coming. For instance, U.S. Cyber Command was only declared fully operational in late 2010. It was not until nation-states demonstrated advanced cyber capabilities that the Air Force began to build up cyberspace defenses intended to challenge those advancing threats.[45] U.S. law and policy has gone through a similar evolution as cyber threats challenged established conventions.

U.S. law currently defines which entities can act against cyber threats to the nation. The law's current structure authorizes various actions to address the cyber threat by U.S. intelligence services, cyber defense entities, law enforcement, counterintelligence entities, and the U.S. military. The U.S. intelligence services responsible for activities in cyberspace targeting cyber threat actors include NSA, Central Intelligence Agency (CIA), and the Defense Intelligence Agency (DIA). The federal government's cyber defense entities are numerous and include the Department of Homeland Security, NSA's Information Assurance Directorate,[46] Defense Information Systems Agency (DISA), DoD service network defenders (e.g. 24 AF), and many more. Law Enforcement entities include Federal, State, and local agencies. The Federal Bureau of Investigation (FBI) operates as the U.S. Governments principle investigative authority when it comes to cyber crime and nation-state exploitation.

The Department of Homeland Security (DHS) is often assumed to have a significant role in the United States cyber operations portfolio. Law and policy has not yet enabled DHS to act against cyber threats and it does not have a law enforcement or counterintelligence role. DHS is primarily operating a defensive posture without a means to actively go after threats and stop them. DHS is focused on a defensive mission called "securing cyberspace"[47] that provides cyber

security updates and incident coordination. Even with this narrow focus, DHS has largely been a failure in its cyber security efforts. A recent U.S. Senate review of DHS's performance found DHS was not likely to protect the nation from cyber security threats.[48] DHS is just not a significant factor in the defense, pursuit, or countering of cyber threat actors and is an example of how focusing on defense is not sufficient. DHS, however, is not alone in its inability to do much about sophisticated threats. The entities who have the capacity to challenge sophisticated threats are finding U.S. law and DoD policy both slow to evolve.

The authorities enabling NSA's collection of intelligence are derived from two sources: Executive Order (E.O.)12333 and the Foreign Intelligence Surveillance Act of 1978 (FISA).[49] Executive Order 12333 was originally signed in 1978 and is the foundational authority for all intelligence and counterintelligence entities in the United States. E.O. 12333 was revised in 2008 and that revision defined roles in the intelligence community, specifically directing NSA to collect, retain, analyze, and disseminate foreign signals intelligence information[50] and clearly directs intelligence activity to be focused on foreign persons outside the United States.[51]

To effect intelligence activities pursuant to E.O. 12333 NSA must; identify foreign entities (persons or organizations) with information responsive to an identified foreign intelligence requirement, identify how the foreign entities communicate, identify the telecommunications infrastructure used, seek out vulnerabilities that will enable the collection (if needed), exploit those vulnerabilities, and collect the intelligence required.[52] NSA is subject to oversight and controls designed to ensure intelligence collection is focused on and responsive to only valid foreign intelligence requirements.[53]

One of the challenges of NSA's activities pursuant to EO 12333 is the fact intelligence is collected from global communications systems using sources and methods that are very sensitive. Releasing those collections outside of a highly classified environment would likely

compromise the processes used to successfully gather the information.[54]

NSA's other key enabler is the Foreign Intelligence Security Act (FISA). FISA's section 702 established legal standards and processes which enables NSA to target non-U.S. persons who are reasonably believed to be located outside the United States, as their communications traverse U.S. based service providers.[55] Once approved by the FISA court, the U.S. service providers are compelled to assist NSA in acquiring the communications associated with the authorization.[56] NSA's ability to exercise section 702 and conduct surveillance of Foreign Intelligence activity as that activity moves through U.S. networks is key to understanding adversary intentions and capabilities. Like SIGINT however, FISA harvests are held as close secrets to prevent signaling the adversary that its actions are being observed. Using FISA knowledge to overtly target and counter the adversary could represent an unacceptable OPSEC risk. It is for this reason FISA collections are not used to actively pursue and counter the adversary.

Like NSA, AFOSI derives its authority to operate from two main sources; one is E.O. 12333 and the other is Public Law 99-145, Section 1223. While E.O. 12333 authorizes AFOSI to conduct intelligence and counterintelligence activities, Public Law 99-145 forms the foundation for AFOSI's criminal investigative authorities.

Executive Order 12333 constitutes guidance by the President of the United States and lists expectations of U.S. Counterintelligence (CI) organizations (for which AFOSI is one) by defining CI as "information gathered and activities conducted to identify, deceive, exploit, disrupt or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist activities."[57] E.O. 12333 does not limit counterintelligence entities to only do counterintelligence activities, but it also gives counterintelligence forces the additional

mission to collect intelligence.[58] The order establishes DoD's authority to engage in offensive and defensive counterintelligence operations through paragraph 1.10, as it directs the SECDEF to execute intelligence missions for the nation and also directs the SECAF to conduct counterintelligence activities.[59]

In furtherance of E.O. 12333 the Deputy Secretary of Defense published Department of Defense Directive (DoDD) 5240.02 in March of 2015. This directive details the DoD's Counterintelligence program and states: CI activities are undertaken as part of an integrated DoD and national effort to detect, identify, assess, exploit, penetrate, degrade, and counter or neutralize espionage, intelligence collection, sabotage, sedition, subversion, assassination, and terrorist activities conducted for or on behalf of foreign powers, organizations, persons, or their agents directed against U.S. national security interests or DoD and its personnel, information, materiel, facilities, and activities.[60] Additionally, DoD Manual 5240.01, Procedures Governing the Activities of DoD Intelligence Components, is a manual that defines what entities are Defense Intelligence Components and lists AFOSI as one.[61]

AFOSI's criminal investigative enabler is Public Law 99-145, Section 1223. This law provides authority for independent criminal investigations by Navy and Air Force investigative units. The law does so by stating: "The Secretary of the Air Force shall prescribe regulations providing to the Air Force Office of Special Investigations authority to initiate and conduct criminal investigations on the authority of the Commander of the Air Force Office of Special Investigations." [62]

Public Law 99-145 is implemented in the Department of Defense by DoD Instruction 5505.3, Initiation of Investigations by Defense Criminal Investigative Organizations (DCIO), dated 24 Mar 11. DoD Instruction 5505.3 establishes DoD policy that directs the DCIOs such as AFOSI, Army Criminal Investigations Command (also known as "CID"), and Naval Criminal

Investigative Service (NCIS) to undertake independent investigations by establishing the ground rules that the DCIOs do not require approval to investigate violations of law from any outside authority.[63] This independence is crucial for AFOSI, NCIS, and CID's ability to pursue criminals regardless of rank and influence.

The public law solidifying AFOSI's status as a federal investigative agency is 10 U.S. Code (USC), section 9027. This law grants authority to the Secretary of the Air Force to authorize civilian Special Agents of the Office of Special Investigations to execute warrants and make arrests.[64] Some relevant examples of U.S. code AFOSI can investigate are:

- 18 USC 1030; Computer Fraud and Abuse Act
- 18 USC 2701; Unlawful Access to Stored Communications
- 18 USC 1028(a)(7); Identity Theft
- 18 USC 1028A; Aggravated Identity Theft
- 18 USC 1029; Access Device Fraud
- 18 USC 1037; CAN-SPAM Act
- 18 USC 1343; Wire Fraud
- 18 USC 1362; Communication Interference

The laws and policy that drive AFOSI's criminal and counterintelligence missions clearly enable AFOSI to traverse the spectrum of threats currently targeting the Air Force. AFOSI is not limited by SIGINT and FISA dissemination concerns and can action information derived from its law enforcement and counterintelligence activities.

USCYBERCOM and AFCYBER derive their authorities from the same source yet AFCYBER serves as subordinate function to USCYBER. USCYBERCOM's authority to execute its mission begins with Title 10, USC section 164, which directs the Commander of USSTRATCOM to perform duties under the authority and control of the Secretary of Defense.[65]

As a sub-unified command, USCYBERCOM works for the Secretary of Defense though the USSTRATCOM commander in accordance with the Unified Command Plan.[66] USCYBERCOM's mission is to plan, coordinate, integrate, synchronize, and conduct activities to: direct the operations and defense of specified Department of Defense information networks and prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure U.S./Allied freedom of action in cyberspace and deny the same to the nation's adversaries.[67] Current law and policy ensures USCYBERCOM focuses on defending the DoDIN, supporting combatant commanders, and enhancing the nation's ability to withstand and respond to cyber-attacks.[68]

The Fiscal Year (FY) 2017 National Defense Authorization Act (NDAA) is U.S. law describing how the Defense Department will function and includes direction on where resources are to be allocated. FY 2017's NDAA acknowledges there is a cyber structure shortfall by fixing that gap with a provision to improve Office of Secretary of Defense (OSD) oversight and integration of defense cyber activities. The act recognizes that the "responsibility" for cyber is split between different organizations within OSD.[69] The NDAA attempts to solve this split by consolidating power in an Assistant Secretary of Defense for Information who would oversee the security of the DoDIN as well as defense space policy and cyber war fighting activities. While this new position would wrangle NSA, DISA, and USCYBERCOM, it does not address nor resolve the need for the DoD to act against cyber threats throughout the spectrum of conflict.

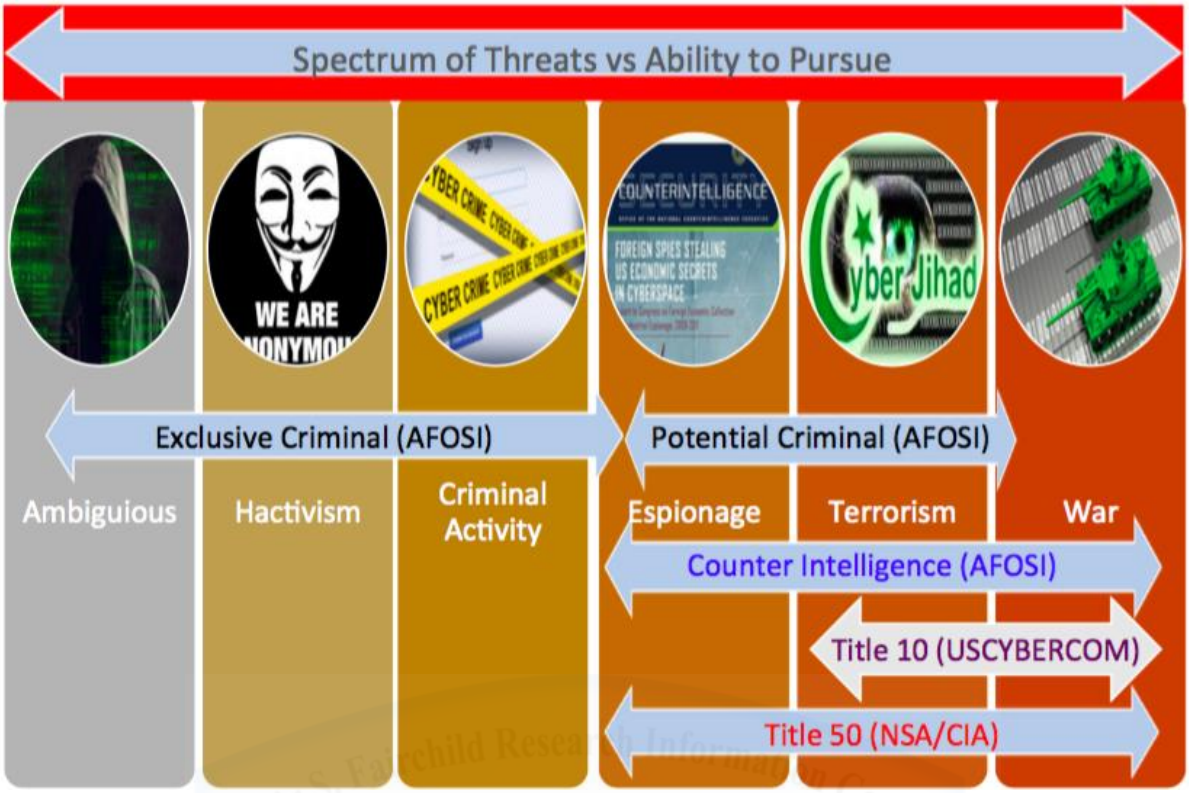

Figure 1.

U.S. cyber capabilities rely on threats to be characterized and defined in order to trigger the appropriate law and polices for any response. For instance, criminal actors that hack into computers violate federal law and the appropriate response to a violation of law is a federal criminal investigation. The results of the investigations are then provided to a prosecuting authority for action.

The threat spectrum chart (Figure 1) illustrates where cyber threats intersect the different authorities. The Criminal, Counterintelligence, War fighting, and Intelligence functions listed are all activities able to execute some action to impact an offending threat actor when enabling conditions are right. Law enforcement agencies are responsible for the investigation, pursuit, and prosecution of cyber threat actors who conduct criminal activity in cyberspace. AFOSI, FBI, NCIS, and others are pursuing these types of criminal actors day in and day out. The chart accurately excludes USCYBER, AFCYBER, and NSA as action authorities for criminal matters,

given that their only role during criminal investigations is to report criminal activity when observed and to support investigative activity when requested.

One type of criminal activity to note is "hactivism." Hactivists are activist who are seeking to make a statement by exploiting computer systems for some politically oriented effect. In Figure 1. hactivists are described as subject to criminal authorities because they often violate federal law when they compromise a computer system. Hactivists for instance, have hacked into DoD web pages and replaced the original content with their message of choice.[70] When that situation occurs on Air Force systems, the AFOSI investigates the intrusion to identify the responsible party and works with a U.S. Attorney to prosecute that entity. It can be argued the recent compromise of Democratic National Committee emails was done by hactivists since the apparent intended effect was for political impact. USCYBER, AFCYBER, and NSA are once again in more of a defensive posture against this type of threat. AFOSI and other federal law enforcement agencies are empowered to pursue and assist in the prosecution of activists who conduct crimes in furtherance of their activities.

Terrorists and insurgents are targets USCYBER and AFCYBER can engage once the Secretary of Defense tells USSTRATCOM to do so. USCYBER cannot go after all terrorists, just ones they are ordered to target. Currently, an order only exists for the targeting and exploitation of ISIS.[71] AFOSI and the FBI, however, can pursue and counter terrorists and insurgents when either demonstrates a threat to U.S. interests.

Engaging nation-states during peacetime has proven to be a difficult problem to address for the United States. If a nation-state conducts criminal activity or espionage during peacetime, USCYBERCOM and AFCYBER are once again, playing defense. NSA has a broad mission to conduct SIGINT in order to observe hostile nation-state activity, but NSA's mission does not suggest NSA will take some active action to degrade or counter nation-state activity, during

peacetime. Even if it could, OPSEC concerns limits NSA's ability to act. AFOSI and the FBI however are charged with pursuing and countering nation-state activity, throughout the spectrum of conflict.

The threat spectrum chart (Figure 1.) highlights where employing Title 10 military authorities is appropriate. During times of conflict USCYBER and AFCYBER's mission and role make them the nation's primary cyber war fighting capability. While USCYBERCOM has previously argued for a larger mission and scope that would expand their charge beyond terrorists and state actors; to date that expansion has not been successful. Admiral Mike Rogers, Commander of USCYBERCOM, recently stated that offensive cyber operations are treated like nuclear weapons in the sense that using them outside a defined area of hostilities is not yet delegated down to the combatant commands.[72] Conversely, AFOSI and FBI can operate beyond terrorists and nation-states yet through their counterintelligence authorities also have a distinct role supporting Title 10 USC military operations; including support of a combatant commander's efforts.

The point to take from the threat spectrum chart is that the characterization of the threat will define what U.S. capability will respond. If a threat actor or group conducts malicious activity against the DoD and the activity or origin is not attributed to a nation-state or foreign military, then the activity is initially investigated as a criminal matter. Federal investigations are uniquely enabled to pursue and prosecute unknown actors and ambiguous threats. AFOSI is not beholden to ensuring the actor or system is a legitimate military target since AFOSI focuses on the violation of U.S. code and whether the Air Force or DoD is a victim of that violation. Like traditional investigations, one main objective for pursuing threats in cyberspace could be to find out whom in fact, is the criminal.

SECTION 5: RESULTS

Even though a review of policy and mission suggests AFOSI has a broad ability to challenge and counter cyber threats and is enhanced by a diverse foundation of enablers, Air Force leadership have not yet provided AFOSI with additional funds or manpower allocations to further exploit those enablers. Much of the effort in DoD and the Air Force to operate in and secure cyberspace has gone to AFCYBER and USCYBERCOM. The Air Force processes responsible for establishing and building the service's cyber portfolio bypassed AFOSI through passive exclusion when the time came to fund additional capabilities and allocate manpower.

An argument might be made suggesting that bypassing decentralized centers of authority such as AFOSI was by design; that USCYBERCOM and AFCYBER did so intentionally to ensure strategic control of cyber effects and offer time to mature the roles and capabilities in the domain. If true, neither USCYBERCOM nor AFCYBER got the word to the interagency and its whole of government efforts. Coordination and approval for strategic cyber operations is currently championed and vetted by the National Security Counsel (NSC) staff, not USCYBERCOM. This suggests USCYBERCOM does not control strategic decisions and likely only bypassed capabilities like AFOSI to ensure resources flowed directly for their benefit, without being diluted by agencies such as AFOSI. In fact, the NSC effectively bypasses USCYBERCOM when they entertain an AFOSI strategic cyber operation proposal. While AFOSI includes USCYBERCOM and AFCYBER during the interagency coordination process, neither are included in the NSC approval chain. If USCYBERCOM leaders would have assessed AFOSI and its peers accurately during the outset of its cyber evolution it would have likely sought to own and control AFOSI's cyberspace mission so that it could benefit from AFOSI's broad ability to operate. The reality is USCYBER and DoD likely ignored entities like AFOSI to focus resource allocations and ensure those allocations benefit USCYBER and NSA. It was

likely in USCYBERCOM's and NSA's best interest to be seen as the primary value for national investments in cyberspace capabilities.

A recent congressional research report confirms one important challenge that highlights why AFCYBER and USCYBERCOM are incomplete solutions for actively engaging cyber threats. It rightly stated that there is not yet a clear process to determine if a cyber-attack is a criminal matter, the result of hactivism, terrorism, or equivalent to an armed attack emanating from a nation-state.[73] It is this ambiguity that can prevent the United States from responding with USCYBERCOM capabilities. Among other things, the target of military operations must be viewed as legitimate and proportional. Responding to an unknown actor who is conducting criminal intrusions into DoD systems with a DoD cyber-attack against that actor's local electrical grid is not likely to be viewed as proportional.[74] This example is one reason AFCYBER and USCBERCOM are limited to military operations against specific terrorist or nation-state threats. Conversely, law and policy is clear that AFOSI has a broad mission to target and counter threats across the threat spectrum, independent of or in concert with, military operations.

SECTION 6: RECOMMENDATIONS

In order for the Air Force to move forward and exploit cyber threat actors across the full spectrum of authorities, the Air Force should create enabling policy, supply additional resources, and increase AFOSI's cyber investigative manpower allocations.

Air Force policy should be updated and expanded to integrate AFOSI's mission into the Air Force's core cyber functions. Air Force Policy Directive (AFPD) 17-1 should be re-tooled to include AFOSI as a key component to the overall Air Force information dominance policy. AFPD 17-1 should direct AFOSI to develop a cyberspace threat pursuit and effects plan that is aligned with AF Information Dominance plans. AFPD 17-1 should also call out AFOSI to:

participate in cyberspace governance forums; establish capability needs and requirements for cyber threat pursuit infrastructure; coordinate counterintelligence activities required to fully identify; pursue, and counter the cyber threat; and advocate for the integration of AFOSI cyberspace capabilities into AF operational capabilities-based planning and development processes.

Air Force policy experts should also work with AFOSI to build counterintelligence activities and law enforcement effects into the Joint Forces Air Component Commander's maneuvering through Joint Doctrine updates. Specifically, the Air Force should update Air Force Doctrine such as Annex 3-12, Organization of Cyberspace Operations, to include AFOSI and its threat pursuit and counterintelligence capabilities.

The Air Force Chief Information Officer (CIO) should partner with AFOSI to conduct a formal mission study. The study should at determine what additional resources would be needed for AFOSI to adequately supply Air Force leadership with cyber effects options that support peacetime defense as well as military operations during hostilities.

AFOSI's manpower allocated to pursuing and countering cyber threats competes with other AFOSI missions. Currently, AFOSI would have to move manpower from one of its other missions in order to add manpower to cyber operations. Moving agent billets from positions investigating sexual assaults, murders, and significant fraud (among others) will create mission execution gaps in traditional operations. AFOSI must still adequately investigate major crimes on Air Force bases so moving resources internally will likely negatively impact the currently assigned mission. In order for the Air Force and DoD to effectively exploit AFOSI's access to a larger part of the cyber threat spectrum, additional manpower allocations for AFOSI are needed.

A comprehensive study is needed to conclusively define what effects the Air Force wants to achieve in cyberspace while contrasting all of its current capabilities against a desired end

state. This study should include Air Force operational and cyberspace leadership, AFCYBER operators, AFOSI experts, and USCYBERCOM. The study would explore current capabilities across the service, existing expectations and missions, highlight redundancy, and recommend change to better allocate resources across all of the Air Force's requirement spectrum.

SECTION 7: CONCLUSIONS

AFCYBER, USCYBERCOM, the National Security Agency, and the Department of Defense network defense capabilities are not adequately enabled by policy or law to actively target cyber threat actors throughout the spectrum of conflict. U.S. law limits DoD cyber security entities and military activities to a narrow window of maneuverability.

In contrast, AFOSI is enabled by law and policy to investigate and counter cyber threats during peacetime and war, whether criminal actors or nation-state entities. AFOSI can project forces outside the boundaries of a base, DoD network, and U.S. soil in its pursuit of cyber threats. AFOSI represents a unique capability as well as an opportunity for the Air Force to achieve more in and through cyberspace

Current cyber activities executed by AFCYBER, USCYBERCOM, the DoD, DHS, and throughout the nation are not enough. Law enforcement and counterintelligence capabilities should be given more resources to act. Until now, Air Force leadership has largely bypassed AFOSI's cyber threat pursuit capabilities through passive exclusion. AFOSI has not received sufficient manpower from the Air Force to fully exploit its ability to conduct cyber investigations and operations across cyberspace. The force currently executing cyber investigations and operations was built over time using internal resources and should have benefitted from additional capabilities as the Air Force built its cyberspace portfolio.

While the Air Force has built AFCYBER to a more than 5000 member strong force, it is

a force unable to traverse the cyber threat spectrum. It stands to reason the Air Force should embark on a study of its current cyber portfolio with an eye towards re-allocating some of those 5000 personnel, updating policy, and re-allocate cyber resources to better equip AFOSI so that the Air Force has a broader impact across the cyber threat spectrum.

Notes

[1] 24th Air Force, Fact Sheets, "About Us," 27 Jul 16, http://www.24af.af.mil/About-Us/Fact-Sheets/Display/Article/458567/24th-air-force-afcyber, accessed 28 Jan 17.

[2] Ibid.

[3] Joint Publication 1, "Doctrine for the Armed Forces of the United States," DTIC.mil,23 Mar 13, http://www.dtic.mil/doctrine/new_pubs/jp1.pdf, I-5, accessed 28 Jan 17.

[4] Pellerin, Cheryl. U.S. Department of Defense, "Rogers Discusses Near Future of U.S. Cyber Command," DoD News, 24 Feb 17, https://www.defense.gov/News/Article/Article/1094167/rogers-discusses-near-future-of-us-cyber-command, accessed 25 Feb 17.

[5] Air Force Doctrine Center, Annex 3-12 Cyberspace Operations, "Organization of Cyberspace Operations, https://doctrine.af.mil/download.jsp?filename=3-12-D09-CYBER-Organization.pdf, accessed 18 Sept 16.

[6] Office of the National Counterintelligence Executive, "Foreign Spies Stealing US Economic Secrets in Cyberspace," Report to Congress on Foreign Economic Collection and Industrial Espionage, Oct 2011, https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf, accessed 21 Jan 17.

[7] Ibid.

[8] TIME. "U.S. Counterintelligence Chief Not Convinced China Has Halted Espionage." Time.Com [serial online]. November 19, 2015, available from: Military & Government Collection, Ipswich, MA. Accessed 10 Sep 2016.

[9] Jones, S. (2016). Cyber espionage: A new cold war? FT.Com, Retrieved from http://aufric.idm.oclc.org/login?url=http://search.proquest.com.aufric.idm.oclc.org/docview/1820518857?accountid=4332, accessed 18 Sept 16.

[10] Ramsby, C. M., USAF., & Yannakogeorgos, P. A. (2016). A reality check on a cyber force. Strategic Studies Quarterly, 10(2), 116-133. Retrieved from http://aufric.idm.oclc.org/login?url=http://search.proquest.com.aufric.idm.oclc.org/docview/1793664601?accountid=4332, accessed 18 Sept 16.

[11] Moore, Johannes. School of Advanced Air and Space Studies, " From Conception to Birth: The Forces Responsible For AFCYBER'S Evolution, June 2014, www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA626419, accessed 21 Jan 17, 7.

[12] Markoff, John and Bergman Lowell. The New York Times, "Internet Attack is Called Broad and Long Lasting," 10 May 2005,

Notes

http://query.nytimes.com/gst/fullpage.html?res=9906E4DF1330F933A25756C0A9639C8B63&pagewanted=all, accessed 21 Jan 17.

[13] Ibid.

[14] Rogin, Josh. FCW.com, "Cyber officials: Chinese hackers attack 'anything and everything," 13 Feb 2007, https://fcw.com/articles/2007/02/13/cyber-officials-chinese-hackers-attack-anything-and-everything.aspx, accessed 21 Jan 17.

[15] Moore, Johannes. School of Advanced Air and Space Studies, " From Conception to Birth: The Forces Responsible For AFCYBER'S Evolution, June 2014, www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA626419, accessed 21 Jan 17. 62.

[16] Ibid.

[17] Ibid.

[18] Ibid.

[19] Ibid.

[20] Air Force Doctrine Center, Annex 3-12 Cyberspace Operations, "Organization of Cyberspace Operations, https://doctrine.af.mil/download.jsp?filename=3-12-D09-CYBER-Organization.pdf, accessed 18 Sept 16.

[21] STRATCOM Factsheet."U.S. Cyber Command (USCYBERCOM),"20 Sep 16, ttp://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/, accessed 28 Jan 17.

[22] Joint Publication 1, "Doctrive for the Armed Forces of the United States, DTIC.mil, 23 Mar 13, http://www.dtic.mil/doctrine/new_pubs/jp1.pdf, I-5, accessed 28 Jan 17.

[23] Office of the National Counterintelligence Executive, "Foreign Spies Stealing US Economic Secrets in Cyberspace," Report to Congress on Foreign Economic Collection and Industrial Espionage, Oct 2011, https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf, accessed 21 Jan 17.

[24] Ibid.

[25] Kramer, Andrew, "Russia Updates Plan to Counter Cyberattacks and Foreign Influence," New York Times, 6 Dec 16, https://www.nytimes.com/2016/12/06/world/europe/russia-putin-cyberattacks.html?_r=0, accessed 28 Jan 17.

[26] 24th Air Force, Fact Sheets, "About Us," 27 Jul 16, http://www.24af.af.mil/About-Us/Fact-Sheets/Display/Article/458567/24th-air-force-afcyber, accessed 28 Jan 17.

[27] Ibid.

Notes

[28] Ibid

[29] Ibid.

[30] U.S. Strategic Command (USSTRATCOM) Factsheet. "U.S. Cyber Command (USCYBERCOM)," 30 Sep 16, http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/, accessed 28 Jan 17.

[31] Ibid.

[32] Ibid.

[33] Ibid.

[34] Ibid.

[35] National Security Agency, "Frequently Asked Questions," 28 Jun 16, https://www.nsa.gov/about/faqs/about-nsa-faqs.shtml, accessed 28 Jan 17.

[36] National Security Agency, "About Us," 3 May 16, https://www.nsa.gov/about/mission-strategy, accessed 28 Jan 17.

[37] Ibid.

[38] National Security Agency, "What We Do," https://www.nsa.gov/what-we-do/information-assurance/, 4 May 16, accessed 28 Jan 17.

[39] Air Force Office of Special Investigations, "Fact-Sheet," 9 May 11, http://www.osi.af.mil/About/Fact-Sheets/Display/Article/349945/air-force-office-of-special-investigations/, accessed 28 Jan 17.

[40] Ibid.

[41] Ibid.

[42] Ibid.

[43] Ibid.

[44] Ibid.

[45] Moore, Johannes, School of Advanced Air and Space Studies, " From Conception to Birth: The Forces Responsible For AFCYBER'S Evolution," June 2014, www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA626419, accessed 21 Jan 17, vi.

[46] NSA.gov, "Curt Dukes (IAD) - Overview of NSA's Cyber Security Mission," 1 Oct 15,

https://www.nsa.gov/news-features/news-stories/2015/in-discussion-with-curt-dukes.shtml, accessed 11 Feb 17.

[47] Department of Homeland Security, "Safeguard and Secure Cyberspace," 21 Mar 16, https://www.dhs.gov/safeguard-and-secure-cyberspace, accessed 11 Feb 17.

[48] Senator Colburn, Tom. "A Review of the Department of Homeland Security's Missions and Performance," U.S. Senate Committee on Homeland Security and Governmental Affairs, Jan 2015, 12.

[49] NSA.gov, "The National Security Agency: Missions, Authorities, Oversight and Partnerships," https://www.nsa.gov/news-features/press-room/statements/2013-08-09-the-nsa-story.shtml, accessed 4 Feb 17.

[50] Central Intelligence Agency, CIA.gov, "About CIA: Executive Order 12333 United States Intelligence Activities," https://www.cia.gov/about-cia/eo12333.html, accessed 4 Feb 17.

[51] Ibid.

[52] NSA.gov, "The National Security Agency: Missions, Authorities, Oversight and Partnerships," https://www.nsa.gov/news-features/press-room/statements/2013-08-09-the-nsa-story.shtml, accessed 4 Feb 17.

[53] Ibid.

[54] Ibid.

[55] Ibid.

[56] Ibid.

[57] The White House. "Executive Order: Further Amendments to Executive Order 12333, United States Intelligence Activities," News & Policies, July 2008, http://georgewbush-whitehouse.archives.gov/news/releases/2008/07/20080731-2.html, accessed 15 Oct 16.

[58] Ibid

[59] Ibid.

[60] Department of Defense, Directive 5240.02, "Counterintelligence," 17 Mar 15, http://www.dtic.mil/whs/directives/corres/pdf/524002p.pdf, accessed 4 Feb 17.

[61] Department of Defense Manual 5240.01, "Procedures Governing The Conduct of DoD Intelligence Activities," 8 Aug 16, http://www.dtic.mil/whs/directives/corres/pdf/524001m.pdf, accessed 4 Feb 17.

Notes

[62] Public Law 99-145, Section 1223, "Department of Defense Authorization Act, 1986," U.S. Government Publishing Office, https://www.gpo.gov/fdsys/pkg/STATUTE-99/pdf/STATUTE-99-Pg583.pdf, accessed 14 Jan 17.

[63] Department of Defense Instruction 5505.03, "Initiation of Investigations by Defense Criminal Investigative Organizations," 24 Mar 11, http://www.dtic.mil/whs/directives/corres/pdf/550503p.pdf, accessed 4 Feb 17.

[64] United States Code, Title 10 § 9027, "Civilian special agents of the Office of Special Investigations: authority to execute warrants and make arrests," https://www.law.cornell.edu/uscode/text/10/9027, accessed 4 Feb 17.

[65] Cornell University Law School, "10 U.S. Code § 164 - Commanders of combatant commands: assignment; powers and duties," Legal Information Institute, https://www.law.cornell.edu/uscode/text/10/164, accessed 11 Feb 17.

[66] U.S. Department of Defense, "Unified Command Plan," https://www.defense.gov/About/Military-Departments/Unified-Combatant-Commands, accessed 11 Feb 17.

[67] U.S. Strategic Command (USSTRATCOM) Factsheet. "U.S. Cyber Command (USCYBERCOM)," 30 Sep 16, http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/, accessed 28 Jan 17.

[68] Ibid.

[69] 114th Congress 2d Session, H.R. 4909, ''National Defense Authorization Act for Fiscal Year 2017," https://www.congress.gov/114/bills/hr4909/BILLS-114hr4909rh.pdf, accessed 15 Oct 16.

[70] Denning, Dorothy. "The Rise of Hactivism,"Georgetown Journal of International Affairs, 8 Sep 15, http://journal.georgetown.edu/the-rise-of-hacktivism/, accessed 25 Feb 17.

[71] Ellen Nakashima, "U.S. military has launched a new digital war against the Islamic State," Washington Post, 15 July 2016, https://www.washingtonpost.com/world/national-security/us-militarys-digital-war-against-the-islamic-state-is-off-to-a-slow-start/2016/07/15/76a3fe82-3da3-11e6-a66f-aa6c1883b6b1_story.html?utm_term=.1bb32f93a5ca, accessed 18 Feb 17.

[72] Pellerin, Cheryl. "Rogers Discusses Near Future of U.S. Cyber Command," U.S. Department of Defense News, 24 Feb 17, https://www.defense.gov/News/Article/Article/1094167/rogers-discusses-near-future-of-us-cyber-command, accessed 25 Feb 17.

[73] Catherine A. Theohary and John W. Rollins, "Cyberwarfare and Cyberterrorism: In Brief," Congressional Research Service Report, 27 Mar 15, 2.

[74] Ibid, 49.

Bibliography

114th Congress 2d Session, H.R. 4909. ‘‘National Defense Authorization Act for Fiscal Year 2017,” https://www.congress.gov/114/bills/hr4909/BILLS-114hr4909rh.pdf (accessed 15 Oct 16).

24th Air Force, Fact Sheets. “About Us,” 27 Jul 16, http://www.24af.af.mil/About-Us/Fact-Sheets/Display/Article/458567/24th-air-force-afcyber (accessed 28 Jan 17).

Air Force Office of Special Investigations.“Fact-Sheet,” 9 May 11, http://www.osi.af.mil/About/Fact-Sheets/Display/Article/349945/air-force-office-of-special-investigations/ (accessed 28 Jan 17).

Annex 3-12 Cyberspace Operations, “Organization of Cyberspace Operations, Air Force Doctrine Center, https://doctrine.af.mil/download.jsp?filename=3-12-D09-CYBER-Organization.pdf (accessed 18 Sept 16).

Colburn, Tom (U.S. Senator). “A Review of the Department of Homeland Security’s Missions and Performance,” U.S. Senate Committee on Homeland Security and Governmental Affairs, Jan 2015, 12.

Denning, Dorothy. “The Rise of Hactivism,”Georgetown Journal of International Affairs, 8 Sep 15, http://journal.georgetown.edu/the-rise-of-hacktivism/ (accessed 25 Feb 17).

Department of Defense Directive 5240.02, “Counterintelligence,” DTIC.mil, 17 Mar 15, http://www.dtic.mil/whs/directives/corres/pdf/524002p.pdf (accessed 4 Feb 17).

Department of Defense, Instruction 5505.03, “Initiation of Investigations by Defense Criminal Investigative Organizations,” 24 Mar 11, http://www.dtic.mil/whs/directives/corres/pdf/550503p.pdf, accessed (4 Feb 17).

Department of Defense Manual 5240.01, “Procedures Governing The Conduct of DoD Intelligence Activities,” 8 Aug 16, http://www.dtic.mil/whs/directives/corres/pdf/524001m.pdf (accessed 4 Feb 17).

Department of Defense, “Unified Command Plan,” https://www.defense.gov/About/Military-Departments/Unified-Combatant-Commands (accessed 11 Feb 17).

Department of Homeland Security. “Safeguard and Secure Cyberspace,” 21 Mar 16, https://www.dhs.gov/safeguard-and-secure-cyberspace (accessed 11 Feb 17).

Joint Publication 1.“Doctrine for the Armed Forces of the United States, 23 Mar 13, Defense Technical Information Center, http://www.dtic.mil/doctrine/new_pubs/jp1.pdf (accessed 28 Jan 17).

Jones, S. (2016). “Cyber espionage: A new cold war?” FT.Com, Retrieved from

http://aufric.idm.oclc.org/login?url=http://search.proquest.com.aufric.idm.oclc.org/docview/1820518857?accountid=4332 (accessed 18 Sept 16).

Kramer, Andrew. "Russia Updates Plan to Counter Cyberattacks and Foreign Influence," New York Times, 6 Dec 16, https://www.nytimes.com/2016/12/06/world/europe/russia-putin-cyberattacks.html?_r=0 (accessed 28 Jan 17).

Markoff, John and Bergman Lowell."Internet Attack is Called Broad and Long Lasting," The New York Times,10 May 2005, http://query.nytimes.com/gst/fullpage.html?res=9906E4DF1330F933A25756C0A9639C8B63&pagewanted=all (accessed 21 Jan 17).

Moore, Johannes. School of Advanced Air and Space Studies, " From Conception to Birth: The Forces Responsible For AFCYBER'S Evolution," June 2014, www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA626419 (accessed 21 Jan 17).

Nakashima, Ellen. "U.S. military has launched a new digital war against the Islamic State," Washington Post, 15 July 2016, https://www.washingtonpost.com/world/national-security/us-militarys-digital-war-against-the-islamic-state-is-off-to-a-slow-start/2016/07/15/76a3fe82-3da3-11e6-a66f-aa6c1883b6b1_story.html?utm_term=.1bb32f93a5ca (accessed 18 Feb 17).

National Security Agency. "Frequently Asked Questions," 28 Jun 16, https://www.nsa.gov/about/faqs/about-nsa-faqs.shtml (accessed 28 Jan 17).

National Security Agency. "Curt Dukes (IAD) - Overview of NSA's Cyber Security Mission," News Stories,1 Oct 15, https://www.nsa.gov/news-features/news-stories/2015/in-discussion-with-curt-dukes.shtml (accessed 11 Feb 17).

National Security Agency. "The National Security Agency: Missions, Authorities, Oversight and Partnerships," https://www.nsa.gov/news-features/press-room/statements/2013-08-09-the-nsa-story.shtml (accessed 4 Feb 17).

Public Law 99-145, Section 1223, "Department of Defense Authorization Act, 1986," US Government Publishing Office, https://www.gpo.gov/fdsys/pkg/STATUTE-99/pdf/STATUTE-99-Pg583.pdf (accessed 14 Jan 17).

Office of the National Counterintelligence Executive, "Foreign Spies Stealing US Economic Secrets in Cyberspace," Report to Congress on Foreign Economic Collection and Industrial Espionage, Oct 2011, https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (accessed 21 Jan 17).

Pellerin, Cheryl. "Rogers Discusses Near Future of U.S. Cyber Command," U.S. Department of Defense News, 24 Feb 17, https://www.defense.gov/News/Article/Article/1094167/rogers-discusses-near-future-of us-cyber-command (accessed 25 Feb 17).

Ramsby, C. M., USAF., & Yannakogeorgos, P. A. (2016). “A reality check on a cyber force,” Strategic Studies Quarterly, 10(2), 116-133. Retrieved from http://aufric.idm.oclc.org/login?url=http://search.proquest.com.aufric.idm.oclc.org/docview/1793664601?accountid=4332 (accessed 18 Sept 16).

Rogin, Josh. “Cyber officials: Chinese hackers attack 'anything and everything,” FCW.com,13 Feb 2007, https://fcw.com/articles/2007/02/13/cyber-officials-chinese-hackers-attack-anything-and-everything.aspx (accessed 21 Jan 17).

U.S. Strategic Command (USSTRATCOM) Factsheet. “U.S. Cyber Command (USCYBERCOM),” 20 Sep 16, ttp://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/ (accessed 28 Jan 17).

The White House. “Executive Order: Further Amendments to Executive Order 12333, United States Intelligence Activities,” News & Policies, July 2008, http://georgewbush-whitehouse.archives.gov/news/releases/2008/07/20080731-2.html, accessed 15 Oct 16.

Theohary, Catherine A. and Rollins, John W. “Cyberwarfare and Cyberterrorism: In Brief,” Congressional Research Service Report, 27 Mar 15.

TIME Magazine. “U.S. Counterintelligence Chief Not Convinced China Has Halted Espionage.” Time.Com [serial online]. November 19, 2015, available from: Military & Government Collection, Ipswich, MA.

United States Code Title 10 § 9027. “Civilian special agents of the Office of Special Investigations: authority to execute warrants and make arrests,” https://www.law.cornell.edu/uscode/text/10/9027 (accessed 4 Feb 17).

United States Code Title 10 § 164. “Commanders of combatant commands: assignment; powers and duties,” Cornell University Law School, Legal Information Institute, https://www.law.cornell.edu/uscode/text/10/164 (accessed 11 Feb 17).