REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
04/15/2016	Master's of Military Studies	SEP 2015 - APR 2016

4. TITLE AND SUBTITLE
Stacking Cybersecurity: Crossing the Virtual to Physical Incident Investigation Threshold

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Duncan, Patrick E. Major, USMC

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

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

10. SPONSOR/MONITOR'S ACRONYM(S)
Dr Matthew Flynn
LtCol Douglas Lemott

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

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The official designation of cyberspace as an operational domain and the recent DoD-wide efforts to develop and defend a Joint Information Environment create the need for dynamic and effective capabilities, which do not currently exist. The Marine Corps must recognize the emerging threats, both internal and external, and outpace them to ensure its ability to employ the right force at the right place at the right time. This paper outlines current deficiencies and several solutions for the Marine Corps to expand its organic capability and capacity for a layered defense-in-depth of the MCEN, specifically through leverging counterintelligence authorities in support of cybersecurity.

15. SUBJECT TERMS
Cyber; Cyberspace; Cybersecurity; Intelligence; Counterintelligence; Investigation.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
					19b. TELEPHONE NUMBER *(Include area code)*
Unclass	Unclass	Unclass	UU	32	(703) 784-3330 (Admin Office)

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: STACKING CYBERSECURITY – CREATING A CULTURE OF COMPLIANCE AND CROSSING THE VIRTUAL TO PHYSICAL INCIDENT INVESTIGATION THRESHOLD

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

AUTHOR:

Major Patrick Duncan, USMC

AY 15-16

Mentor and Oral Defense Committee Member: _____
Approved: _____
Date: _____ 4/13/16

Oral Defense Committee Member: _____
Approved: _____
Date: 4/13/16

Executive Summary

Title: Stacking Cybersecurity – Creating a Culture of Compliance and Crossing the Virtual to Physical Investigation Threshold

Author: Major Patrick Duncan, United States Marine Corps

Thesis: The Marine Corps must develop a process for MARFORCYBER to hold policy violators accountable, a mechanism to track individual users' record of non-compliant activities, and develop the capability and capacity to leverage counterintelligence authorities to enhance its ability to identify and investigate incidents affecting the Marine Corps Enterprise Network.

Discussion: In 2015, the Marine Corps Network Operations Security Center (MCNOSC) reported 4,643 cyberspace incidents affected the Marine Corps Enterprise Network (MCEN). MCNOSC defines an incident as an assessed occurrence having actual or potentially adverse effects on an information system. The volume of annual incidents exceeds MCNOSC's capacity to effectively investigate and attribute the source of each incident. Additionally, there is currently no process to empower MARFORCYBER to hold MCEN users accountable for violations of DoD and SECNAV Computer Network Defense policies. This in turn forces both organizations to rely on a policy violator's respective command or the local Regional Network Operations Security Center to counsel policy violators and provides no means to track repeat violators or actions taken against violators. This adversely affects MCNOSC's ability to perform logical security of the MCEN and increases the ability for adversaries to penetrate its networks. Logical Security is an emerging concept that encompasses a blend of physical security, counterintelligence activities, cybersecurity, and insider threat mitigation unique to the cyberspace domain.

Conclusion: The Marine Corps must fight to acquire the range of service counterintelligence authorities available to all other services, and develop deliberate processes to effectively investigate cyberspace incidents in order to develop a holistic, defense-in-depth of the Marine Corps Enterprise Network and comply with Secretary of Defense guidance in the 2015 DoD Cyber Strategy.

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.

Table of Contents

Figures

Page

Introduction

Every US Marine, whether indoctrinated through boot camp or Officer Candidate School, understands they serve as a basic rifleman or rifle platoon commander. A primary tenet of this baseline training instills basic weapons handling procedures, weapons safety, and weapons maintenance into every recruit and candidate. It is ingrained throughout training because their rifles are an extension of themselves through these training evolutions and are either physically located on their body, under the positive control of a designated guard, or locked inside a secure, guarded armory. All three aspects of weapons handling become muscle memory, yet that mentality completely fails to register with these same Marines when it comes to another mission-essential system most use every day, their individual workstations. The bottom line is that "cyber" does not register to military personnel as a potential weapon system, even as that technology is critical to completing essential tasks related to command and control, logistics, and personnel services, and provides a unique ability to affect each warfighting domain.

Why is this? First, there is an existing cultural assumption that cybersecurity is solely the responsibility of unit system administrators or the service's Computer Network Defense Service Provider (CNDSP), not the responsibility of unit leadership or the individual user. Second, there is no culture of compliance or effective means to hold leaders or individual users accountable for negligence or lack of adherence to existing DoD cybersecurity policies and directives. These gaps create vulnerabilities that adversaries can exploit and can directly impact mission success. This paper first calls attention to the Marine Corps' lack of ability to hold individual users accountable for lack of compliance to existing policies and regulations. Second, it highlights the Marine Corps' lack of capability and capacity to leverage existing counterintelligence (CI) authorities to conduct investigations into anomalies, a failing that puts the Marine Corps at risk.

The other services, including the US Coast Guard, recognize the Secretary of Defense's tasking and its individual service necessity to leverage CI authorities to conduct holistic investigations of network anomalies and attribute them to physical personas.

The Marine Corps is lagging behind the other services and needs to catch up. It can do this by implementing any of the multiple recommendations in this paper, such as developing and implementing an effective incident response process, publishing summaries of confirmed policy violations at each Marine Corps Installation Command (MCICOM), or development of an organic service capability similar to the U.S. Army's Cyber Crime Investigative Unit (CCIU). The Marine Corps must address these shortfalls, but even doing so will not affect the same mindset afflicting all services and the private sector, a sloppy user disregarding basic adherence to proper cybersecurity practices. This issue exists across the DoD and the private sector. While some of the services are mitigating this problem, the Marine Corps is not there yet and ultimately, commanders will likely need to feel the pain of losing network access for this culture to truly change.

While a slow process, the Marine Corps must overcome this cultural deficiency to safeguard the basic information flow required to conduct and manage each warfighting function in today's information environment. This paper provides the initial research to eliminate seams in service and joint efforts to enhance cybersecurity. First, this paper gives an overview of the most recent and relevant DoD initiatives to bring attention to and mitigate identified deficiencies. Second is a brief overview of the Marine Corps' CNDSP, the Marine Corps Network Operations Security Center (MCNOSC). Third is an overview of the current cyber threats affecting DoD-wide, Marine Corps, and private sector networks to outline the scale of user-induced vulnerabilities due to poor security practices. Fourth is an overview of service counterintelligence authorities in the

cyberspace domain and the method each service cyber component leverages those authorities. Finally, this paper provides three near-term and one long-term recommendation the Marine Corps can improve organic cybersecurity efforts and better adhere to existing DoD directives.

DoD Cybersecurity Source Documents and Initiatives

The overarching DoD instruction on cybersecurity, DoDI 8500.1, *DoD Cybersecurity*, references 106 different policies and orders, which is difficult for any service CNDSP to navigate through, let alone ensure and enforce compliance to them. In 2011, the Secretary of Defense (SecDef) officially included cyberspace as the fifth operational domain to enable the organizing, training, and equipping of the military's cyber forces. Each service has worked to enhance its organic network defense capabilities and capacities, which are individual efforts due to the reliance on separate Computer Network Defense Service Providers (CNDSP) to manage its network infrastructure and services. Since 2015, the DoD developed four mutually supporting efforts to increase effectiveness of computer network defense (CND) in order to standardize network architecture and processes across the DoD: the publication of the 2015 DoD Cyber Strategy, the re-establishment of the Defense Information Security Agency (DISA) as Joint Force Headquarters (JFHQ)-DoD Information Network (DoDIN), the 2015 DoD Cybersecurity Culture and Compliance Initiative (DC3I), and the establishment of the Directive Authorities for Cyberspace Operations (DACO). Despite being a difficult and lengthy endeavor, the result will be a streamlined, whole of government capability to protect the DoDIN from both internal and external threats. The following sections provide an overview of these recent efforts to show how the DoD intends to enhance its cybersecurity posture.

2015 DoD Cyber Strategy

The 2015 DoD Cyber Strategy serves as the SecDef guidance to the services for operating in cyberspace by outlining five strategic goals and three primary missions. One of its primary goals is to defend both the DoD Information Network (DoDIN) and service-owned networks, systems, and information. In direct conflict with this mission is the fact the private sector owns and operates over 90 percent of the infrastructure and networks used by the government.[1] To mitigate this the Secretary of Defense directs the development of a holistic defense that includes extensive coordination, partnerships, and information sharing with private sector companies and interagency partners to include law enforcement, intelligence, counterintelligence, and policy organizations.

Of the SecDef's five strategic goals, the second goal to "defend the DoD Information Network, secure DoD data, and mitigate risks to DoD missions" is directly applicable to defensive cyberspace operations (DCO) enhancement. Furthermore, two key elements of this goal will greatly assist the efforts of DCO personnel if properly utilized/integrated: (1) build the Joint Information Environment (JIE) single security architecture and (2) Use DoD counterintelligence capabilities to defend against intrusions.

The intent of the JIE is to provide Joint Force Headquarters (JFHQ)-DoDIN a feasible means to coordinate network defense through a manageable network architecture by reducing the complexity of the network and enabling real-time situational awareness of threats to the network. This replaces the current, disparate efforts of each service managing its own unique networks with a unified DoD enterprise network, which reduces the attack surface of the DoDIN. According to the DoD Cyber Strategy, a unified network will not only ensure standardization in acquisition, operation, and defense; it will reduce modernization costs, increase awareness of

user-level activity across the enterprise, and minimize complexity for synchronizing DCO response actions when required.[2]

The SecDef tasks each military department to develop a strategy that maximizes the capabilities and authorities of its respective counterintelligence agencies to identify, attribute, and defend against cyber intruders. The SecDef also recognizes that service counterintelligence authorities are "uniquely positioned to improve our insight into and frustrate and defeat cyber espionage."[3] Based on this, he tasks each military department's counterintelligence agency to collaborate with external intelligence community and law enforcement agencies specifically to enhance investigations into cyber incidents and conduct human intelligence and technical operations to thwart cyber-enabled intellectual property theft. Currently, each service outlines its plan to incorporate counterintelligence activities as part of its respective service cyber strategies, with the exception of the Department of the Navy. In fact, the term "counterintelligence" does not appear in the US Fleet Cyber Command / TENTH Fleet 2015-2020 Strategic Plan, which could indicate its lack of intent to leverage counterintelligence authorities as part of its cybersecurity strategy.[4]

Directive Authorities for Cyberspace Operations (DACO)

In an effort to create unity of effort across the DoDIN, the SecDef re-established DISA as JFHQ DoDIN. While the major concepts and exact mission are still in development, it was also given the authority to order a DoD component to remove a system from the DoDIN if it is deemed a threat to its ability to effectively command and control its networks. This authority is titled the Directive Authorities for Cyberspace Operations (DACO). It is currently considered "ill-defined," but it provides JFHQ DoDIN a means to achieve unity of effort for DCO by

providing a single DoD authority the ability to order any DoD organization to perform a wide range of tasks affecting the DoDIN, including incident response.[5]

Department of Defense Cybersecurity Culture and Compliance Initiative (DC3I)

The DoD recognizes there is an inherent lack of cybersecurity policy compliance and accountability for violations of policy by both individual users throughout the workforce and system administrators. The DC3I, published in September 2015, is a SecDef and Chairman of the Joint Chiefs of Staff (CJCS) initiative to transform this culture of non-compliance and lack of accountability. This culture shift is necessary at all levels, from the employment of proper cyber hygiene by units and individual users to the accountability of senior leadership for the cybersecurity performance of his or her organization. Workforces must receive training that enables them to identify indicators of suspicious activity and develop an attitude of questioning related activity rather than merely accepting it. Simultaneously, as this culture of compliance and questioning attitude is developed, "both IT professionals AND leaders must immediately and aggressively investigate where and why the incident occurred,"[6] similar to the negligent discharge of a kinetic weapons system. Together, these initiatives represent the most recent priorities of focus to improve cybersecurity across the DoDIN.

The Marine Corps Network Operations and Security Center

The Marine Corps Network Operations and Security Center (MCNOSC) is the Marine Corps' Computer Network Service Provider (CNDSP) and serves as the service's Global Network Operations Security Center (GNOSC) for the Department of Defense (DoD). MCNOSC's mission is to direct global Network Operations (NETOPS), to include Computer Network Defense (CND) of the Marine Corps Enterprise Network (MCEN). As part of this

mission, it is responsible for intelligence gathering and analysis to develop and enhance defensive capabilities and are tasked to provide technical support Marine Corps and joint forces operating across the globe. The MCNOSC is under the operational control of US Marine Corps Forces Cyberspace Command (MARFORCYBER) and supports its operational requirements to enhance freedom of action across all warfighting domains while denying the efforts of adversaries to degrade or disrupt this advantage through cyberspace.[7]

The Defensive Cyberspace Operations Section (DCOS) within the MCNOSC oversees and manages CND activities. Its key tasks include defense of the MCEN, collecting and sharing DoD Information Network (DoDIN) situational awareness, reporting and directing actions that proactively address threats and vulnerabilities, and response to operational incidents affecting the MCEN. As the frontline of a layered defense in depth, DCOS identifies, investigates, and reports all anomalies affecting the MCEN based on the CJCS Manual 6510.01B – *Cyber Incident Handling Program* (CIHP). The CIHP tasks the MCNOSC to provide three CND services: (1) protect; (2) monitor, analyze, and detect; and (3) respond. Despite robust efforts to meet the challenges of both network threats and adherence to DoD policies and regulations, MCNOSC lacks a robust capability to conduct end-to-end investigations that cross both virtual and physical boundaries of cyber threats. The capacity to conduct robust investigations is necessary in order to identify the true intent of the threat, attribute the threat to a specific actor, or to operationalize events when the opportunity exists.

Overview of Current Cyber Threats and Poor Cybersecurity Practices

Cyber Threats Affecting the DoD Information Network

Human error, usually stemming from a lack of compliance to policies and regulations, is a systemic issue throughout the DoD. Despite this, service efforts to mitigate attempts to penetrate

and exploit networks from external threats are increasingly effective. The DC3I highlights the DoD's ability to mitigate intrusion attempts, stating "less than 0.1 percent of the 30 million known malicious intrusions on DoD networks between September 2014 and June 2015 compromised a cyber system."[8] Despite these improvements, unauthorized intrusions still occur by nefarious actors in large part due to end-user deficiencies within the DoD:

> Roughly 80 percent of incidents in the cyber domain can be traced to three factors: poor user practices, poor network and data management practices, and poor implementation of network architecture. Thus, technical upgrades and cyber organizational changes are only part of the equation when it comes to protecting the DoDIN. A separate and significant challenge is identifying and protecting against harm due to human error by both IT professionals and the great number of everyday DoD users.[9]

This theme of user-induced vulnerabilities due to poor cyber hygiene is the focus for purposes of this paper.

Cyber Threats Affecting the Marine Corps Enterprise Network

During Calendar Year (CY) 2015, the MCEN averaged 62 million "raw" events per day. MCNOSC detected these events through multiple sensing technologies to include firewalls, Intrusion Prevention Systems (IPS), Host Based Security Systems (HBSS), and Anti-Virus software. Of these events, MCNOSC conducted detailed analysis of 4,643 events and reported them in accordance with the CIHP.

These incidents primarily fall into four of the nine incident categories established in the CJCS Instruction 6510.01F, *Information Assurance and Support to CND* as seen in Figure 1 and Appendix A.[10] Category 3 events (Unsuccessful Access Attempt – 1,943 incidents) consist of unattributed intrusion attempts stopped due to a properly functioning defensive measure such as an HBSS, anti-virus, or "signature prevention software." Category 5 events (Poor Security or Non-Compliance – 1,857 incidents) consist of cross-domain violations (CDV), the introduction of un-approved software, use of unauthorized peer-to-peer (P2P) services, or a system with

outdated patches. Category 7 events (Malware – 127 incidents) consist of a system infection due to introduction of external media and an assortment of authorized and unauthorized web browsing or web mail activity. Category 9 events (Explained Anomaly – 776 incidents) consist of suspicious activity determined to be legitimate network or host traffic following an assessment with DCOS oversight.[11] Ultimately, it is unrealistic for DCOS personnel to prevent every attempt to penetrate the MCEN, but these metrics show that a minimum of 43% of network vulnerabilities result from Category 5 and 7 events due to poor user security practices, non-compliance to cybersecurity policies, or malware introduced through user activity.

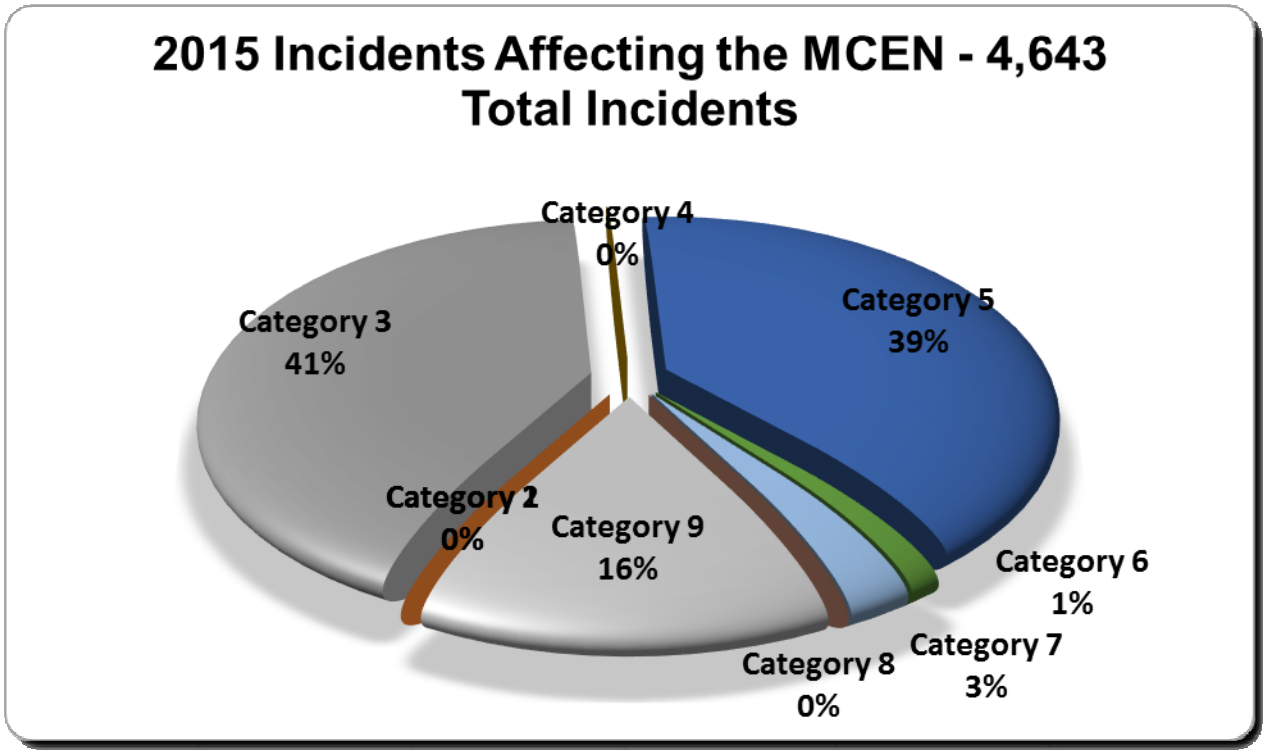


Figure 1 – Incidents Affecting the MCEN

Additionally, of these incidents, it may be of significance that the highest rate of incidents occur within the Regional Network Operations Security Center (RNOSC) – Pacific, where the rate of incidents is .41 per workstation, almost double the rate of .23 incidents per workstation at the next highest, RNOSC – Atlantic. The RNOSCs are integrated into the DCOS Incident

Management Process and provide Network Operations oversight, approval authorities, and tasking/reporting frameworks in their respective areas of responsibility.[12]

Cyber Threats Affecting the Private Sector

The range of threats the DoD faces is neither unique nor distinct from the range of threats affecting the private sector. The second annual *Cyberthreat Defense Report*, from the CyberEdge Group, presents the results of a survey provided to 814 qualified Information Technology (IT) security decision-makers and practitioners from organizations with over 500 employees, representing 19 unique industries within North America and Europe. To ensure a common baseline for the survey participants, the CyberEdge Group considered a cyber threat, "any type of malicious activity or actor that leverages computers and networks to adversely impact other computers and networks, to include everything from well-known forms of malware (e.g., viruses, worms, and Trojans) to malicious insiders and targeted attacks."[13] The results of the survey showed distinct commonalities with the range of threats faced by DoD and at the service level by MCNOSC, which inhibit DCO personnel from defending against cyber threats.

The primary concern of IT security practitioners for both surveys to date was "low security awareness among employees." This also mirrors metrics provided by the prominent cybersecurity firm, Kaspersky, which states human error is the cause of approximately 80% of all cyber incidents.[14] Low security awareness or adherence leads to users visiting unsecure public websites, opening suspicious email attachments, and revealing personal information that could enable a nefarious actor to engineer a user's system access credentials. Ultimately, this lack of adherence to local IT security policies increases the amount of self-induced white noise IT security practitioners must sift through to identify and investigate deliberate malicious threats. The DC3I serves as the DoD's effort to address this issue and increase user-level awareness of

the vulnerabilities induced by lack of adherence to cybersecurity policies and directives. Just as the U.S. military has led the national effort on issues such as desegregation, it will do so again with cybersecurity awareness.

In order to combat threats caused by lack of adherences to security policies, 32% of survey participants stated they plan to incorporate a dedicated threat intelligence service to reinforce existing defenses and better plan future security strategies and investments during 2015.[15] The use of threat intelligence services is a means to advance a "relatively immature" aspect of the IT security framework, which is the end-to-end investigation of cyber threats in order to identify the intent of the threat and attribute the threat to a specific actor. Currently, it is common for IT security professionals in both the DoD and the private sector to simply detect and block threats, with maintaining operational functionality of networks serving as the primary end state. This aspect of investigating a cyber threat is a critical point addressed later in this essay, as these are capabilities authorized by DoD counterintelligence authorities and achievable through DoD counterintelligence activities.

DoD Counterintelligence Authorities in the Cyberspace Domain

Intelligence Community CI entities are responsible for identifying, deceiving, exploiting, disrupting, countering, or neutralizing malicious cyber activity by foreign powers, organizations, persons, their agents, or international terrorist organizations. The CI cyber mission also includes countering threats to the U.S. Government supply chain and threats from trusted insiders, additional threat vectors that create risks to CND.[16] According to DoD Directive 5240.2, *DoD Counterintelligence* (CI), counterintelligence activities shall be undertaken to detect, identify, assess, exploit, and counter or neutralize the intelligence collection efforts, other intelligence activities, sabotage, terrorist activities, and assassination efforts of foreign powers, organizations,

or persons directed against the Department of Defense, its personnel, information, materiel, facilities and activities.[17] The unique authorities of service counterintelligence agencies enable them to conduct investigations of network intrusions to attribute and identify motivations of threat actors such as foreign intelligence entities (FIE), violent extremist organizations (VEO), hacktivists, criminal organizations, or insider threats. These authorities also enable them to conduct a range of activities to counter physical and virtual espionage of the DoDIN and the information residing on it. DoDD 5240.06, *Counterintelligence Awareness and Reporting*, includes Table 3 (See Appendix B), "Reportable FIE-Associated Cyberspace Contacts, Activities, Indicators, and Behaviors" and tasks the Heads of DoD Components to not only report indicators outlined in Table 3, but to administer appropriate judicial, administrative, or punitive action to military or civilian personnel who fail to report identified threats.

Unfortunately, this effort is only effective if users, command staff, and network administrators are aware this specific directive and table of indicators exists, yet another aspect of the human error that enables network vulnerabilities. The incorporation of counterintelligence personnel onto the tables of organization (T/O) of cyber-related military organizations will ensure awareness these directives exist and serve as a layer of defense in support of CND.

Service Counterintelligence Support to Cybersecurity

The US Army, Air Force, and Coast Guard specifically address the use of their CI agencies to counter cyber threats in its respective service cyber strategies under the authorities of its Military Department Counterintelligence Agencies (MDCA). The Marine Corps is the only service that does not have an MDCA, therefore the DoN MDCA serves as the CI Executor for Marine Corps counterintelligence activities. SECNAV 3850.2C, *DoN Counterintelligence*, tasks the Director, Naval Criminal Investigative Service (NCIS) to "direct, manage and control the

execution of all DoN CI functions, to include primary responsibility for CI investigations and operations, except those functions within the responsibility of the Commandant Marine Corps via the Director of Intelligence."[18] These functions are limited to the conduct of CI collection, CI preliminary inquiries, and liaison with U.S. and foreign officials in support of deployed and deploying Marine Corps forces, but do not authorize credentialed Marine Corps CI agents to conduct CI investigations or operations. The ability to conduct CI investigations and operations is critical to effectively defend against physical and virtual network intrusions and meet the intent of the 2015 DoD Cyber Strategy, but the Marine Corps can only conduct these activities when approved and directly managed by NCIS. In order to meet the SecDef's direction in the 2015 DoD Cyber Strategy, the Marine Corps must have a means to protect its own equities, rather than competing with DoN priorities and the NCIS capacity to support.

U.S. Army Cyber Crime Investigative Unit

According to the U.S. Army's *LandCyber White Paper (2018-2030),* counterintelligence specialists, along with counter-reconnaissance and cyber hunt teams, "will work inside the Army enterprise to actively search for and locate threats that have penetrated the Army enterprise."[19] A significant player in the Army's holistic CND effort is the Computer Crime Investigative Unit (CCIU). The CCIU uses an array of specialists, including attorneys, counterintelligence (CI) agents, forensic examiners, technical analysts, and information assurance technicians to provide technical assistance and guidance to external Army Criminal Investigation Command field office investigations involving computers. Its primary mission is "to conduct worldwide criminal investigations of intrusions and related malicious activities, including insider threats, involving U.S. Army networks, personnel, and data."[20]

The CCIU also provides forensic assistance and vulnerability assessments from CCIU special agents who receive advanced technical training from the Defense Cyber Investigations Training Academy (DCITA) to process and analyze digital evidence. This technical training is critical to collect and maintain the integrity of forensic data in a manner that will stand up as evidence in a court of law. The vulnerability assessments are part of a new Cyber Crime Prevention Program that identifies vulnerabilities in networks that create "crime-conducive conditions," which the respective army commander must proactively address to prevent malicious network activity. Additionally, the CCIU progressively integrates CI agents based on the unique authorities it can bring to bear in the identification, investigation, and potential attribution of a malicious activity on a network. Based on the increased demand signal of investigation involving, or related to cyberspace, the CCIU is doubling the number of CI agents supporting its investigations.[21] The success of the CCIU assisted in solving a glaring weakness in Army CND efforts and serves as a model for each service to replicate. Additionally, the capability the CCIU provides should become a function within JFHQ-DoDIN's JIE construct and serve as a strategic CND capability.

US Air Force Office of Special Investigations

The Air Force Office of Special Investigations (AFOSI) serves as a federal law enforcement, investigative, and counterintelligence agency. Its blend of authorities makes them particularly effective in countering cyber threats. AFOSI is the only organization in the Air Force authorized to investigate intrusions or sabotage of service-owned computer networks and to conduct cyber CI operations.[22] In addition, the Air Force serves as the Executive Authority for the Defense Cyber Crimes Center (DC3), established in 1998. DC3's mission is to conduct digital forensics and cyber analytics in support of information assurance, critical infrastructure protection (CIP), law enforcement and counterintelligence, document and media exploitation, and

counterterrorism. DC3 also manages the only government organization dedicated solely to cyber investigations training and certification, DCITA, which serves as a defacto Center of Excellence for most DoD and federal agencies. Based on these assets, the Air Force is also a critical component to enable a truly Joint enterprise in leveraging CI authorities and activities in support of CND.

Coast Guard Criminal Investigative Service and Counterintelligence Service

Similar to AFOSI, the Coast Guard has multiple authorities that enable them to serves as a federal law enforcement, investigative, and counterintelligence agency with a focus on activities within the maritime domain and within the service itself. As outlined in the 2015 Coast Guard Cyber Strategy, the Coast Guard Criminal Investigative Service (CGIS) will seize and exploit digital information systems, conduct legally sanctioned cyber activities to preserve evidence of illegal activity, and supports investigations into criminal cyber activity targeting or originating in Coast Guard networks or by uniformed members of the Coast Guard. The Coast Guard Counterintelligence Service will conduct cybersecurity investigations and operations to identify and prevent FIE efforts to exploit Coast Guard networks and systems. As part of its investigation methodology, the Coast Guard will conduct forensics analysis to determine the methods and paths of malicious activity, determine the impact to infrastructure, provide evidence for prosecution, inform the development of countermeasures, and inform DCO personnel. In addition to cybersecurity investigations, it is also responsible for analyzing and managing risks to the Coast Guard information and communications supply chain. Specific to the human aspect, CGIS will deter malicious insiders and advance individual accountability by ensuring that members of its workforce are subject to administrative or judicial action if they knowingly,

willfully, or negligently compromise the security of Coast Guard information systems or violate information system security policies.[23]

Department of the Navy / Naval Criminal Investigative Service Support to Cyberspace

According to SECNAV 3850.2C, counterintelligence is critical to the protection of Navy and Marine Corps forces, operations, information, facilities, equipment and networks from attack and the intelligence activities of foreign governments and international terrorist organizations. SECNAV 5430.107, *Missions and Functions of the NCIS*, tasks NCIS with primary jurisdiction within the DoN for certain cyber-related functions as they apply to DoN computer networks, to include infrastructure protection operations and cyber-related criminal investigations regarding unauthorized access, intrusion, denial of service, or viruses/malicious code. Additionally, it tasks NCIS to maintain a staff skilled in investigations of computer crime.

Another authoritative document, SECNAV 5239.3B, *Department of the Navy Information Assurance* Policy, directs that "NCIS maintains investigative authority for criminal acts or espionage related to computer network security incidents, and coordinates information regarding such incidents with the law enforcement counterintelligence community."[24] In it, DoN Chief Information Officer (CIO) tasks the Director, NCIS, with the following:

> (1) Conduct all investigations regarding operations, proactive programs, and related analyses of cyber incidents and targeting involving DoN IT assets.
>
> (2) Collect, track, and report threats to DoN IT assets and disseminate this information to other law enforcement agencies, Department of Defense,

Department of the Navy, DoN CIO, and other national agencies, as needed.

(3) Conduct cyber-related criminal investigations regarding root level intrusions, user level intrusions, denial of service, malicious logic incidents, and aforementioned suspected incidents (Categories 1, 2, 4, and 7). Provide recommendations based on analysis of forensics to the DoN CIO for incorporation into potential IA/CND policy.

(4) Investigate fraud, waste, abuse, and other criminal violations involving DoN IT.

(5) Maintain a staff skilled in the investigation of computer crime. The staff should be sufficient in size to handle multiple major incidents and respond to increasing demands of the DoN.

Marine Corps Counterintelligence Support to Cyberspace

The DoN is the only service that does not address the use of NCIS or include the term "counterintelligence" in its service cyberspace component's strategic plan for cyberspace operations.[25] Conversely, the Marine Corps addresses CI support to cyberspace operations in two recent Marine Corps Orders (MCO). MCO 5239.2B, *Marine Corps* Cybersecurity, states the requirement to inform the appropriate chain of command, LE, or CI agency, cyber-related activities affecting Marine Corps operations such as unusual network activities; violations of Federal, DoD, DON, and Marine Corps cybersecurity policies; and criminal acts conducted on Marine Corps IT resources. It also directs the Marine Corps Director of Intelligence (DIRINT) to provide Marine Forces with service-level intelligence support of foreign cyber intelligence

threats.[26] MCO 3100.4, *Cyberspace Operations*, directs the DIRINT to "develop plans and policies to conduct counterintelligence activities in support of cyberspace operations...while affording Marine Corps operating forces and garrison commanders, to the greatest extent possible, the authority to conduct intelligence, surveillance, and reconnaissance (ISR) operations in and through cyberspace."[27] Additionally, it states to ensure counterintelligence mechanisms for cyberspace operations are in place in accordance with general guidance for CI activities outlined in SECNAV 3850.2C. The Marine Corps clearly recognizes the importance of adhering to SecDef guidance and leveraging CI activities to support full spectrum cyberspace operations, but lacks the service-level authorities to leverage its organic CI capacity.

Recommendations

Despite the recent efforts by the DoD to increase its ability to mitigate threats across the information environment through its 2015 Cyber Strategy, the creation of JFHQ-DoDIN and DACO authorities, and the DC3I initiative the Marine Corps must conduct organic efforts to remain proactive vice reactive to the evolving range of threats. The following recommendations outline both short-term and long-term solutions the Marine Corps can implement to combat threats affecting the MCEN. These recommendations require further research to outline the legal and policy requirements inherent to each effort.

1. Develop an effective incident response process.

The first short-term recommendation is the development of an effective incident response process that includes reporting procedures, reporting chains, investigation requirements, measures to hold policy violators accountable, and strict timelines for both MCNOSC/MFCY and the violator's parent command. Upon awareness of an incident, MCNOSC will immediately notify the appropriate senior leader at the affected command. That individual is responsible for

immediate quarantine of the workstation associated with the incident to prevent a user from accessing it physically or remotely, immediate suspension of the identified user's network privileges, and completion of a Preliminary Inquiry within a specified number of working days upon notification of the incident. The workstation should remain connected to the MCEN unless there are indications it is actively beaconing to a known or suspected command and control server. Simultaneously, the MCNOSC DCOS begins initial forensic analysis to determine the root cause of the incident and attempt to confirm attribution of the incident's source.

If an incident meets the criteria of an activity, indicator, or behavior of a potential Foreign Intelligence Entity (FIE) outlined in Table 3 of DoDD 5240.06, MCNOSC shall forward the information regarding the incident to its local Marine Corps CI representative or NCIS within 72 hours.[28] During the life-cycle of a Law Enforcement (LE) or CI investigation, coordination and deconfliction will occur between the investigating organization and the LE/CI element at either USCYBERCOM or JFHQ-DoDIN as appropriate. Finally, the affected command will ensure the unit's Security Manager annotates the user's loss of network privileges and any additional actions in a global tracking database. This provides a mechanism to track repeat offenders and the Security Manager at future commands can identify the user as a previous policy violator when he submits a System Authorization Access Request (SAAR) for local network privileges.

2. Publish weekly summaries of confirmed violations on the Marine Corps homepage.

The second recommendation is for each RNOSC to publish a summary of confirmed violations each week on the homepage for each Marine Corps Installation Command (MCICOM) and publish a consolidated list each month on the Marine Corps homepage via the Commandant Marine Corps Public Affairs Office. Additionally, MCNOSC/MFCY can share these summarized results with other service cyber components and JFHQ-DoDIN to provide

awareness of the frequency and types of violations occurring on the MCEN. There is a current precedent for similar actions regarding the publishing of courts-martials as outlined in MARADMIN 505/13.[29] Currently, neither MCNOSC nor MFCY have the authority to subject policy violators from an external command to punitive actions. The intent is to provide awareness to users operating on the Marine Corps portion of the DoDIN and pressure commanders to hold violators accountable at the local level.

3. Initiate a cyber pilot program between NCIS and the USMC CI/HUMINT enterprise.

The third recommendation is to initiate a pilot program between NCIS and the USMC CI/HUMINT enterprise that mirrors the Army's CCIU capability, both in garrison and deployed, to investigate incidents associated to the cyber-related activities, indicators, or behaviors outlined in DoDD 5240.06, Table 3, which is located in Appendix B. A cyber investigation is a systematic and formal inquiry into a qualified threat or incident using a full range of criminal investigative tools, including but not limited to interview techniques, surveillance, and digital forensics to determine the events that transpired and to collect evidence.[30] Based on the tailored training obtained through DCITA, these investigative teams will possess the skill sets to conduct a deliberate and thorough investigation by gathering and analyzing forensic data, maintaining a proper chain of custody, and adhering to proper incident handling techniques while preserving the integrity of forensics evidence in accordance with CJCSI requirements illustrated in Figure 2. Appendix C illustrates DCITA career tracks and curriculum. The blend of Title 10, Title 18, and Title 50 authorities resident on these teams provides them the unique ability to seamlessly continue an investigation from the virtual domain to the physical domain. Additionally, the wide ranges of operational expertise will enhance development of tactics, techniques, and procedures

as a Joint Navy/Marine Corps team to more effectively mitigate the range of cyber-related threats and meet the increasing demand signal for this type of capability.

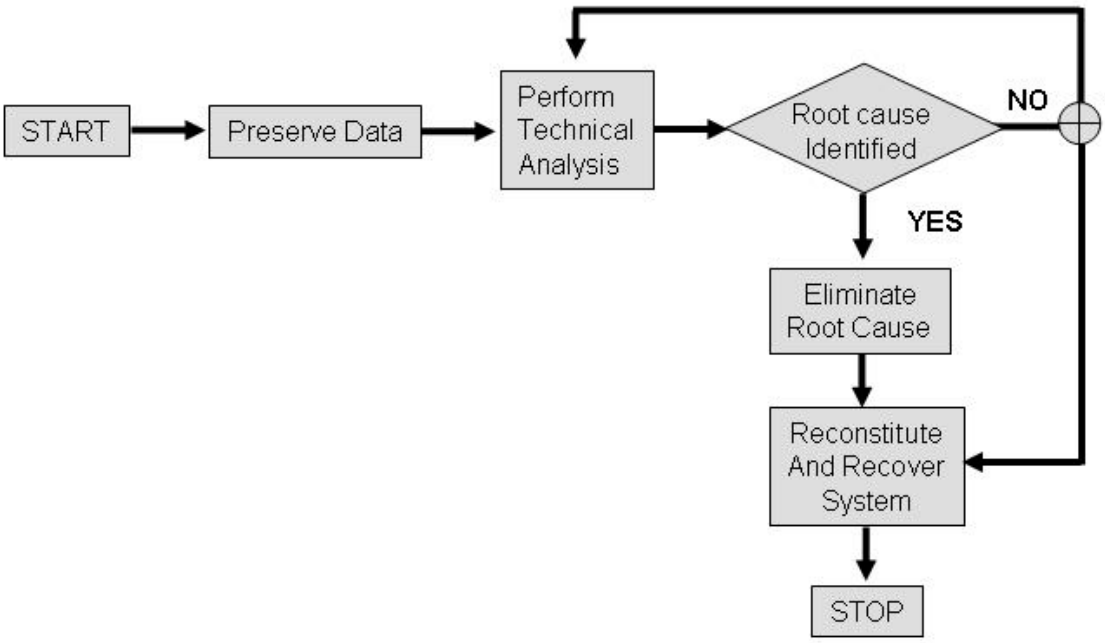


Figure 2: Cyber Incident Analysis Relationship to Preserving Data

4. Create a Marine Corps capability similar to the Army's CCIU.

The long-term recommendation involves two deliberate steps resulting in the creation of an organic Marine Corps capability similar to the Army's CCIU that is able to meet demands of the cyber domain in both in garrison and forward deployed environments. The first step is to develop and codify a training pipeline for CI/HUMINT Specialists (Military Occupational Specialty 0211) that certifies them to conduct full spectrum cyber investigations. Upon completion of specified certifications outlined below, the Marine earns an Additional MOS of 021X, which enables the Marine Corps to track and resource these unique skill sets when required. The second step is to reassess the range of counterintelligence authorities delegated by

the Secretary of the Navy to the Marine Corps to enable them the organic authorities to conduct investigations of anomalies on the MCEN.

The first step, the development and codification of a cyber training pipeline for 0211s, does not mandate a prerequisite skillset, but operational experience as a 0211 is desirable in order to apply the foundations of the CI and HUMINT disciplines to the cyberspace domain. The required training is available through DCITA, located in Linthicum, MD, but approximately one-third of the courses are available on-line, or through blended seminars. Courses are available to any active DoD service member serving in a Title 10 status and are also available to DoD or Federal agency civilians. Courses range from digital forensic investigation basics to collecting, preserving, and examining digital media in a wartime environment and enable students the ability to respond, image, process and analyze digital evidence, and properly document findings.[31]

Appendix C outlines the five career tracks available at DCITA. The Technology Track courses provide students with an understanding of technology fundamentals and focuses on basic computer hardware, operating systems, and networking theory, which serve as the foundation for cyber investigations. The Responders Track introduces students to basic forensic collection of digital evidence and provides training in first-response fundamentals, basic cyber investigative practices, and management of an investigative team. The Forensic Track focuses on the art and science of full-spectrum digital media examination and enables the skills to examine media from multiple operating system platforms in both a lab environment and a deployed setting. The Network Investigations Track focuses on foundational networking concepts, intrusion scenarios, and malware analysis through interactive, hands-on experience and provides a deeper awareness of cyber security and threat intelligence. The Cyber Counterintelligence Track focuses

specifically on improving the effectiveness of cyber counterintelligence personnel and provides the skills to protect sensitive information and process and analyze digital evidence to support the needs of counterintelligence agents.

The five tracks result in one of three DoD-recognized certifications, which should then earn the Marine an AMOS of 021(X), Cyber CI/HUMINT Specialist. The first certification, Cyber Crime Investigator, enables a credentialed law enforcement/counterintelligence person to investigate the spectrum of cyber crime, to include the examination and analysis of digital evidence. The second certification, Digital Forensics Examiners, specialize in the analysis of digital media. The third certification, Digital Media Collector, serve as first-responders to a scene in order to secure, preserve and/or collect digital evidence at crime scenes. To maintain certification, personnel must conduct at least three acquisitions of digital media or information and attend a minimum of 60 hours of approved continuing education training every three years.[32]

The second step of the long-term solution, reassessment of the range of counterintelligence authorities delegated to the Marine Corps, is essential to enable the Marine Corps the organic ability to investigate and mitigate the range of cyber threats affecting the MCEN as part of a holistic CND enterprise. This requires the designation of the Marine Corps Intelligence Activity (MCIA) as a Military Department Counterintelligence Agency with responsibilities commensurate with Army CI, the Naval Criminal Investigative Service, and the Air Force Office of Special Investigations. The SECNAV has delegated the Marine Corps the authority to conduct, among other functions, CI collection and CI preliminary inquiries in support of deployed and deploying forces.[33] Joint Publication (JP) 1-02, *DoD Dictionary of Military and Associated Terms*, defines force as "an aggregation of military personnel, weapon systems, equipment, and necessary support, or combination thereof." The Marine Corps, as America's

force-in-readiness is in a perpetual state of deployment and must maintain its ability to "deploy rapidly, arrive quickly, and operate immediately, in accordance with *Expeditionary Force 21*. Additionally, DoDD 5240.2, *DoD Counterintelligence*, states CI activities should safeguard "the Department of Defense, its personnel, information, materiel, facilities, and activities."[34] The cyberspace environment is an inherent aspect to both "deployed and deploying forces" and a component of the "aggregation of military personnel, weapons systems, equipment, and necessary support," based on its definition in JP 1-02. These definitions with regard to the cyberspace domain logically meet the spirit and intent of the existing SECNAV Instruction 3850.2C and should enable the Marine Corps to expand its scope of organic CI authorities in support of service requirements. Additionally, a rewrite to the SECNAV 3850.2C has been in a draft state for several years, which makes the timing of this issue extremely relevant.

CONCLUSION

The official designation of cyberspace as an operational domain and the recent DoD-wide efforts to develop and defend a Joint Information Environment create the need for dynamic and effective capabilities, which do not currently exist. Additionally, the cyberspace domain does not register to military personnel as a potential weapon system, even as that technology is critical to completing mission essential tasks. This paper outlines current deficiencies and several solutions for the Marine Corps to expand its organic capability and capacity for a layered defense-in-depth of the MCEN. The Marine Corps must recognize the emerging threats, both internal and external, and outpace them to ensure its ability to employ the right force at the right place at the right time. Implementation of both these near-term and long-term recommendations will produce results and meet the intent of recent SecDef and CJCS directives tasked of each service. The true range of ways to leverage counterintelligence authorities in support of

cybersecurity will take years to develop, but the Marine Corps must take the necessary steps to align its organic authorities and capabilities with those of every other service. Furthermore, while other service applications to this problem set exist, the Marine Corps can rely on its history of innovation to develop new ways to ensure accountability of security violations, employ CI activities in support of cybersecurity, and apply them to the Joint Information Environment at the strategic level.

[1] US Department of Defense, *2015 Cyber Strategy*, April 2015, 5, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/

[2] DoD, *Cyber Strategy*, 18.

[3] DoD, *Cyber Strategy*, 24.

[4] U.S. Fleet Cyber Command/TENTH fleet, *Strategic Plan 2015-2020*, 2015, http://www.navy.mil/strategic/FCC-C10F%20Strategic%20Plan%202015-2020.pdf.

[5] Jared Serbu, "Pentagon Readies Standup of Regional Cyber Defense Commands," *Federal News Radio*, July 06, 2015, http://federalnewsradio.com/defense/2015/07/pentagon-readies-standup-regional-cyber-defense-commands.

[6] US Department of Defense, *Cybersecurity Culture and Compliance Initiative,* September 30, 2015, 4, http://www.defense.gov/Portals/1/Documents/pubs/OSD011517-15-RES-Final.pdf.

[7] "U.S. Marine Corps Forces Cyberspace Command," Marine Corps Concepts & Programs, accessed February 06, 2015, https://marinecorpsconceptsandprograms.com/organizations/operating-forces/us-marine-corps-forces-cyberspace-marforcyber.

[8] DoD, *Cybersecurity Culture*, 1.

[9] DoD, *Cybersecurity Culture*, __.

[10] Chairman of the Joint Chiefs of Staff, *Cyber Incident Handling* Program, Manual 6510.01B, July 10, 2012, D-2, http://www.dtic.mil/cjcs_directives/cdata/unlimit/m651001.pdf.

[11] Marine Corps Network Operations Security Center (MCNOSC), "MCEN Incident Summary," PowerPoint Presentation, Quantico, Virginia, January 06, 2016.

[12] MCNOSC, "MCEN Incident Summary."

[13] CyberEdge Group, "2015 Cyberthreat Defense Report: North America and Europe," 2015, 4, https://www.bluecoat.com/sites/default/files/documents/files/CyberEdge_2015_CDR_Report.pdf.

[14] "Kaspersky Lab," accessed February 29, 2016, http://www.kaspersky.com/enterprise-security/intelligence-services.

[15] CyberEdge, "Cyberthreat Defense Report," 11.

[16] U.S. Coast Guard, *Cyber* Strategy, June 2015, 21, https://www.uscg.mil/seniorleadership/DOCS/cyber.pdf.

[17] U.S. Department of Defense, *DoD Counterintelligence*, Directive 5240.2, May 22, 1997, 2, http://fas.org/irp/doddir/dod/dodcount.htm.

[18] Secretary of the Navy, *Counterintelligence*, Instruction 3850.2C, July 20. 2005. 5, https://fas.org/irp/doddir/navy/secnavinst/3850_2c.pdf.

[19] U.S. Army Cyber Command/2nd U.S. Army, "LandCyber White Paper: 2018-2030," September 09, 2103, 46, http://dtic.mil/dtic/tr/fulltext/u2/a592724.pdf.

[20] "Computer Crime Investigative Unit," U.S. Army Criminal Investigation Command, accessed Feb 06, 2016, http://www.cid.army.mil/cciu.html.

[21] Computer Crime Investigative Unit.

[22] Secretary of the Air Force, *Criminal investigations and Counterintelligence,* Policy Directive 71-1, November 13, 2015, 6, http://static.e-publishing.af.mil/production/1/saf_ig/publication/afpd71-1/afpd71-1.pdf.

[23] U.S. Coast Guard, *Cyber* Strategy, 25.

[24] Secretary of the Navy, *Information Assurance Policy*, Instruction 5239.3B, June 17, 2009, 5, http://www.doncio.navy.mil/ContentView.aspx?id=1121.

[25] U.S. Fleet Cyber, *Strategic Plan*.

[26] Commandant of the Marine Corps, *Cybersecurity*, MCO 5239.2B, November 05, 2015, 15, http://www.marines.mil/Portals/59/MCO%205239.2B.pdf.

[27] Commandant of the Marine Corps, *Cyberspace Operations*, MCO 3100.4, July 27, 2013, 8, http://www.marines.mil/Portals/59/Publications/MCO%203100.4.pdf.

[28] U.S. Department of Defense, *Counterintelligence Awareness and Reporting*, Directive 5240.06, May 30, 2013, 13, http://www.dtic.mil/whs/directives/corres/pdf/524006p.pdf.

[29] Commandant of the Marine Corps, *Public Release of Courts-Martial* Results, MARADMIN 505/13, September 26, 2013,

HTTP://WWW.MARINES.MIL/NEWS/MESSAGES/MESSAGESDISPLAY/TABID/13286/ARTICLE/150850/PUBLIC-RELEASE-OF-COURTS-MARTIAL-RESULTS.ASPX.

[30] U.S. Coast Guard, *Cyber* Strategy, 41.

[31] "Defense Cyber Investigations Training Academy," accessed December 28, 2015, https://www.dcita.edu/training.html.

[32] "Defense Cyber Investigations Training Academy."

[33] DoDD 5240.2, *Counterintelligence*, 6.

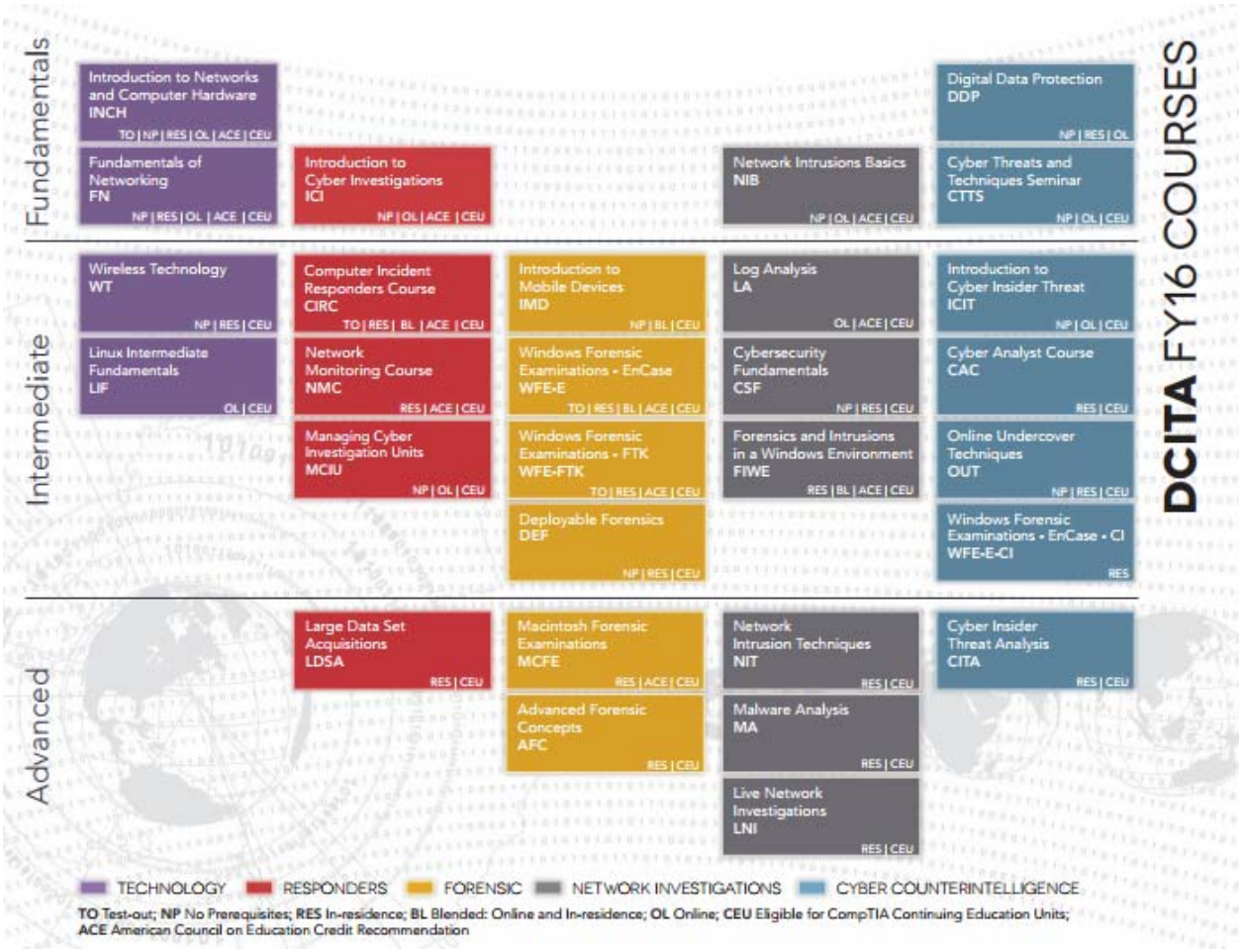
[34] DoDD 5240.2, *Counterintelligence*, 2.

Appendix A - Cyber Incident and Reportable Cyber Event Categories

Category	Description
0	**Training and Exercises**—Operations performed for training purposes and support to CC/S/A/FA exercises.
1	**Root Level Intrusion (Incident)**—Unauthorized privileged access to an IS. Privileged access, often referred to as administrative or root access, provides unrestricted access to the IS. This category includes unauthorized access to information or unauthorized access to account credentials that could be used to perform administrative functions (e.g., domain administrator). If the IS is compromised with malicious code that provides remote interactive control, it will be reported in this category.
2	**User Level Intrusion (Incident)**—Unauthorized non-privileged access to an IS. Non-privileged access, often referred to as userlevel access, provides restricted access to the IS based on the privileges granted to the user. This includes unauthorized access to information or unauthorized access to account credentials that could be used to perform user functions such as accessing Web applications, Web portals, or other similar information resources. If the IS is compromised with malicious code that provides remote interactive control, it will be reported in this category.
3	**Unsuccessful Activity Attempt (Event)**—Deliberate attempts to gain unauthorized access to an IS that are defeated by normal defensive mechanisms. Attacker fails to gain access to the IS (i.e., attacker attempts valid or potentially valid username and password combinations) and the activity cannot be characterized as exploratory scanning. Reporting of these events is critical for the gathering of useful effects-based metrics for commanders. Note the above CAT 3 explanation does not cover the "run-of-themill" virus that is defeated/deleted by AV software. "Run-of-themill" viruses that are defeated/deleted by AV software are not reportable events or incidents and should not be annotated in JIMS.
4	**Denial of Service (Incident)**—Activity that denies, degrades, or disrupts normal functionality of an IS or DoD information network.
5	**Non-Compliance Activity (Event)**—Activity that potentially exposes ISs to increased risk as a result of the action or inaction of authorized users. This includes administrative and user actions such as failure to apply security patches, connections across security domains, installation of vulnerable applications, and other breaches of existing DoD policy. Reporting of these events is critical for the gathering of useful effects-based metrics for commanders.
6	**Reconnaissance (Event)**—Activity that seeks to gather information used to characterize ISs, applications, DoD information networks, and users that may be useful in formulating an attack. This includes activity such as mapping DoD information networks, IS devices and applications, interconnectivity, and their users or reporting structure. This activity does not directly result in a compromise.
7	**Malicious Logic (Incident)**—Installation of software designed and/or deployed by adversaries with malicious intentions for the purpose of gaining access to resources or information without the consent or knowledge of the user. This **only** includes malicious code that does not provide remote interactive control of the compromised IS. Malicious code that has allowed interactive access should be categorized as Category 1 or Category 2 incidents, not Category 7. Interactive active access may include automated tools that establish an open channel of communications to and/or from an IS.
8	**Investigating (Event)**—Events that are potentially malicious or anomalous activity deemed suspicious and warrant, or are undergoing, further review. No event will be closed out as a Category 8. Category 8 will be recategorized to appropriate Category 1-7 or 9 prior to closure.
9	**Explained Anomaly (Event)**—Suspicious events that after further investigation are determined to be non-malicious activity and do not fit the criteria for any other categories. This includes events such as IS malfunctions and false alarms. When reporting these events, the reason for which it cannot be otherwise categorized must be clearly specified.

Appendix B - Reportable FIE-Associated Cyberspace Contacts, Activities, Indicators, and Behaviors	
1	Actual or attempted unauthorized access into U.S. automated information systems and unauthorized transmissions of classified or controlled unclassified information.
2	Password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading.
3	Network spillage incidents or information compromise.
4	Use of DoD account credentials by unauthorized parties.
5	Tampering with or introducing unauthorized elements into information systems.
6	Unauthorized downloads or uploads of sensitive data.
7	Unauthorized use of Universal Serial Bus, removable media, or other transfer devices.
8	Downloading or installing non-approved computer applications.
9	Unauthorized network access.
10	Unauthorized e-mail traffic to foreign destinations.
11	Denial of service attacks or suspicious network communications failures.
12	Excessive and abnormal intranet browsing, beyond the individual's duties and responsibilities, of internal file servers or other networked system contents.
13	Any credible anomaly, finding, observation, or indicator associated with other activity or behavior that may also be an indicator of terrorism or espionage.
14	Data exfiltrated to unauthorized domains.
15	Unexplained storage of encrypted data.
16	Unexplained user accounts.
17	Hacking or cracking activities.
18	Social engineering, electronic elicitation, e-mail spoofing or spear phishing.
19	Malicious codes or blended threats such as viruses, worms, trojans, logic bombs, malware, spyware, or browser hijackers, especially those used for clandestine data exfiltration.

Appendix C – Defense Cyber Investigations Training Academy Career Tracks



BIBLIOGRAPHY

Chairman of the Joint Chiefs of Staff. *Cyber Incident Handling* Program. Manual 6510.01B, July 10, 2012. http://www.dtic.mil/cjcs_directives/cdata/unlimit/m651001.pdf.

Commandant of the Marine Corps. *Cybersecurity*. MCO 5239.2B. Washington, DC, November 05, 2015. http://www.marines.mil/Portals/59/MCO%205239.2B.pdf.

Commandant of the Marine Corps. *Cyberspace Operations.* MCO 3100.4. Washington, DC, July 27, 2013. http://www.marines.mil/Portals/59/Publications/MCO%203100.4.pdf.

CyberEdge Group, "2015 Cyberthreat Defense Report: North America and Europe." Annapolis, MD, 2015. https://www.bluecoat.com/sites/default/files/documents/files/CyberEdge_ 2015_CDR_Report.pdf.

Headquarters, United States Marine Corps. *Public Release of Courts-Martial Results*. MARADMIN 505/13. Washington, DC, September 26, 2013. HTTP://WWW.MARINES.MIL/NEWS/MESSAGES/MESSAGESDISPLAY/TABID/13 286/ARTICLE/150850/PUBLIC-RELEASE-OF-COURTS-MARTIAL-RESULTS.ASPX.

Marine Corps Network Operations Security Center (MCNOSC). "MCEN Incident Summary," PowerPoint Presentation. Quantico, VA, January 06, 2016.

Secretary of the Air Force. *Criminal investigations and Counterintelligence.* Policy Directive 71-1. Washington, DC, November 13, 2015 http://static.e-publishing.af.mil/ production /1/saf_ig/publication/afpd71-1/afpd71-1.pdf.

Secretary of the Navy. *Counterintelligence*. Instruction 3850.2C. Washington, DC, July 20, 2005. https://fas.org/irp/doddir/navy/secnavinst/3850_2c.pdf.

Secretary of the Navy. *Information Assurance Policy*. Instruction 5239.3B. Washington, DC, June 17, 2009. http://www.doncio.navy.mil/ContentView.aspx?id=1121.

Serbu, Jared. "Pentagon Readies Standup of Regional Cyber Defense Commands." *Federal News Radio*, July 06, 2015. http://federalnewsradio.com/defense/2015/07/pentagon-readies-standup-regional-cyber-defense-commands.

U.S. Army Cyber Command/2nd U.S. Army. "LandCyber White Paper: 2018-2030." Fort Meade, MD, September 09, 2103. http://dtic.mil/dtic/tr/fulltext/u2/a592724.pdf.

U.S. Coast Guard. *Cyber Strategy*. Washington, DC, June 2015. https://www.uscg.mil/seniorleadership/DOCS/cyber.pdf.

U.S. Department of Defense. *Counterintelligence Awareness and Reporting.* Directive 5240.06. Washington, DC, May 30, 2013. http://www.dtic.mil/whs/directives/corres/pdf/524006p.pdf.

U.S. Department of Defense. *DoD Counterintelligence*. Directive 5240.2. Washington, DC, May 22, 1997. http://fas.org/irp/doddir/dod/dodcount.htm.

U.S. Department of Defense. *Cyber strategy*. April 2015. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

U.S. Department of Defense. *Cybersecurity Culture and Compliance Initiative.* Washington, DC, September 30, 2015. http://www.defense.gov/Portals/1/Documents/pubs/OSD011517-15-RES-Final.pdf.

U.S. Fleet Cyber Command/TENTH fleet. *Strategic Plan 2015-2020*. Washington, DC, 2015. http://www.navy.mil/strategic/FCC-C10F%20Strategic%20Plan%202015-2020.pdf.