REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
04-05-2018	Master's of Military Studies	AUG 2017 - APR 2018

4. TITLE AND SUBTITLE

Offensive Cyberspace Operational Readiness: A Usable Framework to Define Offensive Cyberspace Operational Readiness for Military Leaders

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
McMurray, Niklas, J, 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. Christopher Stowe

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

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Offensive Cyberspace Operations (OCO) are some of the most complex and dynamic military operations currently being conducted by the US military. That complexity has shrouded these operations in mystery that prevents policy and decision-makers from fully understanding current capabilities and limitations contained within this new domain. Current readiness assessment frameworks do not adequately translate these capabilities and limitations into a usable and understandable narrative and lack the specificity required to fully comprehend operational readiness of those forces. Readiness Systems such as Status of Resources and Training System (SORTS) and Defense Readiness Reporting System-Strategic (DRRS-S) capture the force readiness of US military units, but lack the fidelity to clearly define operational readiness, which is required within OCO for those assessments to be meaningful. Examples exist which highlight the complexity of cyber-weapons, from the time needed to develop weapons to the expertise required to ensure they execute as planned. Only when those nuances are captured within an operational-readiness framework can these capabilities and limitations be translated to policy and decision-makers for employment consideration.

15. SUBJECT TERMS

Cyber; Cyberspace; Cyberspace Operations; Offensive Cyberspace Operations; Readiness; Operational Readiness

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					USMC Command and Staff College
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	UU	41	**19b. TELEPHONE NUMBER** *(include area code)*
Unclass	Unclass	Unclass			(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

OFFENSIVE CYBERSPACE OPERATIONAL READINESS: A USABLE FRAMEWORK TO DEFINE OFFENSIVE CYBERSPACE OPERATIONAL READINESS FOR MILITARY LEADERS

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

MAJOR NIKLAS J MCMURRAY, USMC

AY 2017-18

Mentor and Oral Defense Committee Member: CHRISTOPHER S. STONE
Approved: [signature]
Date: 4/4/18

Oral Defense Committee Member: MATTHEW FLYNN
Approved: [signature]
Date: 4/4/18

COL HUNTER RAWLINGS
[signature]
04 APR 18

Executive Summary

Title: Offensive Cyberspace Operational Readiness: A Usable Framework to Define Offensive Cyberspace Operational Readiness for Military Leaders

Author: Major Niklas J McMurray, United States Marine Corps

Thesis: A new readiness framework is required to capture the *operational readiness* of Offensive Cyberspace Operations (OCO) forces in order to understand their capabilities and capacities for employment during combat operations.

Discussion: OCO are some of the most complex and dynamic military operations currently being conducted by the US military. That complexity has shrouded these operations in mystery that prevents policy and decision-makers from fully understanding current capabilities and limitations contained within this new domain. Current readiness assessment frameworks do not adequately translate these capabilities and limitations into a usable and understandable narrative and lack the specificity required to fully comprehend *operational readiness* of those forces. Readiness Systems such as Status of Resources and Training System (SORTS) and Defense Readiness Reporting System-Strategic (DRRS-S) capture the force readiness of US military units, but lack the fidelity to clearly define operational readiness, which is required within OCO for those assessments to be meaningful. Examples exist which highlight the complexity of cyber-weapons, from the time needed to develop weapons to the expertise required to ensure they execute as planned. Only when those nuances are captured within an operational-readiness framework can these capabilities and limitations be translated to policy and decision-makers for employment consideration.

Conclusion: A new operational readiness framework will help highlight the potential of OCO for use during combat operations and help simplify capabilities and limitations so that policy and decision-makers can fully comprehend and understand military power within cyberspace.

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.

Illustrations

List of Acronyms

AV	Anti-Virus
C2	Command and Control
CAS	Conduct Close Air Support
CCMD	Combatant Command (refers to unit)
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CMT	Combat Mission Team
CO	Cyberspace Operations
COCOM	Combatant Command (refers to command authority)
CONPLAN	Concept Plan
CRS	Chairman's Readiness System
CSA	Combatant Command, Service, and Combat Support Agency
CST	Combat Support Team
Cyberspace ISR	Cyberspace Intelligence, Surveillance and Reconnaissance
Cyberspace OPE	Cyberspace Operational Preparation of the Environment
DCO	Defensive Cyberspace Operations
DOD	Department of Defense
DODIN Ops	Department of Defense Information Network Operations
DRRS-S	Defense Readiness Reporting System-Strategic
GEF	Guidance for Employment of the Force
IAEA	International Atomic Energy Agency
IC	Intelligence Community
ICS	Industrial Control Systems
IO	Information Operations
IP	Internet Protocol

JCCA	Joint Combat Capability Assessment
JFRR	Joint Force Readiness Review
JSCP	Joint Strategic Capabilities Plan
JWICS	Joint Worldwide Intelligence Communications System
MET	Mission Essential Tasks
METL	Mission Essential Task List
MOS	Military Occupational Specialty
MRX	Mission Rehearsal Exercise
NDS	National Defense Strategy
NIPRNet	Non-Secure Internet Protocol Router Network
NMS	National Military Strategy
OCO	Offensive Cyberspace Operations
OPLAN	Operation Plan
RA	Readiness Assessment
SCADA	Supervisory Control and Data Acquisition
SIGINT	Signals Intelligence
SIPRNet	Secure Internet Protocol Routing Network
SOP	Standard Operating Procedures
SORTS	Status of Resources and Training System
TCP	Theater Campaign Plans
T&R	Training and Readiness
UCP	Unified Command Plan
UIC	Unit Identification Code
UJTL	Universal Joint Task List
USCYBERCOM	US Cyber Command

Table of Contents

Preface

I would like to thank everyone who helped contribute to this paper, either directly or indirectly, throughout my military career. My unraveling of this concept began upon checking into US Marine Corps Forces Cyberspace Command, where my initial duties aligned toward force-readiness reporting. This quickly exposed me to anything and everything readiness-related, both within the cyberspace domain and military readiness in general. Military readiness is truly a wicked problem that requires study, real-time emersion, and thoughtful reflection to fully understand and comprehend. After doing these things, the only thing I am sure about is that I still do not fully understand the subject, especially with regard to cyberspace. I hope this paper provides a solid foundation to continue this study.

I would especially like to thank my wife, Jessica, for her unwavering support during my year at Command and Staff. As my editor-in-chief, she continuously provided me with expert advice regarding all my papers at the schoolhouse, not just my Master's thesis. I could not have completed this year without her.

I would also like to thank my MMS mentor, Dr. Christopher Stowe, and my Military Faculty Advisor, LtCol Hunter Rawlings, for their help with completing this paper. Their personal and professional guidance has helped me succeed during a busy academic year.

INTRODUCTION

The US military has fully embraced the newest warfighting domain: cyberspace. The establishment of a sub-unified combatant command, US Cyber Command (USCYBERCOM), and each individual service cyber component (Army, Navy, Air Force, and Marine Corps) stands as a testament that the United States seeks to dominate militarily in cyberspace for the purpose of maintaining a decisive advantage over adversarial forces. This includes not only defending US and coalition computer networks, but also projecting power within the domain in terms of offensive actions. While most agree that this new domain is critically important, both civilian and military leaders in the US Government misunderstand its true potential. The complexity of cyberspace does not allow for decision-makers to fully understand or comprehend the digital domain the way they understand the physical domains of land, air, sea, or space. Turning policy and decision-makers into cyber experts is not possible, but also not necessary. What is required; however, is a framework to help translate cyberspace capabilities into an understandable narrative that allows decision-makers to employ them effectively during combat operations.

Military and political experts have wrestled with the concept of military readiness since the dawn of warfare. What constitutes a ready military force? What is that force ready to do? How long will it take a force to be ready? Historically, military readiness referred to a nation's ability to *mobilize* forces, both men and equipment, in order to wage war. This type of military readiness also referred to the sustainability of those forces once mobilized. Sustainability meant not only maintaining a force in the field (e.g. rations, fodder, clothing, etc.), but also replenishing those forces with fresh troops and equipment as wartime conditions eroded combat power. This type of military readiness relied entirely on the peacetime economic backbone of a nation, which would realign towards the war effort once mobilization began. Standing armies were less

common, as maintaining a large permanent army proved an inefficient method of expending national resources during periods of prolonged peace.[1]

While the ability to mobilize military forces remains a concern for many nations, starting in the 1950s, after the Korean War and with the beginning of the Cold War, the United States and the Soviet Union began to understand that *mobilization readiness* was irrelevant if the opposing side could quickly conquer an adversary and not allow for mobilization to occur. Standing, ready forces became a requirement to deter first-strike attacks and serve as a time buffer which would allow for mobilization to begin. This became a severe draw on national resources during peacetime, but became the norm over the next forty years of the Cold War.[2] This ready-force mentality still remains valid today, especially within cyberspace. The phrase *Fight Tonight* refers to the ability of the US military to wage combat within a short amount of time -- typically within minutes, hours, or days. With the development of Offensive Cyberspace Operations (OCO), and the capabilities this domain can provide to Geographic and Functional Combatant Commands (CCMD), cyber-weapons must sit on the ready bench of potential military options. However, unlike most conventional counterparts, cyber-weapon employment requires unique subject matter experts to develop and launch those weapons within a highly complex manner.

The term *readiness* has become a buzz phrase for US political and military leaders. But what does readiness really mean? Richard Betts states in his book *Military Readiness* that "readiness is vital, yet hardly anyone really knows what it is."[3] This is even more true for readiness within cyberspace, as the domain by itself is misunderstood, and trying to assess its readiness is impossible without understanding the domain. Traditional methods of assessing readiness do not encompass the true nature of cyberspace and severely misrepresent the actual

readiness status of cyberspace capabilities. This is especially true for OCO and current readiness assessments of the units tasked with conducting those operations: Combat Mission Teams (CMTs). A new readiness framework is required to capture the *operational readiness* of those teams in order to understand their capabilities and capacities for employment during combat operations. Without a new framework, OCO runs the risk of over promising operational capabilities or deferring potential capability for more conventional military strike options.

This paper will outline the requirements for a new offensive cyberspace operational readiness framework in a number of sequential steps. First, the paper will conduct a literature review of current readiness models and frameworks. This will allow for a full understanding of how the US military currently conducts readiness assessments of military forces. This will conclude with readiness theories outside of current readiness assessments produced by academics within the military-readiness field. Second, the paper will outline the research methodology used to define and analysis what constitutes OCO and cyber-weapons. This will be accomplished with current Department of Defense (DOD) doctrine and publications as well as a case study of the Stuxnet cyber-weapon. This section will identify what portions of OCO will be required within a operational readiness framework. Third, the paper will identify the findings and analysis of offensive cyberspace operational readiness by developing an operational readiness framework that truly depicts what constitutes a ready cyber capability. This framework can be used as starting point to develop a standardized readiness model that allows policy and decision-makers to understand offensive cyberspace operational readiness within the US military.

LITERATURE REVIEW

US military readiness is a top priority of strategic planners, both within the executive and legislative branches of government. Currently a number of joint guides, instructions, and directives provide guidance and instruction on military readiness reporting. Additionally, military analysts within the DOD and academia have also published various informational articles, papers, and books regarding the theory of military readiness and how to use those theories to determine resource allocations and, ultimately, guide the creation and maintenance of military forces that can win wars. Unfortunately, cyberspace operations do not surface within these documents due to the fact that this is a new domain, and government and military leaders believe it follows the traditional readiness framework of conventional forces.

This literature review will begin with a synopsis of the Chairman's Readiness System, composed of the Joint Combat Capability Assessment (JCCA) and Force Readiness Reporting. This system constitutes the current readiness assessment framework used within the entire DOD. The Force Readiness Reporting instruction is the current tactically focused readiness reporting framework used by all US military units, and is broken up into two different models: the Status of Resources and Training System (SORTS) and the Defense Readiness Reporting System-Strategic (DRRS-S). The next part of the literature review focuses on military readiness theory and how those theories are formulated into usable readiness assessments and how they can be used for future readiness frameworks.

The Chairman's Readiness System

The fundamental readiness reporting framework within the US DOD stems from the Chairman's Readiness System and is described and outlined within the *Chairman of the Joint*

Chiefs of Staff Guide to the Chairman's Readiness System (CJCS Guide 3401D) published in 2013:

> The Chairman's Readiness System (CRS) provides a common framework for conducting commanders' readiness assessments, blending unit-level readiness indicators with combatant command (COCOM), Service, and Combat Support Agency (CSA) (collectively known as the C/S/As) subjective assessments of their ability to execute the National Military Strategy (NMS).[4]

This system serves as the aggregate of the DOD's multiple readiness reporting systems covering the strategic, operational, and tactical levels of warfighting within the US military. It provides the framework that ultimately informs the executive and legislative branches on the current readiness status of all military services and joint forces. The guide defines readiness as "the ability of U.S. military forces to fight and meet the demands of the NMS."[5] This means the US military, at the strategic level, must be ready to accomplish tasks outlined within the NMS, which draws from the National Security Strategy (NSS) and the National Defense Strategy (NDS). From an operational perspective, the readiness frameworks draw upon tasks within the Unified Command Plan (UCP), Guidance for Employment of the Force (GEF), Joint Strategic Capabilities Plan (JSCP), theater campaign plans (TCPs), and named operations (including Operation Plans [OPLANs] and Concept Plans [CONPLANs]). Tactical-level readiness looks at unit-level readiness, which includes all joint forces down to the battalion, squadron, and group level. Combined together, these multiple frameworks provide readiness criteria that form the basis of required readiness reporting within the DOD. To simplify matters, the CRS breaks down readiness reporting into the JCCA (providing a strategic snapshot of US military readiness to the executive and legislative branches of government) and Force Readiness Reporting (providing an internal look at tactical level units within the military). Combined and aggregated

together, these two sub-systems make up the CRS, and are each governed by their own Chairman of the Joint Chiefs of Staff Instruction (CJCSI).[6]

Joint Combat Capability Assessment (JCCA)

The JCCA is the readiness system managed and maintained by the Joint Staff. The overall guidance and conduct of the JCCA is outlined in CSCSI 3401.01E, published in 2014. The instruction encompasses three sub-sections outlining responsibilities of reporting parties, the inputs required for the system to function, and the outputs it produces for consumption by the Office of the Secretary of Defense and the executive and legislative branches of government. The JCCA directs Unified and Specific Combatant Commands, Services, Combat Support Agencies, and the National Guard Bureau to report unit readiness via the Force Readiness Reporting System (more on this later). The organizations directed to report produce an overall Readiness Assessment (RA) of their organization based on a scale from 1 to 4 (1 being the most ready and 4 being the least ready). This assessment derives from an analysis of whether those organizations can execute assigned missions in support of the NMS, as directed by the GEF and JSCP.[7]

There are three outputs from the JCCA: the Joint Force Readiness Review (JFRR), the Plan Assessments, and the Readiness Deficiency Assessment. The JFRR is the overall assessment of the CRS. This is the aggregation of C/S/As unit-readiness data, synthesized into an assessment of whether or not the DOD can meet NMS requirements. The Plan Assessments analyzes the Combatant Command's ability to execute contingency plans (OPLANS and CONPLANs). This includes force sourcing from the services to meet requirements within these plans and the logistical requirements to ensure plans are supportable and sustainable. This assessment will identify risk to high-visibility plans in a timely manner to implement measures to

negate or reduce those risks. The Readiness Deficiency Assessment is an aggregate of all C/S/A readiness shortfalls that impact the successful execution of the NMS. This will prioritize appropriate resourcing to negate or reduce those shortfalls, or cause leaders to plan around these shortfalls.[8]

Force Readiness Reporting

The Force Readiness Reporting system is directed within CJCSI 3401.02B, published in 2014. The instruction is broken into three parts: the responsibilities of reporting units, guidelines for reporting, and reporting requirements. Just as in the JCCA, the Force Readiness Reporting systems directs C/S/As to report their readiness status to the Joint Staff, where the J-3 will aggregate those reports and input them into the JCCA (specifically the JFRR). The guidelines and reporting requirements of the instruction explain how reporting will be conducted. The two methods of reporting readiness are contained within two readiness systems: SORTS and DRRS-S. All US military units (battalion, squadron, group level, and above) are assigned an individual unit identification code (UIC) and are required to report within the automation readiness systems on a monthly basis or as their readiness status changes. All real-world readiness data is classified SECRET and the automated readiness system resides on the Secret Internet Protocol Routing Network (SIPRNet).[9]

SORTS is a resource-based reporting system, based on a unit's ability to meet a generic wartime mission. SORTS breaks down units into tangible factors, including personnel, equipment, equipment condition, and training. Each factor is then broken down into 4 readiness levels, 1 through 4 (1 being the most ready and 4 being the least ready) based on standardized criteria. Figure 1 outlines the SORTS ratings system:

Personnel (P-Level)	Equipment (S-Level)	Equipment Condition (R-Level)	Training (T-Level)
P1	S1	R1	T1
P2	S2	R2	T2
P3	S3	R3	T3
P4	S4	R4	T4

Figure 1: SORTS Rating System

Once a unit determines the scores associated with each rating, those ratings are aggregated into an overall Resource Category-Level (C-Level), again based on a scale from 1 to 4. The C-Level is not an average of the P, S, R, and T-Levels, but aligns to the lowest of the four. For example, if a unit reports a score of 1 for P, S, and R, but a score of 4 for T, the aggregate C-Level would be a 4, aligned to the lowest level of the four readiness categories. The CJCSI contains all the specific criteria per resource area, to ensure standardization across the joint force in order to ensure all units report similarly. [10]

DRRS-S, on the other hand, is a mission-focused, capabilities-based framework to assess readiness. Instead of using tangible resource criteria like SORTS, DRRS-S uses more intangible mission assessments based on a unit's ability to accomplish assigned Mission Essential Tasks (METs). METs are standardized across the joint force and a list of every MET can be found within the Universal Joint Task List (UJTL) and service specific Task Lists. Examples of METs include "Conduct Offensive Operations" and "Conduct Close Air Support (CAS)."[11] Each individual MET is assessed via a three-tier scale: *Yes*, *Qualified Yes*, and *No* (*Yes* being completely ready, *Qualified Yes* being partially ready, and *No* being not ready), based on specified standards and conditions. These conditions and standards are unique to individual unit types. A unit's overall collection of METs creates a Mission Essential Task List (METL). After individual MET assessments, the aggregate of those METs provides an overall grade for the METL. Unlike SORTs, DRRS-S assessments are averaged, meaning that if a majority (> 50%)

of the METs within a unit's METL are grade *Yes*, then the units overall readiness assessment is *Yes*. Below is an example unit METL assessment:

	YES	QUALIFIED YES	NO
MET 1	**X**		
MET 2		**X**	
MET 3			**X**
Overall METL		**X**	

Figure 2: DRRS-S METL Assessment

Combined together, SORTS and DRRS-S are the readiness systems that provide unit-level readiness reports for all units within the DOD. These systems are the functional output of current US military readiness theory and provide the only formalized method to report unit readiness to the Joint Staff, and then onto the executive and legislative branches of government via the JCCA.[12]

Military Readiness Theory

Military readiness has been a source of contention since the end of World War II. As the United States began to develop and maintain an immediate readiness capacity during the Cold War, methods of measuring and quantifying that readiness have led to multiple different and competing frameworks and models. The most recent of those models falls under the Chairman's Readiness model described above. However, the theory of military readiness is still vastly misunderstood and many within the military and political communities use the term without fully grasping its true meaning.

Richard Betts began to unravel the true nature of military readiness within his comprehensive book on the topic. Betts broadly defines military readiness as the relationship between available time and needed capacity, and that "a country is militarily ready as long as the time needed to convert potential capability into the actual capability needed is not longer than the time between the decision to convert and the onset of war."[13] Historically, this has been the

mobilization period that leads up to war. However, with the onset of the Cold War, countries must maintain immediate readiness to respond to enemy aggression.

Betts breaks down military readiness into three categories: structural readiness, operational readiness, and mobilization readiness. Structural readiness is concerned with mass and fundamentally looks at the *size* of a standing military force. Today this would encompass authorized troop strength and the amount of equipment on hand. The focus of assessments for structural readiness is outward looking, based on the conceptual effectiveness against an enemy force. This type of readiness is difficult to maintain when multiple adversaries exist that threaten a nation (the current US position with China, Russia, North Korea, Iran, and terrorist organizations). Operational readiness is concerned with the actual effectiveness of a standing military force. Most military planners are concerned with operational readiness, which are what systems like SORTS and DRRS-S measure and shows a force's "immediate capacity for combat."[14] Both of these readiness models are based on time, but whereas structural readiness is defined as *speed times mass*, operational readiness refers to *speed times efficiency*. The last form of readiness is mobilization readiness. Prior to the 20th century and the Cold War, most nation-states maintained only a small standing army and relied on mobilization readiness to convert potential civilian power into military power. Mobilization readiness still remains relevant within modern warfare, but only if time limits allow, meaning that countries must maintain enough structural readiness at a high enough operational readiness status to allow mobilization to occur. All three forms of readiness overlap to an extent and a successful nation must maintain a degree of all three to achieve victory in combat.[15]

Changing Military Readiness

As the United States entered a period of military uncertainty after the end of the Cold War, military readiness experts have tried hard to evolve and mature readiness theory into a structured framework that enables users to understand readiness data and use that data to make decisions regarding national security. Laura J. Junor proposes an economic-based framework to determine and understand risk within military readiness. Junor argues that readiness can be broken down into the "supply of ready forces" and the "demand for ready forces." This construct works well within the context of the military structure of the United States, but only focuses on the operational and strategic level of military readiness. Junor believes that systems like SORTS and DRRS-S provide the correct amount of data to be useful at the tactical level, but those systems are unable to identify the causes of readiness deficiencies. For Junor, "a healthy readiness management framework must monitor DOD force generation pipelines well enough to signal deficiencies and their likely consequences clearly and before those consequences are high."[16]

Within the United States, the individual military services have a legal obligation to man, train, and equip military forces. Functional and geographic CCMDs then employ those forces when conducting operations. Junor uses this established structure to develop her readiness model of supply and demand. The combatant commands demand ready forces for use during operations and the services supply those forces. If supply exceeds demand, resources are wasted, and if demand exceeds supply, the United States is unready to conduct military operations. The issue she seeks to rectify is the ability to predict shortfalls within military readiness in order to allow for time to fix or negate those shortfalls. The supply side of military readiness starts with the various and interconnected service production pipelines of personnel and equipment and how

those resources eventually produce and maintain operational readiness. This in turn is formulated upon the demand side of readiness, which is based on the combatant command demand for either steady-state rotational forces or forces needed for contingency operations.[17]

Junor uses these theories to develop frameworks for readiness analysis, specifically static and dynamic readiness models. A static analysis assesses the readiness of operational forces and contingency planning. This type of analysis lends itself to the operational readiness described by Betts, insofar as CCMDs demand a certain amount and type of military force to achieve objectives. If the services are unable to meet those requirements, the military readiness of the United States is degraded. This provides a very static type of readiness analysis and can only identify deficiencies, and not necessarily determine causality. Dynamic analysis takes this readiness measurement one step further. This assessment determines the military's ability to meet national objectives within an ever-changing world. It includes "transit time…the availability of sustainment enablers…the expected role of allies…reactions of adversaries…and the probability of success for each objective."[18] This type of readiness is much more telling of *actual* military readiness, but is also extremely difficult to assess and equally difficult to synthesize down into simplified and usable information for policy makers to act on. While Junor's analysis and model for military readiness help planners understand the complexity of military readiness, it restricts itself to the high operational and strategic level of readiness assessment.[19]

RESEARCH METHODOLOGY

In order to develop a framework to help display and communicate OCO readiness to decision-makers, a fundamental understanding of what OCO is and what constitutes a cyber-weapon is required. To accomplish this task, the research methodology will be broken down into two distinct parts. First, this section will define what OCO is, according to joint military doctrine. Second, the methodology will use an unclassified case study, based on the Stuxnet cyber-weapon, to breakdown what constitutes a cyber-weapon and its fundamental components. This part will conclude with a basic layout of the requirements needed for cyber-weapon development, maintenance, and employment.

Offensive Cyberspace Operations (OCO)

There are three distinct parts of what the military considers Cyberspace Operations (CO): Defensive Cyberspace Operations (DCO), Department of Defensive Information Network Operations (DODIN Ops), and OCO. The first two (DCO and DODIN Ops) encompasses the installation, operation, maintenance, and security (both passive and active) of DOD cyberspace (including networks, weapon systems, industrial control systems, etc). On the other hand, "OCO are CO intended to project power by the application of force in and through cyberspace."[20] Like conventional kinetic fires (artillery, air-to-surface bombs, etc.), the military seeks to use cyberspace as a method to impose its will on the enemy. This means using cyberspace as an avenue to introduce effects within the enemy's cyberspace to support the commander's intent or objectives.

The main goal of OCO is to deliver a Cyberspace Attack on enemy forces to achieve a specific outcome, just as in the conventional environment. Cyberspace Attack includes effects that seek to *deny* or *manipulate* cyberspace components of the enemy force. The denial of

cyberspace to an adversary includes the ability to "degrade, disrupt, or destroy access to, operation of, or availability of a target by a specified level for a specific time."[21] This can include the physical or logical components of cyberspace and their immediate peripherals. This type of attack resembles conventional kinetic attacks. Additionally, within Cyberspace Attack, effects can be reversible; meaning that unlike conventional kinetic attacks, physically destroying a target is not a requirement.

Manipulation includes controlling or changing an "adversary's information, information system, and/or networks in a manner that supports the commander's objective."[22] This type of Cyberspace Attack closely aligns within the doctrine of Information Operations (IO). IO seeks "to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries."[23] While not all IO are conducted through cyberspace, the domain provides IO a large conduit to conduct these operations. The ability to manipulate data and information within an enemy's cyberspace is a powerful capability, not by just denying its use, but by destroying completely the trust and reliability of those systems. When combined, both denial and manipulation constitute a robust capability within the cyberspace domain.

Just like any other military operation, planning and preparation is required to enable a Cyberspace Attack. Within the larger context of OCO, Cyberspace Attack is only the final step. Prior to the denial or manipulation effect taking place, Cyberspace Intelligence, Surveillance and Reconnaissance (Cyberspace ISR) and Cyberspace Operational Preparation of the Environment (Cyberspace OPE) must occur. Cyberspace ISR includes the collection of operationally relevant information regarding a planned Cyberspace Attack. This collection occurs through military-collection efforts or through using signals intelligence (SIGINT) derived from the Intelligence Community (IC). It is important to note that Cyberspace ISR and SIGINT are not synonymous

and are conducted using different authorities. However, the information collected is used in the same manner; that is, to conduct detailed planning for a Cyberspace Attack. Cyberspace OPE is similar to conventional OPE, but within the cyberspace domain. During this phase of the cyberspace operation, cyber operators may exploit certain security vulnerabilities within an enemy network and implant tools that allow for access at a later time. Cyberspace OPE is typically conducted in a covert manner to ensure enemy forces are unable to take defensive actions and prevent further Cyberspace Attacks. The three parts of OCO (Cyberspace ISR, Cyberspace OPE, and Cyberspace Attack) can fit into the construct of phasing. Each phase occurs sequentially starting from intelligence collection, but they typically overlap.[24] The below graphic depicts OCO phasing:

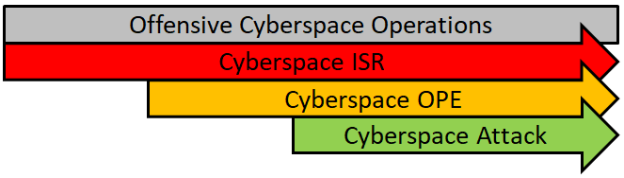

Figure 3: OCO Phases

Case Study: Stuxnet

In 2010, inspectors from the International Atomic Energy Agency (IAEA) noticed that centrifuges within Iranian Natanz nuclear facility were wearing out at a higher-than-normal rate. Nuclear centrifuges are cylinder-shaped devices that spin uranium at high rates of speed in order to enrich the uranium for use in nuclear power production. Those same methods of enrichment can also highly enrich uranium for use in nuclear weapons. By 2010, Iran had only recently began expanding its nuclear enrichment program, so the IAEA inspectors attributed the higher-than-normal wear out rate of the centrifuges to inexperience in the enrichment process. While exact numbers are difficult to ascertain, the IAEA inspectors estimate that Iran replaced between

900-1000 centrifuges during 2010, while some within the international community double that number.[25]

In June of 2010, the Belarusian Anti-Virus (AV) firm VirusBlokAda received a telephone call from one of its Iranian computer clients with an issue stemming from the constant rebooting of computers within their company. VirusBlokAda began an investigation of the computers in question and soon discovered what is known within the cyber community as a Zero Day exploit. Zero Days are vulnerabilities within computer systems that are previously unknown to the cybersecurity enterprise. This means that these vulnerabilities remain exploitable because patches (updated computer programming) have not been developed or implemented within the at-risk system or program because the vulnerabilities are unknown. Additionally, AV programs are unable to identify them for the same reason. The Zero Day that VirusBlokAda identified allowed malicious code (typically referred to as a computer virus or worm) to jump between computer systems via an exploit contained in how thumbdrives activate once they are plugged into a computer system. Once the Zero Day was discovered, VirusBlokAda shared the vulnerability with other companies in the cybersecurity community, including Kaspersky Lab, understanding that deconstructing the virus would take a massive amount of expertise and manpower.[26]

After months of tedious code reading, analyzing, and testing, cybersecurity experts were able to piece together what the malicious virus was intended for and how it accomplished that intent. Ultimately, the virus, dubbed Stuxnet (based on lettering contained within the code itself), intended to undermine the Iranian nuclear program by subtly destroying the centrifuges used for uranium enrichment. Stuxnet was actually comprised of four different Zero Days with the intent of exploiting security measures and the Industrial Control Systems (ICS) at the Iranian

facility that controlled the speed in which the centrifuges spun. Cybersecurity experts agreed that the complexity of the virus and use of multiple Zero Day exploits could only mean that a nation-state actor was behind the attack. Stuxnet not only sought to destroy the centrifuges in manner than was consistent with nuclear engineering inexperience, but also fed manipulated data to the ICS to cover its tracks. Stuxnet was by all appearances a fully functioning cyber-weapon that accomplished its intended mission.[27]

The research, development, and employment of cyber-weapons is unique within the context of military weaponry, specifically in the amount of time needed for research and development, the limitations of employment, and the notion of *one-time-use* weapons. As seen with Stuxnet, cyber-weapon development is extremely complex, requiring expertise in not only cyberspace operations, but also in particular sciences and engineering. Additionally, time for development is lengthy, from the time needed to gather relevant intelligence and information to actually coding the cyber-weapon for employment. For Stuxnet, after determining that the Iranian nuclear program was the target and that the Cyberspace Attack would require non-attribution to the employing party, planning needed to occur on where the disruption was to take place within the program as a whole. This would require nuclear engineers to determine a suitable place to attack the program -- in the case of Stuxnet, the enrichment process. This would now require detailed intelligence on the specific centrifuges used within the facility and how they operate. OCO requires a vast amount of intelligence, both within cyberspace and the other physical domains. As development continues, weapon testing is needed, requiring either sophisticated computer simulations or acquisitioning and testing on actual physical components to determine if the code actually works. The analogy that works best for cyber-weapon development is that of conventional munitions such as an aircraft or missile system. This

research and development would take months, if not years, to accomplish. And this process would need to be conducted for *each* cyber-weapon developed.

Unlike conventional munitions, the shelf life and employment considerations of a cyber-weapon is typically limited. Zero Day exploitations are only useful for as long as they remain secret from public and military cybersecurity communities. Once their exploits are known, they become null and void because security postures and mechanisms can be incorporated into cybersecurity systems to ensure those exploits are identified and protected against. The lifespan of a Zero Day ranges on average 6.9 years before either software developers identify the vulnerability prior to exploitation or hackers use the Zero Day to exploit a system, thereby triggering cyber forensics to identify the exploitation, like what occurred with Stuxnet.[28] Once Stuxnet was discovered, AV firms installed patches on their cybersecurity software to identify and protect against the security vulnerabilities that Stuxnet sought to exploit. This is vastly different from conventional weapon systems and munitions. A bomb or missile dropped or launched from an aircraft cannot be immediately and indefinitely countered just because the enemy knows this capability exists. Cyber-weapons must be continuously developed and maintained to ensure proper functionality and employment. Additionally, once a cyber-weapon is used during combat operations, the chances of successfully using that same weapon again become significantly lower because the enemy now knows about the vulnerability and can take steps to render it safe.

To help understand how cyber-weapons function, Kim Zetter describes that each weapon is broken down into two major components: the payload and the missile.[29] The payload of a cyber-weapon refers to the overall intent of that weapon, specifically the effect that the weapon will have on its target. Within the context of Stuxnet, the payload caused the centrifuges to spin

at higher rotations, which eventually led to them wearing out faster than normal. It also contained a function that told the ICS to report everything was functioning normally. The payload component of a cyber-weapon is typically the most complex because it incorporates specific information on the system being manipulated or denied. In the case of Stuxnet, this meant the payload contained information regarding the ICSs that controlled the centrifuges and the Supervisory Control and Data Acquisition (SCADA) system that ran the entire enrichment system. For cyber-weapons development, specific systems must be targeted and their systems completely understood for the weapon to be effective. If a cyber-weapon was developed against an enemy radar site, the software that ran the site would need to be understood and weaknesses found in order to exploit the system. Cyber-weapons development thus becomes extremely complicated and time consuming, and this is only a piece of the overall cyber-weapon.[30]

The second component of the cyber-weapon is the missile portion. This part of the weapon refers to how the payload portion will arrive at the system that will be exploited. The missile portions is usually where Zero Days are incorporated into the weapon, as the missile must exploit or negate cybersecurity systems in order to place the payload effectively. Within the context of Stuxnet, the missile portion contained code that automatically downloaded the payload onto the host machine when a thumbdrive was connected using a Zero Day exploit (as mentioned above, Stuxnet contained four Zero Days that allowed the virus to spread and was much more complicated than a single thumbdrive exploit, but this single example will suffice for the purpose describing the missile portion of a cyber-weapon). The missile portion requires extensive knowledge of current cybersecurity systems and the ability to hack those systems. Additionally, depending on the system being exploited, the missile may also require specific knowledge on very specific computer systems and how it interacts with ICS or SCADA systems.

This again requires expertise on not only cybersecurity, but also specific machinery and engineering systems. Developers for Stuxnet needed knowledge on how the ICS for the centrifuges interacted with other cyber systems to ensure functionality. Combined together, the payload and missile portions of a cyber-weapon are extremely complex, requiring vast expertise and time to develop into a fully functioning cyber weapon. [31]

FINDINGS AND ANALYSIS

Upon reviewing the current literature on readiness reporting models and theories and analyzing how OCO is conducted, a glaring deficiency begins to surface. The US military currently compiles readiness data and produces readiness status reports based on Cold War standards; those standards provide limited insight on the actual readiness of military forces within the context of *operational* readiness. Operational Readiness, as defined by Betts, refers to the ready status of units, that is, their ability to accomplish wartime missions by tangible standards and criteria.[32] This type of readiness reporting is currently conducted within systems such as SORTS and DRRS-S, which looks at concrete readiness data, such as personnel on hand, equipment on hand, etc. While this type of readiness reporting is useful and contributes to the readiness of a military unit, it lacks the actual operational readiness status of a unit. For example, policy and decision-makers use readiness reports within SORTS and DRRS-S to define the operational readiness of a force; that is, what forces are available to fight immediately. This is misleading because in actuality those systems capture *force*-readiness reporting (as the title of the system indicates). The system fails to determine the readiness of those forces against an adversary, which interests most policy and decision-makers. Betts describes this as *relative* readiness, that is, readiness compared to an opposing force.[33] This is a critical component of operational readiness, in terms of a fight-tonight capability. For example, SORTS and DRRS-S reports a US Marine infantry battalion as C-1 and fully mission capable to assigned core missions (e.g. Conduct Offensive Operations). But if that infantry battalion is located in Southern California, how operationally ready is that unit for performing offensive operations against North Korea? Clearly from that standpoint, they are unready (not actually located within

the theater). This highlights a clear distinction between *force* readiness and *operational* readiness.

Offensive Cyberspace Operations are clearly complex both in their planning and execution. Due to those complexities and a lack of understanding of cyberspace operations in general, reporting operational readiness for those capabilities is challenging. Current cyber forces report readiness against the force-readiness standards contained within SORTS and DRRS-S, just like other military units. However, policy and decision-makers rightly view cyberspace as a global domain, and assume that cyberspace operations occur in real-time without considering the complexity of the domain. Readiness reporting for OCO can pull certain aspects from systems such as SORTS and DRRS-S, which provide a very basic sense of the force readiness of those units, but a deeper level of analysis and reporting is necessary to fully understand the true operational capacity of those forces.

This analysis will focus on developing a framework for operational readiness reporting for OCO. The framework will focus on the operational readiness of cyber forces, specifically the CMT. The first few tenets of this proposed OCO readiness framework look similar to those matrixes contained within SORTS and DRRS-S, but the framework will expand and modify on those data sets. Any capability within the military is unit dependent, as those units are the foundation of the military and provide warfighting capabilities. As such, this framework will focus on the CMT to align with current readiness models in order to ease understanding. Additionally, this framework uses a building-block approach, where any shortfalls lower in framework impact those tenets later on. Hopefully, this model can help determine actual offensive cyberspace operational readiness. However, this is only a starting point and requires

deeper analysis and planning in order to standardize the framework and make it useful to policy and decision-makers.

The framework will focus on the following tenets:

- Basic Personnel
- Administrative and Training Environments
- Basic Individual Training
- Basic Team Training
- Assigned Mission
- Critical Personnel
- Advanced Individual Training
- Advanced Team Training
- Cyber-Weapons (Tools)
- Operating Platforms
- Authorities
- Access

Basic Personnel

The composition of personnel within a military is a fundamental component of readiness assessments and must carry over into an operational readiness framework for CMTs. Typically, a table of organization, or a list of required personnel, accounts for this manning consideration. However, because OCO is complex and missions are fundamentally different depending on the intended endstates, CMTs should first account only for basic personnel. These types of billets should include personnel that would be required for any sort of OCO mission. Those include billets like a Team Leader, a Staff Noncommissioned Officer, intelligence analysts, computer network specialists, computer system specialists, etc. These personnel can be military or civilian employees and factor into the overall force structure of the military. This tenet is currently captured within SORTS and should carry over to this cyber readiness framework. However, this tenet does not encompass all personnel within a CMT, as more will be required depending on the assigned mission (more on this later).

Administrative and Training Environments

Like any military unit, a CMT requires access to basic facilities that allow the unit to function properly. This includes access to military computer networks to conduct required military training and administrative functions. This would normally consist of access to the Non-Secure Internet Protocol Router Network (NIPRNet). Further, CMTs require access to classified networks to conduct planning and research. This would require access to systems like SIPRNet and the Joint Worldwide Intelligence Communications System (JWICS). This would also allow for access to intelligence databases. Finally, CMTs need access to secure, closed-network training environments used to conduct individual and team-level training. These Cyber Ranges are key for teams to train, just like rifle ranges are for infantry units. Like other ranges, these are not maintained by the CMT and should be managed and provided to them by supporting entities. The Combat Support Team (CSTs) could easily provide this function.

Basic Individual Training

Like most forms of military training, skills begin to atrophy after a certain amount of time. Basic Personnel should come fully trained to a CMT, based on training standards established by the Military Occupational Specialties (MOS), but should also be required to undergo standardized refresher training on established timelines. This is similar to current military training procedures (e.g. rifle qualification, swim qualification, etc.). These recurring training events must be standardized and draw upon expertise from within the cyber community and training and education commands throughout the US military. This type of readiness is assessed via individual service Training and Readiness (T&R) Manuals per MOS and should be included into the CMT operational readiness assessment framework.

Basic Team Training

Building upon Basic Individual Training, CMTs should be required to undergo standardized team-level training on a recurring basis. This should include all standard operating procedures (SOPs) and processes within the team. This is similar to tank crews or fireteams undergoing training to ensure they can function as a cohesive unit. This training should include joint-targeting processes, command and control of operations, intelligence-analysis processes, etc. Again, this is currently assessed via the individual services T&R Manuals per unit (team, crew, squad, etc) and should carry over into the CMT's operational readiness assessment.

The first four tenets of CMT operational readiness are directly related to the data currently collected and maintained by SORTS and DRRS-S. As stated before, this data is important, but does not encompass all aspects of CMT operational readiness. The following tenets outline the details needed to assess offensive cyberspace operational readiness.

Assigned Mission

Having an assigned mission is paramount to CMT operational-readiness assessments. Without it, the following tenets cannot be applied and the readiness status of the CMT becomes limited to basic force-readiness criteria (current readiness reporting framework). Issuing an assigned mission to a CMT focuses its efforts to a basic intent and potential target set. Unlike conventional forces, CMTs cannot pivot quickly between assigned missions, as the time required to be "fully mission capable" against a specific target takes months, if not years (as identified by the Stuxnet example). Additionally, an assigned mission differs significantly from the METs found within DRRS-S. METs are meant to be broad in nature, providing a basic snapshot of unit readiness regardless of the operational mission or adversary. OCO cannot be assessed in this

manner due to the time it would take to make CMTs operationally ready once an operational mission is assigned. Assigned missions are critical for CMT operational readiness assessments.

Critical Personnel

Once a CMT receives an assigned mission, planning for that mission can begin with the basic personnel on hand. The first step to this planning process should be fully staffing the CMT with personnel required for the assigned mission. Theoretically, if the mission was to attack the Iranian nuclear program (like Stuxnet), it would make sense to bring in planners and experts on Iran, Farsi Linguists, nuclear engineers, Industrial Control Systems specialists, tool developers, etc. These personnel would bolster the roster of the CMT based on mission requirements. Critical Personnel rosters should be a flexible standard as the mission evolves.

Advanced Individual Training

In addition to the Basic Individual Training for Basic Personnel, CMT training should also include advanced training for Basic and Critical Personnel based on mission requirements. This should include mission-specific operating system training, ICS and/or SCADA, language training, etc. Again, like the Critical Personnel, this standard will vary depending on the assigned mission and will continue to evolve as the mission progresses. A lack of advanced training could have significant impacts to the operational readiness of the CMT. This training can be acquired from other military schools (including electronic warfare or information operations) or can be contracted through private vendors. Using Stuxnet as an example, the CMT conducing that mission would require Advanced Individual Training on centrifuge technology and software, Farsi, Iranian command and control procedures, etc.

Advanced Team Training

After being assigned a mission and gathering the requisite critical personnel and advanced individual training, the CMT must train as a military unit to ensure it operates as an effective OCO force. Most importantly Advanced Team Training must include Mission Rehearsal Exercises (MRXs) that replicate how a real-world operation would take place. This also includes command and control procedures within the Combatant Command that the CMT is supporting. This training will require access to cyber-training ranges (described in Administrative and Training Environments). The cyber-training ranges must mirror real-world networks to be effective. The ability to operate as a fully functioning CMT against an assigned mission is critical to operational-readiness assessments. Again, using Stuxnet as an example, the CMT would need to conduct an MRX against simulated or real centrifuge components to ensure the team can operate effectively.

Cyber-Weapons (Tools)

The CMT will need to develop and maintain cyber weapons (or tools) to conduct OCO. Conventional military terminology refers to this as *weaponeering*. This includes the development of exploits to gain access to adversary systems and affect those systems in a manner that is useful to the commander. As described by Zetter, this includes the missile and payload portion of the cyber-weapon.[34] These weapons will require constant maintenance to ensure they function as intended and that the vulnerabilities that these weapons exploit remain open. This is an extremely technical aspect of the operational-readiness status, but also a requirement to ensure tools have been developed and are ready for use to achieve effects within cyberspace.

Operating Platforms

Another fundamental part of conducting OCO is the use of an operating platform. An operating platform is a piece of cyberspace that is used to launch OCO. Typically an operating platform is a covertly acquired logical space within the internet that allows cyber actors to operate without attribution to their own portion of the internet. This is important for two reasons. First, from an operational standpoint, launching cyberspace operations from a non-US military part of cyberspace allows operations to occur successfully. Like exploits, knowing where a cyber-attack is coming from allows defenders to modify defensive postures to negate those attacks. For example, if a cyber-attack is launched from Internet Protocol (IP) addresses that are known US military addresses, a simple configuration change within the firewall or router stops the attack and prevents future attacks. The use of a covert platform prevents the adversary from knowing from where the attack is coming. Additionally, some cyberspace operations will require non-attribution to the United States. Similar to SIGINT collection, not allowing an adversary to know from where the attack is coming allows those forces to operate more freely when conducting sensitive operations.

The easiest way to understand an Operating Platform is the aircraft carrier analogy. The aircraft carrier serves as a launch point to conduct air operations against enemy targets and the aircraft are the weapons that conduct the strike. This is similar to how an Operating Platform functions, as the launch point for OCO and the cyber weapons (missile and payload) are the "aircraft." Also like aircraft carriers, Operating Platforms require extensive maintenance to remain effective. Specifically they require the continuous acquisition of expendable IP addresses and redirectors. If operating platforms are viewed as a weapon system, they require their own personnel to maintain them. The CST would be the best candidate for this maintenance.

Without continuous access and use of a functioning operating platform, CMTs operational readiness is severely impacted.[35]

Authorities

The permission to operate within an area of operation has largely been detached from the readiness paradigm. Force readiness measures a unit's ability to accomplish its core mission set without regard for when and where it will conduct those operations. This is different from OCO, as intelligence collection and preparation of the environment is critical to mission success much further in advance than conventional military operations. Additionally, the methods used to conduct Cyber ISR and Cyber OPE utilize the same methods of vulnerability exploitation that Cyberspace Attack used. Again, it is a building-block process, but all within an adversary's cyberspace. This makes authorities to conduct OCO vitally important to offensive cyber readiness. If a CMT does not gain those authorities well in advance of an operation, the ability to conduct a successful Cyberspace Attack is drastically reduced, if not impossible.

CMTs must be able to operate within their battlespace in order to achieve effects at a specific time and place. The authority level granted to those teams dictates how much it can accomplish beforehand. This could either take months or years (e.g. no authorities) or seconds (e.g. Cyber OPE authorities). This factor must be incorporated into the operational readiness assessment of CMTs due to the inability to conduct operations in a timely manner if tasked. Decision-makers must understand that by limiting or accepting risk (e.g. how many authorities a CMTs maintains) directly impacts whether or not OCO can occur within a designated timeframe. The authorities can be broken down into the levels of OCO, namely Cyber ISR (collect and analyze), Cyber OPE (setting conditions for attack), or Cyber Attack (deny or manipulate). Once these authorities are incorporated into an operational readiness status, decision and policy-

makers can make informed decisions about the risks and rewards of allowing CMTs to set conditions for execution of Cyberspace Attack. [36]

Accesses

The final component of OCO operational readiness considers whether CMTs are able to achieve the intended effects of their mission based on real-time technical limitations. Once the above readiness conditions are met and teams are authorized to conduct certain levels of OCO, they must gain initial access to targeted systems and maintain that access to ensure cyber payloads can be delivered once the order to execute is received. If that access is disrupted in any way, a CMT loses its ability to attack that target. An almost infinite amount of scenarios and circumstances could arise to disrupt or cut off access to a target system, such as a change in the defensive posture of the targeted network, changes in grey space (the internet), Zero Day exploits being discovered, access discovery, etc. The up-to-the-minute status of access to targeted systems is a critical component of a CMT's operational readiness status. Without access, the ability to attack the system is affected, which could take minutes or months to regain, depending on the circumstances surrounding the disruption. This could potentially cause the CMT to start again from the beginning of the planning process to reacquire access, if possible at all.

CONCLUSION

Offensive Cyberspace Operations are some of the most complex and dynamic military operations currently being conducted by the US military. That complexity has shrouded these operations in mystery and has not allowed those within the decision-making process to fully comprehend the capabilities and limitations that currently exist within the new domain. The current readiness reporting method falls short on delivering the information required to accurately describe the operational status of CMTs and OCO as a whole. The above OCO readiness tenets are only a starting point within this discussion and further research must be conducted to complete the readiness model. Readiness reporting is only as good as the framework provided, so clear and specific standards, criteria, and conditions must flesh out the framework to expand its utility.

Once a detailed readiness matrix is created, the data can be used to create the narrative to help policy and decision-makers understand and employ offensive capabilities effectively. While CMT reporting highlights specific shortfalls within the readiness status of units executing OCO, policy and decision-makers must speak in the terms of capabilities, not individual units. Offensive cyberspace capabilities must be listed as a menu of possible military options available to augment current conventional military, diplomatic, economic and informational capabilities. Timelines must also accompany these potential offensive cyberspace capabilities and the shortfalls related to those timelines. If policy and decision-makers understand that authorities are hindering the ability to gain and maintain access to key adversary cyberspace, they may be more inclined to grant or delegate those authorities to increase the operational readiness of CMTs. Without this narrative, OCO runs the risk of being oversold and then underutilized when expectations do not match the actual operational readiness assessments of those teams.

[1] Richard K. Betts, *Military Readiness: Concepts, Choices, Consequences* (Washington DC: The Bookings Institute, 1995), 5-8.
[2] Betts, 19-25.
[3] Betts, 4.
[4] US Department of Defense, *CJCS Guide to the Chairman's Readiness System*, CJCS Guide 3401D (Washington DC: Department of Defense, November 15, 2010), I-1
[5] CJCS Guide 3401D, 1.
[6] CJCS Guide 3401D, 7-19.
[7] US Department of Defense. *Joint Combat Capability Assessment*. CJCSI 3401.01E, May 19, 2014, C-1 to C-2.
[8] CJCSI 3401.01E, D-1 to D-2.
[9] US Department of Defense. *Force Readiness Reporting*. CJCSI 3401.02B, July 17, 2014, A-1 to A-4, B-7.
[10] CJCSI 3401.02B, B-1 to B-2, C-1 to C-17.
[11] US Department of Defense. *Universal Joint Task List*. Last updated February 12, 2018, 857 and 1301, http://www.jcs.mil/Doctrine/Joint-Training/UJTL/
[12] CJCSI 3401.02B, B-2 to B-3, C-18 to C-21.
[13] Betts, 27-28.
[14] Betts, 26.
[15] Betts, 40-43.
[16] Laura J. Junor, *Management Military Readiness*, Strategic Perspectives, no. 23 (Washington DC: National Defense University Press, 2017), 4.
[17] Junor, 2-5.
[18] Junor, 27.
[19] Junor, 25-28.
[20] US Department of Defense. *Cyberspace Operations*. Joint Publication 3-12 (R) (Washington DC: Department of Defense, February 5, 2013), II-2.
[21] JP 3-12 (R), II-5.
[22] JP 3-12 (R), II-5
[23] US Department of Defense. *Information Operations*. Joint Publication 3-13 (Washington DC: Department of Defense, November 20, 2014), I-1.
[24] JP 3-12 (R), II-4 to II-5.
[25] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown Publishers, 2014), 1-5
[26] Zetter, 5-10.
[27] Zetter, 52-68, 88-98.
[28] Lilian Ablon and Andy Bogart, *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits* (Santa Monica, CA: RAND Corporation, 2017), 52.
[29] Zetter, 52-53.
[30] Zetter, 116-128.
[31] Zetter, 52-68.
[32] Betts, 40.
[33] Betts, 145-146.
[34] Zetter, 52-53.
[35] Mark Pomerleau, "Why you'll hear about a 'cyber carrier' in 2018," *Fifth Domain*, December 29, 2017, https://www.fifthdomain.com/dod/cybercom/2017/12/29/why-youll-hear-about-a-cyber-carrier-in-2018/
[36] JP 3-12 (R), IV-1 to IV-15

BIBLIOGRAPHY

Ablon, Lilian and Bogart, Andy. *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*. Santa Monica, CA: RAND Corporation, 2017.

Betts, Richard K. *Military Readiness: Concepts, Choices, Consequences*. Washington DC: The Bookings Institute, 1995.

Junor, Laura J. *Management Military Readiness*. Strategic Perspectives, no. 23. Washington DC: National Defense University Press, 2017.

Pomerleau, Mark. "Why you'll hear about a 'cyber carrier' in 2018." *Fifth Domain*. December 29, 2017. https://www.fifthdomain.com/dod/cybercom/2017/12/29/why-youll-hear-about-a-cyber-carrier-in-2018/

US Department of Defense. *CJCS Guide to the Chairman's Readiness System*. CJCS Guide 3401D. Washington DC: Department of Defense, November 15, 2010.

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

US Department of Defense. *Force Readiness Reporting*. CJCSI 3401.02B, July 17, 2014.

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

US Department of Defense. *Joint Combat Capability Assessment*. CJCSI 3401.01E, May 19, 2014.

US Department of Defense. *Universal Joint Task List*. Last updated February 12, 2018. http://www.jcs.mil/Doctrine/Joint-Training/UJTL/

Zetter, Kim. Countdown to Zero Day: *Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown Publishers, 2014.