



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**DEFINING, MEASURING, AND ANALYZING
DEFENSIBILITY IN THE DEFENSIVE CYBER
OPERATIONS CONTEXT**

by

Bjoern L. Gunnvall Ekstorm

June 2022

Co-Advisors:

Steven J. Iatrou

Richard D. Bergin IV

Second Reader:

Dorothy E. Denning

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.				
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE June 2022	3. REPORT TYPE AND DATES COVERED Master's thesis		
4. TITLE AND SUBTITLE DEFINING, MEASURING, AND ANALYZING DEFENSIBILITY IN THE DEFENSIVE CYBER OPERATIONS CONTEXT			5. FUNDING NUMBERS	
6. AUTHOR(S) Bjoern L. Gunnvall Ekstorm				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) When talking about cyber systems, both researchers and decision makers have used the term "defensibility" widely, but there is no universal definition for it and no method to observe and measure it. This study examines how defensibility can be defined in a defensive cyber operations context, what critical factors constitute it, and how those factors could be measured. This is done by first examining doctrine and research to create a framework of meaning for defensibility. Second, the study proposes seven fundamental capabilities that a defender needs to be able to perform in defensive cyber operations and a set of system attributes that affect those capabilities. Finally, a set of measures for those attributes is proposed to allow defensibility to be observed and measured. The results of this study are a definition of defensibility for the defensive cyber operations context, a list of system attributes that constitute its defensibility, and a set of associated measurements for these attributes. Using these, it is possible to analyze the defensibility of a system to indicate what restrictions a defender might have when conducting operations in the system and the areas where the system needs to improve. This work is the first step in building defensibility into a useful tool that highlights the needs of a defensive actor who conducts dynamic defensive operations in a system, versus the needs of an actor who implements static measures to increase cyber security.				
14. SUBJECT TERMS cyber, cyber defense, defensibility, defensive cyber operations, DCO, DCO-IDM			15. NUMBER OF PAGES 105	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**DEFINING, MEASURING, AND ANALYZING DEFENSIBILITY
IN THE DEFENSIVE CYBER OPERATIONS CONTEXT**

Bjoern L. Gunnvall Ekstorm
Löjtnant, Swedish Navy
BS, Swedish Defence University, 2012

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN NETWORK OPERATIONS AND TECHNOLOGY

from the

**NAVAL POSTGRADUATE SCHOOL
June 2022**

Approved by: Steven J. Iatrou
Co-Advisor

Richard D. Bergin IV
Co-Advisor

Dorothy E. Denning
Second Reader

Alex Bordetsky
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

When talking about cyber systems, both researchers and decision makers have used the term “defensibility” widely, but there is no universal definition for it and no method to observe and measure it. This study examines how defensibility can be defined in a defensive cyber operations context, what critical factors constitute it, and how those factors could be measured. This is done by first examining doctrine and research to create a framework of meaning for defensibility. Second, the study proposes seven fundamental capabilities that a defender needs to be able to perform in defensive cyber operations and a set of system attributes that affect those capabilities. Finally, a set of measures for those attributes is proposed to allow defensibility to be observed and measured. The results of this study are a definition of defensibility for the defensive cyber operations context, a list of system attributes that constitute its defensibility, and a set of associated measurements for these attributes. Using these, it is possible to analyze the defensibility of a system to indicate what restrictions a defender might have when conducting operations in the system and the areas where the system needs to improve. This work is the first step in building defensibility into a useful tool that highlights the needs of a defensive actor who conducts dynamic defensive operations in a system, versus the needs of an actor who implements static measures to increase cyber security.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	PROBLEM AND PURPOSE.....	2
B.	IMPACT	2
C.	RESEARCH QUESTIONS.....	3
D.	DEFINITIONS.....	3
E.	LIMITATIONS.....	4
II.	METHOD	5
III.	LITERATURE REVIEW	7
A.	DEFINITIONS OF DEFENSIBILITY	7
B.	INTERPLAY BETWEEN SYSTEMS AND CYBER OPERATIONS.....	10
C.	CONCLUSIONS	12
IV.	DEFINING DEFENSIBILITY	15
A.	DEFENSE AND DEFENSIVE OPERATIONS	15
B.	CYBER DEFENSE AND DEFENSIVE CYBER OPERATIONS.....	18
C.	ACTIVE DEFENSE MEASURES	24
D.	THE DEFENSIVE ACTOR.....	30
E.	THE DESIGNATED SYSTEM	32
F.	FRAMEWORK OF DEFENSIBILITY	36
V.	OPERATIONALIZING DEFENSIBILITY.....	45
A.	FUNDAMENTAL ACTIVE DEFENSE MEASURES.....	45
B.	SYSTEM ATTRIBUTES	52
1.	Passive Gathering of Data	53
2.	Active Gathering of Data.....	54
3.	Filtration and Correlation of Data	55
4.	Modifying Aspects of the System.....	56
5.	Making Decisions	57
6.	Executing Decisions	58
7.	Summary.....	59
C.	MEASURING DEFENSIBILITY	63
VI.	CONCLUSIONS AND FURTHER RESEARCH.....	71
A.	CONCLUSIONS	71

B.	DISCUSSION	71
C.	RECOMMENDATIONS FOR FURTHER RESEARCH	72
APPENDIX. MAPPING FROM MEASURE TO CAPABILITY		75
LIST OF REFERENCES.....		81
INITIAL DISTRIBUTION LIST		87

LIST OF FIGURES

Figure 1.	Division of tasks and foci in CO. Source: Joint Chiefs of Staff, (2018a, p. II-3)	20
Figure 2.	Elements of a socio-technical system. Adapted from Bostrom and Heinen (1977).	35
Figure 3.	Defensibility framework	43

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Active defense measure capabilities.	50
Table 2.	Defensibility attributes.	59
Table 3.	Defensibility measurements.	64
Table 4.	Measure to capability.	75

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACD	active cyber defense
BDA	battle damage assessment
CCMF	cyber combat mission force
CIA	confidentiality, integrity, and availability
CNMF	cyber national mission force
CO	cyberspace operations
CPF	cyber protection force
CPT	cyberspace protection team
CSSP	cybersecurity service provider
DCO	defensive cyberspace operations
DCO-IDM	defensive cyberspace operations – internal defense measures
DCO-RA	defensive cyberspace operations – response actions
DOD	Department of Defense
DODIN	Department of Defense information network
FCD	fortified cyber defense
HIDS	host-based intrusion detection system
HIPS	host-based intrusion prevention system
IT	information technology
NIDS	network-based intrusion detection system
NIPS	network-based intrusion prevention system
NIST	National Institute of Standards and Technology
NOIR	nominal, ordinal, interval, and ratio
OCOKA	observation and fields of fire, cover and concealment, obstacles, key terrain, and avenues of approach
RCD	resilient cyber defense
YARA	YARA: another recursive acronym, or yet another ridiculous acronym

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I want to thank my advisors, Richard Bergin and Steven Iatrou; I'm glad that you both decided to help me with this passion project of mine, even though it's outside of your respective areas. You are both clearsighted and great thinkers and forced me to untangle my thoughts and express them clearly.

Thank you to Dr. Dorothy Denning, whom I am humbled to have as a second reader. I greatly appreciate your feedback!

Thank you to my colleagues back home. Our long discussions and whiteboard sessions did the mental groundwork for this paper. Let's continue building on it together.

Marianne and Sam, not only did you put up with my long sessions in front of the computer, you supported me during this whole grand adventure. I could not have done this without you.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

According to U.S. Army doctrine, successful defensive operations are characterized by “disruption, flexibility, maneuver, mass and concentration, operations in depth, preparation, and security” (Department of the Army, 2019a, p. 4-1). These principles can also be applied to defensive cyber operations, but their application in practice has not been widely studied. The terms *defensible systems* and *defensible networks* are often used as strategic goals or requirements by senior management when discussing information technology (IT) systems and cyber capabilities (Cyber Operations, 2015; Gorminsky, 2014; Shachtman, 2012; U.S. Strategic Command, 2015; King & Gallagher, 2020). One part that is often included in a system’s *defensibility* is the static measures related to the field of cybersecurity, an area that garners a large amount of research. The second part, however, is less developed and made up of factors related to the *preparation* of the battlespace to enable or support an active cyber defender.

I have spent seven years as a cyber defender, in which I have participated in a range of discussions with technicians, system stakeholders, and senior management about the demands for cyber defensibility, where the lack of a clear operational definition of the term in both doctrine and research has been evident. Focusing only on making a system secure according to principles of cybersecurity can be detrimental to the successful utilization of the capabilities of a cyber defender. Traffic encryption is one example of a measure that can increase the security of a system while at the same time making it harder for a defender. In this example, if no steps are taken to allow defenders to break encryption in a controlled manner, their ability to examine and modify network traffic is restricted, lowering their operational effectiveness and making the system harder to defend.

Establishing a universal definition of cyber defensibility and operationalizing it to determine what system characteristics and related variables are of value for an active defender when conducting operations in blue cyberspace¹ is important to give both

¹ Blue cyberspace, as defined in *Joint publication 3–12: Cyberspace operations*, “denotes areas in cyberspace protected by the U.S., its mission partners, and other areas DOD may be ordered to protect” (Joint Chiefs of Staff, 2018a, p. I-4).

defenders and system stakeholders a better opportunity to accomplish defensible systems together, thus raising the effectiveness of defensive actions and lowering risk. For example, when tasked with defending a system, the defender could use this definition to evaluate the system in terms of what capabilities are possible to employ there and communicate this to stakeholders and decision makers. If any attributes of the system impede the defender's capabilities, these could be pinpointed and communicated.

A. PROBLEM AND PURPOSE

The problem is that the term cyber defensibility in the context of Defensive Cyber Operations is ill defined, especially when describing the characteristics of a network or system that is defensible. The term is often used at a strategic level to signal intent, but the knowledge cyber defenders have about what the requirements on a designated system are is mainly tacit. Furthermore, the cyber defenders themselves lack a common and established vocabulary with which to communicate and measure those requirements.

This is a problem because, without clear definitions, defensibility becomes synonymous with cybersecurity, which can ultimately hinder the realization of the full potential of active cyber defense. Without an accepted universal vocabulary with which to express the capabilities needed to conduct defensive operations, there is a risk of gaps between what defenders are capable of doing under ideal conditions and what is possible to achieve in a given designated system. This can lead to systems that cannot be adequately defended, leadership and stakeholder misconceptions of the status of networks and systems, and underutilization and frustration for cyber defenders.

The purpose of this study is to develop a framework for analyzing and measuring system defensibility in the cyber domain. This includes defining and operationalizing key factors as they apply to preparing the battlespace for an active defender.

B. IMPACT

The primary benefit of this study is that it will provide a common definition of cyber defensibility to allow for better communication among leadership, cyber defenders, and system stakeholders. With the operationalization of critical capabilities, it also provides

a framework of observable variables to start measuring defensibility when evaluating networks or communicating priorities.

Other benefits of this study include promoting the understanding of the gaps that exist between the capabilities of cyber defenders and what they can actually achieve in a given designated system; creating a standard lexicon to improve communication between cyber defenders and IT system stakeholders; giving cyber defenders a model to use when evaluating systems and reporting defense status to decisionmakers; and providing decision makers with clearly operationalized definitions of different aspects and factors of defensibility to enable clearer communication of intent and priorities to system stakeholders.

C. RESEARCH QUESTIONS

How can cyber defensibility be defined in a Defensive Cyber Operations context?

What critical factors and related variables within an analytical framework constitute defensibility for a system in a Defensive Cyber Operations context?

D. DEFINITIONS

Cyberspace: “a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers” (Joint Chiefs of Staff, 2021, p. 55).

Blue cyberspace: “areas in cyberspace protected by the U.S., its mission partners, and other areas DOD may be ordered to protect” (Joint Chiefs of Staff, 2018a, p. I-4). Note that while this study is based on U.S. doctrine and definitions, the aim is for the definition to be usable by a wider audience. Throughout this study, *blue cyberspace* will be used to denote the entirety of the space to be defended, mainly when discussing general concepts and broad capabilities. *Designated system* will be used to discuss an individual system in blue cyberspace that is to be defended in a particular instance.

The U.S. Department of Defense (DOD) Joint Chiefs of Staff (2018a) defines the different types of cyber missions and activities in *Joint publication 3–12: Cyberspace*

Operations (JP 3-12), which will be used to provide the operational context for this study. Defensive Cyberspace Operations (DCO), are divided into Internal Defense Measures (DCO-IDM) and Response Actions (DCO-RA) (Joint Chiefs of Staff, 2018a). This thesis focuses on DCO-IDM, which is defined as missions where “authorized defense actions occur within the defended network or portion of cyberspace” (Joint Chiefs of Staff, 2018a, p. II-4). In *JP 3-12*, the Joint Chiefs of Staff (2018a) also assert the difference between defense and security:

Joint doctrine uses the term “cyberspace security” to distinguish this tactical-level cyberspace action from the policy and programmatic term “cybersecurity” used in Department of Defense (DOD) and United States Government (USG) policy. To enable effective planning, execution, and assessment, doctrine distinguishes between cyberspace security and cyberspace defense actions, a distinction not made in DOD and USG cybersecurity policy, where the term cybersecurity includes the ideas of both security and defense. (p. II-6)

E. LIMITATIONS

Since a global definition needs to be disseminated broadly for it to have an effect, this study will be kept at the unclassified level. This limits the depth that can be addressed when operationalizing cyber defensibility, as it has to focus on broad capabilities rather than specific technical requirements. The reason for this is that specific technical requirements of cyber defenders will outline their capability.

This study focuses on cyber defenders and active defense and leaves out aspects that are solely aimed at static cyber protection. Both are needed for a comprehensive defense and active defense measures often build on sound static protections (Fanelli, 2016).

II. METHOD

As mentioned previously, this study examines cyber defensibility in the context of Defensive Cyber Operations. Defensibility is examined from the perspective of a Cyber Protection Team (CPT), who come from outside of the organizations that work with the designated system on a daily basis (Joint Chiefs of Staff, 2018a). A CPT is a group that is expected to be able to perform qualified defensive actions in any given designated system on short notice (Joint Chiefs of Staff, 2018a). As such, they have requirements for features and capabilities that are outside the normal scope of operations for the system and are often overlooked when assessing system security in daily operations.

This research is conducted in two phases. To develop a definition of defensibility, identify related key factors, and construct framework of meaning, the first phase includes a review and analysis of three categories of sources:

1. Military sources such as doctrines and handbooks enable the identification of the core parts of defensibility. Important questions related to these sources:
 - How are defense and defensive operations defined?
 - How can the preparation aspect of defensive operations be understood in a cyber context?
 - What is the delineation between active and static defense?
2. Current discourse such as press releases, news articles, and policy documents enable the identification of the different values attributed to defensibility. The primary question related to these sources is:
 - What is the general consensus on what problem defensibility as a concept solves?
3. Academic sources enable the identification of what meaning other researchers have assigned to defensibility. The primary questions related to these sources are:

- Is the definition connected with current military theory with regards to defensive operations and cyber operations?
- Does the definition address the problem that defensibility needs to solve? If not, what is missing?

In the second phase of the study, the definition of cyber defensibility is used to further examine and identify characteristics and variables used to measure cyber defensibility. Important considerations during this phase are:

- What constitutes active defensive actions in the cyber domain?
- How does the designated environment support, allow, constrain, or block defensive actions in the cyber domain?
- How can that effect be measured and evaluated?

In this phase, a socio-technical systems perspective is used to ensure that the analysis has a sufficient scope.

III. LITERATURE REVIEW

This review examines two primary threads of literature: definitions of defensibility in a cyber context and interactions between systems and cyber operations. The first thread examines the uses of defensibility in research in a cyber context to find a broadly accepted definition that can be implemented in a narrower defensive cyber operations context. The second thread examines doctrine and research for interactions between systems attributes and cyber operations to find factors and variables that can be related to defensibility.

A. DEFINITIONS OF DEFENSIBILITY

Several studies use the term defensibility when discussing systems in a cybersecurity or cyber defense context, but only a few explicitly define the term and none are dedicated to exploring and operationalizing the term in a military or defensive cyber operations context (Bier & Gutfraind, 2019; Bodeau & Graubart, 2013; Bodeau et al., 2013; Bodeau et al., 2018; Medina, 2016; Ross et al., 2016; Ziring, 2015).

The most extensive definition and use of defensibility is in Ziring's (2015) *The Future of Cyber Operations and Defense*, where its usage is closely linked to the enabling of defensive actions. On the topic of operating in cyberspace, Ziring (2015) states that

effective cyber operations, especially defensive operations, depend on accurate and timely knowledge of the operational context (usually a target network or enterprise), and on the ability of the operational environment to support actions (such as defensive responses). A network that is designed and built to facilitate operations in its own defense, including monitoring and response, is said to be defensible. (p. 3)

On what constitutes cyber defense, *sensors and data collection*, *situational awareness*, and *defense mechanisms* are highlighted as three core elements. In summary, a defensible network has functions that support operations with local and global information and give cyber operators "effective and reliable means to execute actions" (Ziring, 2015, p. 4). While this definition of cyber defensibility is concise and tied strongly to the area of interest for this study, it is not operationalized further to examine what aspects of a system might support what defensive actions.

In *NIST Special Publication 800-160*, Ross et al. (2016) describe a set of multidisciplinary considerations that support the engineering of trustworthy systems. They address perspectives and actions “necessary to develop more defensible and survivable systems, inclusive of the machine, physical, and human components that compose the systems and the capabilities and services delivered by those systems” (p. viii). By including the *human component* as well as processes such as human resources (HR) and knowledge management in their systems security engineering considerations, Ross et al. (2016) take the socio-technical perspective into consideration instead of focusing only on technology. They do not, however, further elaborate on what makes a defensible system. In section 2.3.1. Protection Capability and Security, Ross et al. (2016) define two types of protection capabilities: *active protection* and *passive protection*, with functions that exhibit security protection behavior being the former and the environment in which they, and general system functionality, execute as the latter. This definition is very broad and would encompass characteristics of a system that aid cyberspace security, cyber defense, or both.

Bodeau and Graubart (2013) present an effort to create one unified vocabulary to describe the effects of defensive actions or decisions on adversary behavior in the cyber domain. While they do not define defensibility as part of this vocabulary, they use it as one of three attributes of a system when discussing cyber mission assurance: cyber security, resiliency, and defensibility. In this context, Bodeau and Graubart (2013) define it as “the ability to address ongoing adversary activities” (p. v), without further elaboration. In subsequent work, *Mapping the Cyber Terrain*, Bodeau et al. (2013) expand on this cyber mission assurance trinity in a framework for mapping cyber terrain. The purpose of this framework is to support claims and allow hypotheses to be made regarding cyber security, defensibility, and resiliency solutions (Bodeau et al., 2013). Their aim is to facilitate determination of whether a given claim or hypothesis can be meaningfully applied to a given environment or real-world situation, using a map that is a “representation of knowledge and/or assumptions that determine on influence cyber decisions, i.e., decisions about cyber operations, investments, and architecture intended to improve cyber defensibility, resiliency, and/or security” (p. 1). In this effort, they have the following definition for cyber defensibility: “Cyber defensibility involves causing cyber adversaries

to move more slowly, spend more, and take more risks” (p. 1). This definition is not operationalized further. In a third work, Bodeau et al. (2018) presents a framework of metrics, measures of effectiveness, and scoring for cyber resilience, in which they correlate measuring defensibility with the size of the attack surface, the ability to determine provenance for components, and the ratio of system components that can be selectively isolated.

Bier and Gutfraind (2019) explore the concept of defensibility in more depth, but in a different context. They propose using defensibility as an index in characterizing the overall security of a system alongside resilience, robustness, redundancy, security, and vulnerability. Bier and Gutfraind (2019) define defensibility for systems as “the ability of the defender to reduce the damage to the system below some given initial level (corresponding to any preexisting defenses) using a given level of defense effort” (p. 627) and highlight that it is reliant on factors such as defender and attacker asset valuation and strengths, as well as the nature of the threat. Their definition is focused on cost/benefit—they write that defensibility is “the extent that a modest investment can significantly reduce the damage from an attack or disruption” (p. 626)—i.e., the extent to which the decision to spend resources on protecting a system can be defended from a cost/benefit perspective. Bier and Gutfraind (2019) propose that their defensibility metric be used for system selection when prioritizing a limited defense budget as well as in system design to ensure that systems are prepared for future upgrades while balancing performance, cost, and vulnerabilities. Beyond giving generic examples of defense efforts that can decrease the damage to a system, such as improving security, robustness, or resilience, reducing vulnerability, or increasing deterrence, they do not go into detail about what properties of a system affect defensibility.

Cloud (2007) uses defensibility as an attribute of friendly cyberspace but does not define or elaborate the concept further. The same is true with Fanelli (2016), who, while writing about active and static defense, state that “efforts to ‘maneuver’ or to apply offensive methods for the defense, while appealing, should not get ahead of the fundamental task of optimizing the defensibility of the resources” (p. 61). They do not define defensibility any further.

Finally, Medina (2016) examines cyber defensibility from a legal perspective, striving to support the creation of cybersecurity policies that can be defended if put under scrutiny.

As shown in this review, research contains several different definitions of defensibility in a broad cyber context, but there is no broad consensus and no definition that has been operationalized for a defensive cyber operations context, which is a clear gap in the body of knowledge.

B. INTERPLAY BETWEEN SYSTEMS AND CYBER OPERATIONS

Looking at a broader body of work that examines system attributes in relation to defensive cyber operations and cyber defense, there is a gap in examining system attributes that enable defensive actions.

In their cyberspace operations doctrine *JP 3-12*, the Joint Chiefs of Staff (2018a) define actions and tactics that are utilized to perform defensive operations, but do not address how a designated system should be prepared to best accommodate these—i.e., how to make it more *defensible*. However, in Chapter IV, the Joint Chiefs of Staff (2018a) allude to the concept of defensibility when discussing planning considerations for cyber operations. In this section, they list aspects that affect the timeline of DCO-IDM planning that would also be applicable to the defensibility concept, such as “levels of automation available to manage network posture, availability of security solutions from commercial providers and their licensing requirements, and operational considerations that may impact a defender’s abilities to maneuver or take systems off-line to better manage their protection” (p. IV-2). These considerations are an important driving factor for this study, as a framework for measuring the defensibility of a network in advance of operations will provide planners with better information on how to utilize the resources at their disposal. However, this short list is far from complete in describing all factors that affect the effectiveness of cyber defenders, which is what this research is intended to provide. There is, however, a classified appendix to *JP 3-12* that contains additional planning considerations for cyberspace operations, which is not included in this research (Joint Chiefs of Staff, 2018a, p. A-1). In Chapter IV, section 7. *Assessment of Cyberspace*

Operations, the Joint Chiefs of Staff (2018a) describe how commanders measure progress towards mission accomplishment, but in doing so they take a narrow view that primarily favors Offensive Cyber Operations and is mission focused. They do not address any assessment of the opportunities or limitations offered by characteristics of the designated network in advance of DCO-IDM missions.

In *Measuring Cybersecurity and Cyber Resiliency*, Snyder et al. (2020) propose a framework for the development of metrics to indicate how well a system is expected to perform in a cyber-contested environment. Specifically, they are interested in the survivability and effectiveness of weapons systems. They use the term cybersecurity to signify static countermeasures based on best practices and cyber resilience to signify dynamic actions to respond to an adversary in real time. Thus, defensive actions enabled by cyber defensibility could be contained in his use of cyber resiliency. Snyder et al. (2020) use a socio-technical perspective in that they stress that metrics need to span spatial and temporal dimensions, include hardware, firmware, and software as well as people, organizational performance, and processes, while also proposing to use metrics both at a working level, close to the system, and at an institutional level to assess organizational deficiencies. They propose metrics that are measured on an ordinal maturity scale with five levels, from most immature to highest maturity. At the working level, the metrics proposed by Snyder et al. (2020) are focused on the intersection between (1) an attacker's access, knowledge, capability, and impact and (2) the defender's countermeasures. At the institutional level, their metrics are focused on the ability and tendency of the organization to learn from both failures with an institutional root cause and from best practices of organizations that succeed with minimal institutional failures. Snyder et al. (2020) treat the agent taking defensive actions as part of the system to be assessed, which is something I separate out to account for external cyber defenders stepping in to perform DCO-IDM operations.

Wagner et al. (2017) examine the effects of two types of network-level defensive mitigations on security and mission performance. In their study, they develop a simulation framework to test and measure the effectiveness of mitigations in cyber systems. The measurements are focused on weighing the security gained from the mitigation against the

impact it causes on the mission that utilizes the system in question (Wagner et al., 2017). One important consideration that they note about cyber systems is that they, “like social systems, include human actors and are thus stochastic in nature” (p. 202). This means that two identical systems “under a given set of conditions (e.g., users, attackers, and defense mitigations) will not always lead to the same outcome” (Wagner et al., 2017, p. 202). Their approach to mitigating this is to employ simulations to make recommendations based on probability of outcomes.

In the body of knowledge, there are several sources that examine attributes of a system that offer defensive functions and defensive actions performed by a defender. Some studies take a socio-technical systems approach to examining these attributes, including such factors as the organization and people into their analysis. Doctrine alludes to the effect of system attributes when discussing the planning of defensive cyber operations, but does not address how those effects could be measured. There are no studies on the interaction between a socio-technical system and defender actions.

C. CONCLUSIONS

A thorough review of the literature shows a gap in the body of knowledge in the intersection between the conduct of defensive cyber operations and the attributes of a designated system that may affect those operations. Specifically, while there are several examples of the term *defensible* with regards to systems and system design, there are only a few sources that try to define the term in a defensive cyber operations context and little consensus between them. Only one study, by Ziring (2015), appears to relate cyber defensibility to Defensive Cyber Operations with the goal of enabling more effective defensive operations. There is no clear operationalization of defensibility in a Defensive Cyber Operations context.

As for system-defender interactions, the literature indicates that metrics that are developed to assess aspects that touch on defensibility are often developed with an internal perspective and a focus on the components of the system itself. Hence, it appears that there are no metrics on the ability of a system to accommodate an external CPT that are not a part of the system as a whole. Teams of highly skilled cyber defense operators specialized

in threat hunting or incident handling are a resource that might not be native to the designated system but instead belong to an external organization. As outsiders, they have requirements on system features that are often overlooked when assessing system security since they are not a part of ordinary operations. This study examines the intersection between active defense measures and the designated system that require a measure of defensibility. In doing so, it takes a socio-technical systems perspective. There are several studies that examine aspects of cybersecurity from a socio-technical perspective, but none appear to examine attributes of a socio-technical system that affect the conduct of defensive cyber operations performed by an external CPT.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. DEFINING DEFENSIBILITY

According to the accepted authority on the English language, the *Oxford English Dictionary*, defensible means the ability of something to be defended (Oxford University Press, n.d.b). As such, *defensible* is a simple descriptive term—something either is or is not defensible. However, if we want to examine this deeper and start measuring how well something can be defended, we can use the term *defensibility*, which introduces the notion that there are varying degrees to the ability. This makes the term more complex, as it starts tying into attributes of both the thing itself, the surrounding environment, and the defending actor. It is therefore important to limit our meaning and be precise in our definition.

In order to create a strong definition of cyber defensibility, it is necessary to examine several intermediate concepts and constructs and link them together in a framework of meaning. This chapter begins with a study of military doctrine to establish a foundation of what defense and defensive operations mean. It continues with an examination of the characteristics of the cyber domain and defensive cyber operations in both doctrine and research, followed by the notion of active defense, active defense measures, the defensive actor, and a designated system in defensive cyber operations. The final section examines the literal meanings of defensibility and the uses of the term in policy, research, and discourse to finally synthesize a definition of cyber defensibility as it applies to defensive cyber operations.

A. DEFENSE AND DEFENSIVE OPERATIONS

A definition of *defense* and *defensive operations* in a military context is foundational in building a definition of defensibility. *Encyclopædia Britannica* (n.d.) defines *defense* as “the act of defending someone or something from attack” (definition #1), “something that is used to protect yourself, your country, etc.” (definition #2), or “the things that are done by a country to protect itself from enemies” (definition #4). According to these different definitions, the act of defense can be performed with either active or static measures. Von Clausewitz (1918) writes about defense as a principal form of war and states

that it can be performed with three different motives: *destruction of enemy's force*, *defense of a place*, and *defense of some object* (p. 254).

In *Doctrine for the Armed Forces of the United States (JP 1)*, an operation is defined as “a sequence of tactical actions with a common purpose or unifying theme” (Joint Chiefs of Staff, 2017, p. I-9). Building on the definition of defense, we can then define a defensive operation as a sequence of tactical actions with the aim of protecting something from attack.

As expected, defensive operations in a military context are already well studied in military science and described in doctrine. According to U.S. Army doctrine, “a defensive operation is an operation to defeat an enemy attack, gain time, economize forces, and develop conditions favorable for offensive or stability operations” (Department of the Army, 2019b, p. 3-4). This definition reflects on the fact that defense does not exist in a vacuum, but is intimately tied to a larger context where offensive operations, as opposed to defensive ones, are widely considered to be essential to reach the conclusion of military activities (Clausewitz, 1918, p. 255; Department of the Army, 2019a, p. 4-1). To execute operations, commanders make use of seven different joint warfighting functions: “command and control, [...] intelligence, fires, movement and maneuver, protection, sustainment, and information” (Joint Chiefs of Staff, 2017, p. I-18). Furthermore, the Department of the Army (2019a) also lists seven characteristics of defensive operations: “disruption, flexibility, maneuver, mass and concentration, operations in depth, preparation, and security” (p. 4-1). Those characteristics are primary features of defensive operations that need to be considered for a successful defense. The Department of the Army (2019a) describe *disruption* as “actions that desynchronize an enemy force’s preparations” (p. 4-1), such as “deceiving or destroying enemy reconnaissance forces, breaking up combat formations, separating echelons, and impeding an enemy force’s ability to synchronize its combined arms” (p. 4-1). *Flexibility* is described as the ability to make adaptable plans where the focus can be shifted and resources reallocated accordingly (Department of the Army, 2019a). This requires the planning of “battle positions in depth and the use of reserves” (Department of the Army, 2019a, p. 4-2). The Department of the Army (2019a) state that *maneuver* allows the defender “to achieve and exploit a position

of advantage over an enemy force” (Department of the Army, 2019a, p. 4-2). This is an example of the defense using elements from the offense (Department of the Army, 2019a). *Mass and concentration* is the principle to focus the defending force at “specific locations to support their decisive operations” (Department of the Army, 2019a, p. 4-2) in order to be able to overwhelm the enemy. *Operations in depth* is “the simultaneous application of combat power throughout an area of operations” (Department of the Army, 2019a, p. 4-2), which prevents enemy forces from maintaining their tempo. On *preparation*, the Department of the Army (2019a) state that

defending units prepare their [area of operations] before attacking enemy forces arrive, or they establish the defense behind a force performing a security operation. [...] Defending forces study the terrain, study enemy forces, and prepare engagement areas. They combine natural and man-made obstacles to canalize attacking forces into those engagement areas. Defending forces place information collection assets throughout their [area of operations] to provide intelligence and early warning of enemy actions. Defending forces improve the survivability of their units by constructing field fortifications, using camouflage, and dispersing. Defending forces continue rehearsals and preparations until close combat begins (p. 4-2).

Security is described as the “performance of security, protection, information operations, and cyberspace and electronic warfare tasks” (Department of the Army, 2019a, p. 4-2) to “prevent enemy intelligence, surveillance, and reconnaissance assets from determining friendly locations, strengths, and weaknesses” (p. 4-2) and “provide early warning and continuously disrupt enemy attacks” (pp. 4-2 – 4-3).

Based on these perspectives, the core definition of defense that will be used in this study is: active or static measures taken to protect some asset from an attack.

Defensive operations are groups or sequences of tactical actions made to protect assets from attack, using either static or active measures. To execute operations, commanders use warfighting functions that are categorized as *command and control*, *movement and maneuver*, *intelligence*, *fires*, *sustainment*, *protection*, and *information* (Joint Chiefs of Staff, 2017, p. I-18). While utilizing these functions, it is important to consider the characteristics of defense: “disruption, flexibility, maneuver, mass and

concentration, operations in depth, preparation, and security” (Department of the Army, 2019a, p. 4-1).

B. CYBER DEFENSE AND DEFENSIVE CYBER OPERATIONS

While cyber defense and defensive cyber operations are defined in research and doctrine, we will start by building on the previous section for a baseline description that can be expanded. In this perspective, cyber defense would simply be defense that is concerned with assets in cyberspace and using measures enabled by cyberspace. Defensive cyber operations would be defined as defensive operations that protect cyber assets or use static or active measures enabled by cyberspace. However, by examining doctrine and research, it is possible to add several dimensions to these definitions.

In the *DOD Dictionary of Military and Associated Terms*, the Joint Chiefs of Staff (2021) define both *cyberspace defense* and *defensive cyberspace operations*:

Cyberspace defense – Actions taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach cyberspace security measures and include actions to detect, characterize, counter, and mitigate threats, [...] and to restore the system to a secure configuration (p. 55).

Defensive cyberspace operations – Missions to preserve the ability to utilize blue cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity (p. 60).

These definitions offer a departure from other concepts of defense described in the literature, as they focus on defense as an active effort separate from static security measures. Furthermore, the Joint Chiefs of Staff (2018a, 2021) divide DCO into *internal defense measures* and *response actions*, which will be examined further in the following section.

A third aspect of cyberspace operations is defined in the *DOD Dictionary of Military and Associated Terms: Department of Defense Information Network (DODIN) Operations* (Joint Chiefs of Staff, 2021, p. 61). While also concerned with blue cyberspace, DODIN operations contain tasks such as configuring, securing, operating, maintaining, extending and sustaining DODIN (Joint Chiefs of Staff, 2021, p. 61). They are concerned

with the everyday handling of blue cyberspace, and as such they cover the static aspects of cyberspace security (Joint Chiefs of Staff, 2018a, pp. II-2–II-3, pp. II-5–II-6).

As mentioned previously, the primary doctrine concerned with cyberspace operations is *JP 3-12*, which define defensive cyberspace operations as missions that are

executed to defend the DODIN, or other cyberspace DOD cyberspace forces have been ordered to defend, from active threats in cyberspace. Specifically, they are missions intended to preserve the ability to utilize blue cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity. (Joint Chiefs of Staff, 2018a, p. II-3)

Furthermore, “DCO missions are conducted in response to specific threats of attack, exploitation, or other effects of malicious cyberspace activity” (Joint Chiefs of Staff, 2018a, p. II-3), and they “include outmaneuvering or interdicting adversaries taking or about to take actions against defended cyberspace elements, or otherwise responding to imminent internal and external cyberspace threats” (Joint Chiefs of Staff, 2018a, p. II-4).

Further, the Joint Chiefs of Staff (2018a) state that “DCO missions, which defeat specific threats that have bypassed, breached, or are threatening to breach security measures” differ “from DODIN operations, which endeavor to secure DOD cyberspace from all threats in advance of any specific threat activity” (p. II-3).

The division of tasks and internal/external foci in cyberspace operations is shown in Figure 1. It clearly shows that while characterized as a part of DCO, DCO-RA utilizes actions outside of the cyberspace defense category and has an external focus, outside blue cyberspace.

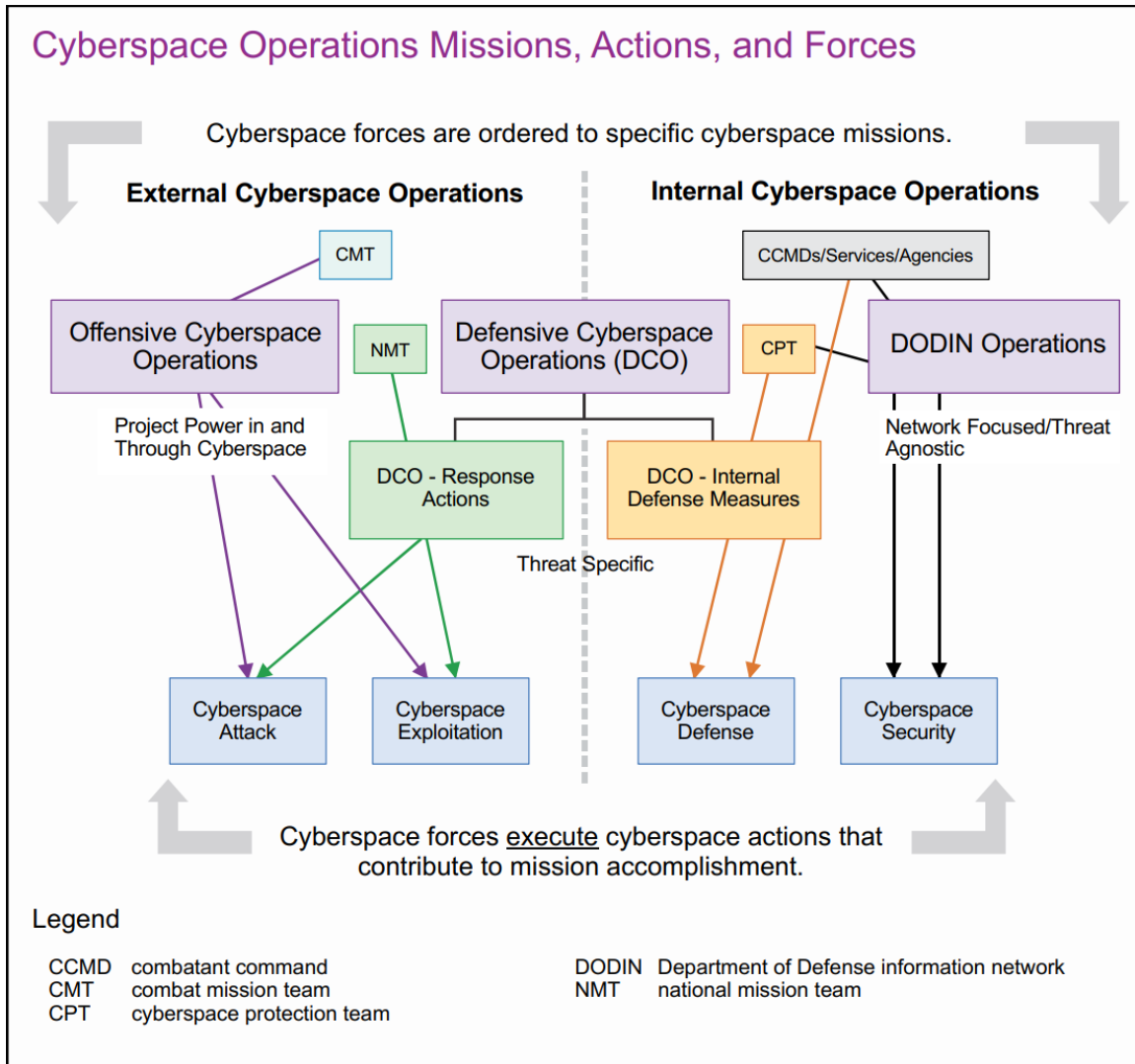


Figure 1. Division of tasks and foci in CO. Source: Joint Chiefs of Staff, (2018a, p. II-3)

When discussing the warfighting functions that make up defense and defining the *protection* warfighting function, the Department of the Army (2019b) and Joint Chiefs of Staff (2018b) include the tasks of cyberspace protection and defense. The purpose of the protection function is to “preserve the force so the commander can apply maximum combat power to accomplish the mission” (Department of the Army, 2019b, p. 5-6). To this effect, one goal of cyberspace defense is to protect and preserve cyber assets so that they can support missions. However, while cyberspace defense is a task under the protection

function that is used to conduct operations, a defensive cyber operation will need to consider all six warfighting functions in and of itself.

In conclusion, U.S. doctrine defines cyberspace defense as active efforts to counter specific threats that have bypassed or are threatening to bypass cyberspace security measures in blue cyberspace. Cyberspace defense includes actions such as detection, characterization, countering and mitigating threats, and the restoration of the system to a secure configuration. While some offensive actions are included under the DCO concept in the form of DCO-RA missions, they have an external focus and do not utilize cyber defense actions.

In *Information Warfare and Security*, published in 1999, Denning uses the term information warfare to include defensive cyberspace operations and states that information warfare defenses can be categorized in six general areas: *prevention, deterrence, indications and warnings, detection, emergency preparedness, and response*. The areas are described as follows:

- Prevention: “serves to keep an attack from occurring in the first place, usually by denying the offensive party access to the target information resource” (Denning, 1999, p. 38).
- Deterrence: “seeks to make an attack unattractive but not necessarily prevent it” (Denning, 1999, p. 38).
- Indications and warning: “aim to recognize a potential attack before it occurs or during the early stages, so that other measures can be taken to avert the attack or diminish its effect” (Denning, 1999, p. 38).
- Detection: “has a similar objective [to indications and warning] but generally refers to the use of monitors to recognize an attack after it has started” (Denning, 1999, p. 39).
- Emergency preparedness: “refers to a capability to recover and respond to attack after they occur” (Denning, 1999, p. 39).

- Response: “refers to actions that are taken after an attack occurs”
(Denning, 1999, p. 39).

Several of the associated measures described by Denning (1999) are concerned with cyberspace security, i.e., static measures, and strategic solutions, such as deterrence through legal means. As such, they do not fit with the definition of cyber defense established by the U.S. military. While strategic deterrence plays a role, it is beyond local commands and cyber defenders to affect it. Other areas, such as indications and warning, detection, and response correspond closely to the military definition of cyber defense.

In a 2007 study, Cloud argues that a defensive cyber doctrine can be broken down into three broad functional areas: posturing, maneuver, and recovery (p. 72). Broadly, they correlate to preparations before, actions in response to, and controls after an attack (Cloud, 2007). Cloud (2007) argues that cyber defense needs to be dynamic and not rely only on static fortifications, that defenders need to “take the initiative in order to outmaneuver their attackers in cyberspace” (p. 74). In this view, his definition closely mirrors that of traditional military views on defense, such as that expressed by the Department of the Army (2019a) in *Offense and Defense* (ADP3-90) when describing the *maneuver* characteristic of defense (p. 4-2). In comparison to U.S. doctrine on cyberspace operations, Cloud’s (2007) definition also asserts the importance of active measures but still maintains that what he calls *fortifications*, i.e., static measures, are a part of defense. Cloud’s concept of posturing can be correlated with the *preparation* characteristic of defensive operations and is interesting in the context of this study, as measures taken to enable or support defensive measures could be argued to increase defensibility. On a larger scale, however, posturing could also be taken to mean static measures that aim to increase cyberspace security. Cloud (2007) does not pose a time limit for posturing, meaning that it should be ongoing until such a time that an attack is imminent or under way.

Fanelli (2016) argues that much discussion of the application of military concepts of offense and defense in cyberspace are “abstracted from the technological reality of the domain” (p. 53) and asks the question what it really means “to conduct offensive or defensive operations” (p. 53) in the cyber domain. In this study, he examines traditional

definitions of offense and defense found in military science and applies them to the cyber domain, referencing fundamental concepts in information system security. He does this in order to provide the concepts of cyber defense and offense with “grounding in the technological reality of cyberspace” (p. 53). Fanelli (2016) defines defense in the cyberspace domain as a contest that “seeks to retain control of information resources in order to maintain cyberspace power or to thwart an opponent’s attempts to gain power” (p. 54). He delves further into the notion of control over information resources and uses a well-established information security model called the CIA triad, consisting of Confidentiality, Integrity, and Availability, to frame the discussion (Fanelli, 2016; Fruhlinger, 2020). This definition focuses on information resources and the preservation of cyberspace-enabled capability as well as actions to counter ongoing enemy activities in cyberspace.

One aspect that sets the cyber domain apart from the physical domain is the speed and relative ease with which terrain can be created or modified (Pantin, 2017; Kallberg, 2017). This aspect, paired with the fact that attacks can be performed at machine speed (Kallberg, 2017), puts a stronger emphasis on the preparation characteristic of defensive cyber operations; since DCO-IDM takes place in blue cyberspace, where we exert control over this malleable terrain, preparations are not only important, they are key to the successful employment of defensive actions. However, while the terrain is flexible, this does not mean that there are no constraints as to what changes can be made in the name of DCO. This is an area where DCO-IDM are intrinsically linked to DODIN operations (Joint Chiefs of Staff, 2018b, p. III-26). Systems are created for operational purposes and the goal of defensive operations must be to protect that purpose within the operational requirements set by the system. A parallel can be drawn here to military ground operations, where a defense can be set up with different requirements or goals in mind: the goal can be to deny the enemy use of some terrain, to deny the enemy the ability to fire upon some terrain, to ensure that we can use the terrain, to delay the enemy’s passage through the terrain, etc. Similar operational requirements need to be defined for DCO, such as what parts of a system is the enemy allowed to interact with and in what way. If the goal is to deny the enemy access completely at any cost, then the system can be brought offline, but if the goal is to ensure continued operations at all costs, the issue becomes more complicated. This is

where the CIA triad is often brought into the discussion to facilitate clearer communication of the priorities of a system regarding what aspects need to be protected.

Based on the original definition from the start of this section, U.S. doctrinal definitions, and the perspectives expressed in research, this study defines cyberspace defense as: defense that is aimed at protecting assets in or capabilities enabled by cyberspace, using active measures realized in cyberspace. Cyberspace defense, which is active, is separated from cyberspace security, which is static in that it is concerned with defeating specific threats that have bypassed, breached, or are threatening to breach security measures, whereas cyberspace security is concerned with threat-agnostic static measures.

Defensive cyberspace operations will, for the sake of this study, only be defined as those operations that have an internal focus, i.e., on blue cyberspace. Thus, DCO-RA will not be included when considering cyber defensibility.

C. ACTIVE DEFENSE MEASURES

When establishing the definition of cyberspace defense, the delineation between active and static defense measures plays an integral role. This section examines doctrine and research to determine what constitutes *active defense* and *active defense measures* in a defensive cyberspace operations context.

As noted in the previous section, U.S. military doctrine delineates between cyberspace security and cyberspace defense in that they are concerned with specific threats and active measures and threat-agnostic and static measures, respectively (Joint Chiefs of Staff, 2018b, 2018a, 2021). The Department of the Army also declares that:

A defending force does not wait passively to be attacked. A defending force aggressively seeks ways of attriting and weakening enemy forces before close combat begins. A defending force maneuvers to place enemy forces in a position of disadvantage and attacks those enemy forces at every opportunity. The static and mobile elements of a defense combine to deprive enemy forces of the initiative. A defending force contains enemy forces while seeking every opportunity to transition to the offense. (Department of the Army, 2019a, p. 4-1)

While this statement is concerned with the physical domain, the spirit of it can be seen in the definitions of cyberspace defense and its focus on actively opposing an attack.

In *JP 3-12*, the Joint Chiefs of Staff (2018a) separate DCO into Internal Defense Measures, or DCO-IDM, and Response Action, or DCO-RA. While DCO-IDM is focused on the internal, or blue, cyberspace and encompass defense in the classic sense, DCO-RA is centered on actions taken outside of the defended network and include offensive actions taken to halt a specific threat (Joint Chiefs of staff, 2018a, pp. II-3–II-4). This definition of DCO-RA is close to the definition of Active Cyber Defense proposed by Lachow (2013) and Denning (2013). Dewar (2014), however, includes aspects of both DCO-IRM and DCO-RA in his definition of Active Cyber Defense.

When discussing cyberspace defense, Fanelli (2016) also makes a distinction between static and active defense. He describes static defense as the foundational security measures that are put in place to create a secure system, but points out that while necessary, static defense is not sufficient on its own for a fully effective defense (Fanelli, 2016). He argues that “a skilled and persistent cyberspace adversary will eventually find and exploit some weakness in a purely static defense” (Fanelli, 2016, p. 61). He elaborates that “active defense measures are needed to defeat these more capable adversaries” (p. 61) that have bypassed the static defenses. Fanelli (2016) lists three examples of active defense measures: “hunting on defended information resources for indicators of compromise, dynamically altering access controls in response to adversary activity, or deploying decoys to mislead and to redirect attackers” (p. 61).

This stance is closely echoed by Ziring (2015), who argues that “secure design and configuration can and do defeat attackers and raise their costs; plus, they provide critical capabilities to enable cyber operations. Nevertheless, operations will still be necessary” (p. 5).

Dewar (2014) goes one step beyond the classic use of static and active defense and defines three separate elements that work in tandem to protect a system: Active Cyber Defense (ACD), Fortified Cyber Defense (FCD), and Resilient Cyber Defense (RCD). Out of these three, FCD and RCD are concerned with static security measures and continuity

of operations, respectively, and will not be considered in this study (Dewar, 2014). He defines ACD as

a method of achieving cyber security predicated upon the deployment of measures to detect, analyse [sic], identify and mitigate threats to and from cyberspace in real-time, combined with the capability and resources to take proactive or aggressive action against threat agents in those agents' home networks. (p. 18)

This is a combination of two prevailing meanings of active defense—deployed and proactive actions in blue cyberspace and aggressive actions in an adversary's cyberspace. In U.S. military doctrine, these are divided into DCO-IDM and DCO-RA.

In this study, the definition of active defense is based on U.S. doctrine as well as Fanelli (2016) and Ziring (2015): Active defense is a dynamic cyber defense in blue cyberspace whose purpose is to counter attacks that have bypassed or are threatening to bypass static defenses. Thus, the key difference between static and active defense is whether the measure is permanent or temporary. In this perspective, defenses that are a part of the system are static, whether they are a technical component, a policy, or personnel tasked with performing defensive actions on a recurring basis. Personnel performing continuous analysis of data from permanent sensors is a part of static defenses; an intrusion prevention system is a static defense; and if there is a policy that specifies that a vulnerability scanner should run with a certain array of tests at a certain time interval, this too is a static defense. What makes a defense active is the notion that it uses measures that are not built into the system. In this sense, we could think of static defense measures as parts of the system itself and active defense measures as outside forces coming in and affecting the system in some way as a response to a perceived or realized threat.

Active defense is dynamic and focused on countering attacks that have bypassed static defenses using different measures. The rest of this section is concerned with examining what categories of measures can be taken to execute active defense. In the *Cyberspace Operations Doctrine JP 3-12*, the Joint Chiefs of Staff (2018a) state that

DCO-IDM of the DODIN is authorized by standing order and includes cyberspace defense actions to dynamically reconfirm or reestablish the security of degraded, compromised, or otherwise threatened DOD

cyberspace to ensure sufficient access to enable military missions. For compromised DODIN elements, specific tactics include rerouting, reconstituting, restoring, or isolation. (p. II-4)

Further, DCO-IDM includes “pro-active and aggressive internal threat hunting for advanced and/or persistent threats, as well as the active internal countermeasures and responses used to eliminate these threats and mitigate their effects” (Joint Chiefs of Staff, 2018a, p. II-4). One point to note in *JP 3-12* is that DCO-IDM does not require any indicators of compromise and can thus be pro-active in nature, explaining the definition of active defense that the attack being countered could only be threatening to bypass static defenses.

In *JP 3-12*, the Joint Chiefs of Staff (2018a) state that any cyber operations mission “requires completion of specific tactical-level actions or tasks that employ cyberspace capabilities to create effects in cyberspace” (p. II-5). In the definition of cyberspace defense actions, they list the categories of actions:

- Detection
- Characterization
- Countering
- Mitigation
- Restoration (p. II-6)

The Joint Chiefs of Staff (2018a) also define countermeasures in cyberspace as a special area with the objective to impair the operational effectiveness of enemy activity (p. II-7). Countermeasures can be performed internally to the defended terrain and can be used preemptively or reactively (Joint Chiefs of Staff, 2018a, p. II-7). They also give as an example “internal countermeasures [that] are cyberspace defense actions taken as part of a DCO-IDM mission; for example, closing router ports being used by an adversary for unauthorized access or blocking malware that is beaconing out of the DODIN” (Joint Chiefs of Staff, 2018a, p. II-7).

Ziring (2015) describes three core elements of cyber defense that he argues are especially important for cyber operations:

1. Sensors and data collection—cyber operations must be supported with accurate information about the particular networks being defended, but also about the global context. Sensors emplaced in a defensible network are essential for the local view. For the global context, it will be necessary to fuse multiple sources: commercial reputation data, threat intelligence, and partner security posture.
2. Situational awareness—collected data must be analyzed to produce coherent and actionable information to support operational decisions. Today's system logs, sensors, and intelligence sources provide large volumes of data; a key aspect of analysis is to filter out noise and to present the most relevant results to operators. Big data analytic technology can provide an effective platform for situational awareness.
3. Defense mechanisms—accurate situational awareness informs action, but cyber operators need effective and reliable means to execute actions. A defensible network includes specifically designed and deployed mechanisms for controlling the assets that comprise the network, as well as orchestration for applying multiple mechanisms in concert. (p. 4)

These elements contain measures that are aimed at detection, correlation, and analysis of data, and mitigation and response actions.

In his study on defensive cyber doctrine, Cloud (2007) defines his proposed core functions for defense as:

- Posture:

Posturing encompasses proactive and reactive actions that increase the survivability of forces in the event of an attack. [...] Posturing tasks include the employment of cover, concealment, dispersal, camouflage, hardening, redundancy, and deception (e.g., decoys) in combination to increase the survivability of friendly cyberspace. (Cloud, 2007, p. 73)

- Maneuver:

Maneuver encompasses proactive and reactive actions taken in response to and during attacks. It also includes offensive and defensive maneuvers to engage with and/or retreat from the enemy. From the defensive perspective, the purpose of maneuvering is to preserve friendly combat power. The basic maneuvering tasks [...] include attacking (the source), defending (fighting in place), relocating (moving to a more advantageous or less vulnerable portion of cyberspace like a redundant command-and-control node or to a

more secure network), augmenting (to shore up defenses), withdrawing (shutting down or abandoning networks or systems), or delaying (any action that buys time for friendly cyber forces to take other actions). Maneuver also implies that defenses should not be dynamic and should not solely rely on static fortifications, as is the accepted methodology today. Cyber defenders must be creative and take the initiative in order to outmaneuver their attackers in cyberspace. (Cloud, 2007, p. 74)

- Recover:

The recover function encompasses actions taken to recover and reconstitute combat capabilities. Recover includes performing battle damage assessment (BDA), repairs, reconstitution, and emergency containment of extreme damage to mitigate its impact on the entire force. (Cloud, 2007, p. 74)

Based on the perspective described in this section, active defense measures are divided into five main categories and one supporting category for the purpose of this study:

- Detection: measures to detect an ongoing or imminent attack. Discussed in Dewar (2014), Fanelli (2016), Joint Chiefs of Staff (2018a), and Ziring (2015).
- Analysis: measures to gather and analyze data regarding an attack that has occurred. Discussed in Dewar (2014), Fanelli (2016), Joint Chiefs of Staff (2018a), and Ziring (2015).
- Mitigation: measures to remediate effects of an attack that has occurred or to remove avenues through which it can be realized. Discussed in Cloud (2007), Dewar (2014), Fanelli (2016), Joint Chiefs of Staff (2018a), and Ziring (2015).
- Response: measures to counter an attacker's actions. Discussed in Cloud (2007), Fanelli (2016), Joint Chiefs of Staff (2018a), and Ziring (2015).
- Restoration: measures to restore adequate capability to the designated system. Discussed in Cloud (2007) and Joint Chiefs of Staff (2018a).
- Command and control: not an active defense measure in and of itself, but a supporting function. It is the "exercise of authority, responsibility, and

direction by a commander [...] to accomplish the mission” (Joint Chiefs of Staff, 2017, p. I-18), i.e., the ability to make and execute decisions in the conduct of operations. Discussed in Joint Chiefs of Staff (2018a).

These categories can also be applied to static defense measures, with the difference being that static measures are built into the system design, whether such measures take the shape of a technological solution or a process. Active defense measures are temporary, dynamic, and brought to affect the system from the outside during a certain period. Static measures are business as usual, ordinary, while active measures are extraordinary, as in something that deviates from the norm of the system.

Active defense is a dynamic cyber defense in blue cyberspace whose purpose is to counter attacks that have bypassed or are threatening to bypass static defenses, using active measures to detect and analyze threats, mitigate attack effects, respond to attacker actions, and restore adequate system capability.

D. THE DEFENSIVE ACTOR

A key component of defensibility as a concept of active defense is the defensive actor required to perform the defense. This section examines doctrine and research to establish a definition of the defensive actor whose capacity will be affected by the defensibility of a system.

In *JP 3-12*, the Joint Chiefs of Staff describe the Cyber Mission Force, which consists of three elements:

1. The Cyber Protection Force (CPF) conducts CO for internal protection of blue cyberspace (Joint Chiefs of Staff, 2018a). It consists of Cyber Protection Teams that are “organized, trained, and equipped to defend assigned cyberspace in coordination with and in support of segment owners, cybersecurity service providers (CSSPs), and users” (Joint Chiefs of Staff, 2018a, p. I-9).
2. The Cyber National Mission Force (CNMF) “conducts CO to defeat significant cyberspace threats to the DODIN and, when ordered, to the

nation” (Joint Chiefs of Staff, 2018a, p. I-9). The CNMF consists of National Mission Teams, National Support Teams, and “national-level CPTs for protection of non-DODIN blue cyberspace” (Joint Chiefs of Staff, 2018a, p. I-9).

3. Cyber Combat Mission Force (CCMF) “conducts CO to support the missions, plans, and priorities of the geographic and functional CDRs” (Joint Chiefs of Staff, 2018a, p. I-9).

According to *JP 3-12*, many defensive actions conducted as DCO-IDM are performed by personnel who are responsible for DODIN operations in accordance with standing orders to restore security (Joint Chiefs of Staff, 2018a, p. II-8). According to the definition of active defense in the previous section, this would make those actions a part of static defense measures, as they are supported by standing procedures, performed by personnel permanently assigned to the system, and as such can be regarded as built into the system. But on more advanced defensive operations, the Joint Chiefs of Staff (2018a) state that

if discovery and mitigation of malicious cyberspace activity requires expertise beyond that available to the network operator and/or the [internet service provider], CPTs may respond to provide support conducting cyberspace defense actions, either remotely or by deploying to the affected location. [...] National-level CPT support can be extended to defend non-DOD mission partners or critical infrastructure networks. (p. II-8)

This indicates that CPTs are generally not a permanent part of the daily operation of a designated system.

In this study, the defensive actor from whose perspective defensibility will be evaluated is a CPT in either CPF or CNMF. Their task, as described in doctrine, is to conduct defense in blue cyberspace. They are tasked with defending a designated portion of cyberspace using active defense measures as a temporary response to an attack or threat.

A defensive actor has certain cyberspace capabilities whose execution can be affected by attributes of the designated system. At the intersection of these capabilities and

what the designated system allows or supports lies the overall defensive posture of a system.

E. THE DESIGNATED SYSTEM

In order to bound the definition of defensibility, the designated system needs to be defined, since it is the entity whose attributes we will be measuring. This section begins with examining the concept of terrain in cyberspace and the layers of cyberspace as defined by U.S. military doctrine, and closes with how a designated system could be understood from a socio-technical systems perspective.

Bodeau et al. (2013) propose a framework for mapping cyber terrain and defines such a map as “a representation of knowledge and/or assumptions that determine or influence cyber decisions” (p. 1). In their framework, they describe cyber terrain using three characteristics: threat, technology, and operations (Bodeau et al., 2013). In this definition, Bodeau et al. include adversary characteristics, which is not done in this study. In *JP 3-12*, the Joint Chiefs of Staff state that traditional military aspects of terrain analysis following the OCOKA acronym—Observation and fields of fire, Cover and concealment, Obstacles, Key terrain, and Avenues of approach—still apply to cyberspace, and they give examples of how those aspects can be understood in the cyber domain (Joint Chiefs of Staff, 2018a, p. I-6 – I-7):

- Observation and fields of fire: “Cyberspace observation and fields of fire refer to areas where network traffic can be monitored, intercepted, or recorded” (p. I-7).
- Cover and concealment: “Cover and concealment may refer to hidden IP addresses or password protected access” (p. I-7).
- Obstacles: “Obstacles in cyberspace may include firewalls and port blocks” (p. I-7).
- Key terrain: “Examples of potential key terrain in cyberspace include access points to major lines of communications (LOCs), key waypoints for

observing incoming threats, launch points for cyberspace attacks, and mission-relevant cyberspace terrain related to critical assets” (p. I-7).

- Avenues of approach: “Avenues of approach can be analyzed by identifying nodes and links, which connect endpoints to specific sites” (p. I-7).

The Joint Chiefs of Staff (2018a) argue that *key terrain* in cyberspace is “analogous to key terrain in the physical domains in that holding it affords any combatant a position of marked advantage” (p. I-6), but that cyberspace is special in that these localities also contain a virtual component, meaning that they are dynamic and volatile, following the reasoning expressed by Pantin (2017) and Kallberg (2017). Pantin argues that the malleability of cyberspace affects maneuverability in cyber operations: “There is no set area for engagement and the route to a target can change in the blink of an eye as the enemy has the potential to change the configuration of the battlefield at any time, making maneuverability a challenge” (2017, p. 41). Kallberg (2017) argues that this is an effect of the relative lack of object permanence in cyberspace as compared to the other domains, a characteristic that undermines the traditional concept of maneuver (pp. 81–82). Hobbs (2007) and Raymond et al. (2014) also study the application of OCOKA and the concept of key terrain in cyberspace and elaborate even further. Hobbs (2007) describes how OCOKA can be used for terrain analysis in cyberspace for both defensive and offensive military operations. However, when describing each element of the abbreviation, he only provides examples that are offensive-focused and gives no regard to the conduct of active defense. Hobbs (2007) also only considers the technical aspects of a system as terrain and gives examples of terrain features only on the logical plane. Raymond (2014), on the other hand, argues that “key terrain in cyberspace exists at all of the cyberspace planes, which include the geographic, physical, logical, cyber persona, and supervisory planes” (p. 287). Raymond expands further on the OCOKA acronym to add examples related to defensive operations, but still maintains a focus on terrain as only the technical side of a socio-technical system. Applegate et al. (2017) criticize the approach of several other researchers, including Raymond (2014) and Bodeau et al. (2014), that examines key terrain in

cyberspace. They state that previous research is mainly focused on the terrain itself and not on how missions and operational requirements affect what parts of the terrain are, in fact, key.

To help with the planning and execution of cyber operations, *JP 3-12* uses a model of cyberspace divided into three interrelated layers: physical network, logical network, and cyber-persona (Joint Chiefs of Staff, 2018a, pp. I-2–I-3). The physical layer “consists of the IT devices and infrastructure [...] that provide storage, transport, and processing of information within cyberspace” (Joint Chiefs of Staff, 2018a, pp. I-2–I-3). Interaction with components at the physical layer may be leveraged to gain logical access (Joint Chiefs of Staff, 2018a). The logical layer consists of network elements that are linked to each other “in a way that is abstracted from the physical network, based on the logic programming (code) that drives network components” (Joint Chiefs of Staff, 2018a, p. I-3). What this means is that the relationships are not based on whether nodes are connected using physical links, but rather their ability to connect to each other and exchange or process data (Joint Chiefs of Staff, 2018a). The cyber-persona layer deals with representations of actor or entity identities in cyberspace, such as user accounts, and their relationships to each other. These three layers, while dealing with different abstraction levels, are all still concerned with the technical side of a socio-technical system and can be used to aid analysis when assessing technological aspects of a designated system.

As just described, models for assessing the operational environment in cyber operations are primarily concerned with the technical domain and treat cyberspace as one cohesive whole that can be separated into blue, grey, and red cyberspace. But even within these three groups, cyberspace consists of individual, heterogenous networks and systems that are not owned and operated by one single entity. This calls for the need to assess not only technical aspects but also broader socio-technical aspects of each individual system that is to be defended. Notably, *NIST Special Publication 800-160: Systems Security Engineering*, by Ross et al. (2016), “addresses the engineering-driven perspective and actions necessary to develop more defensible and survivable systems” (2016, p. viii). In doing so, they include “machine, physical, and human components that compose the system and the capabilities and services delivered by those systems” (p. viii), illustrating

that a broader perspective is necessary when evaluating system attributes that affect system security and cyber defense. As already mentioned, this study uses a socio-technical systems approach to address these issues. When assessing attributes of a designated system, this study uses a model based on Leavitt's Diamond (Leavitt, 1965), modified for socio-technical systems by Bostrom and Heinen (1977). The use of this model is intended to assist in finding attributes of a designated system that affect its defensibility without limiting the analysis to only examining technological aspects. As shown in Figure 2, the model consists of the elements *Structure*, *People*, *Technology*, and *Tasks*, with structure and people in the social subsystem and technology and tasks in the technical subsystem (Bostrom & Heinen, 1977; Leavitt, 1965).

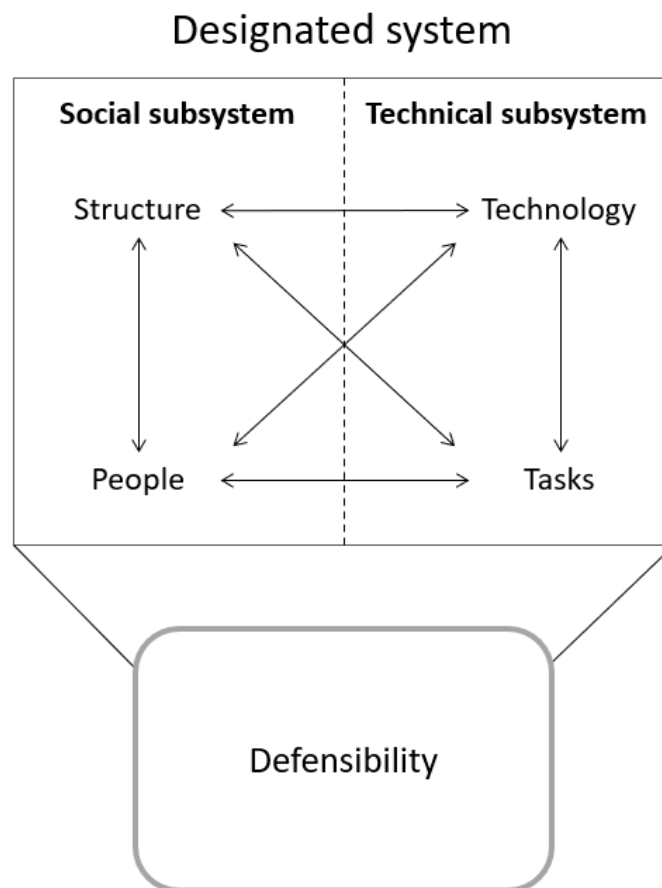


Figure 2. Elements of a socio-technical system. Adapted from Bostrom and Heinen (1977).

In this study, *structure* is used to describe factors related to the hierarchical construction of an organization, layout of departments and internal relationships, coordination, and communication patterns, as well as responsibilities (Bostrom & Heinen, 1977; Leavitt, 1965). The *people* element describes factors related to employees in the organization, specifically their human resource value—skills, competencies, knowledge, and efficiency in performing their tasks (Bostrom & Heinen, 1977; Leavitt, 1965). The *technology* element refers to the hardware, software, configuration, and data that support the organization’s mission (Bostrom & Heinen, 1977; Leavitt, 1965). *Tasks* describe two parts: the tasks that individual employees are assigned within their jobs and the organization’s goals on the tactical, operational, and strategic level, which involves what needs to be done in order to achieve a certain goal of the organization (Bostrom & Heinen, 1977; Leavitt, 1965). These four elements are connected to each other, and the relations between them symbolize the notion that a change in one will affect the others (Leavitt, 1965). Thus, each relationship is meaningful to assess when examining a designated system, as the proper functioning of a measure in one element might rely on a prerequisite in another.

A designated system in the context of this study is defined as any system in blue cyberspace that a defensive actor is tasked with defending, whose attributes will affect the effectiveness of that defense while taking into account both the technical subsystem consisting of cyberspace terrain and tasks, as well as the social subsystem consisting of the associated structure and people. It is important to differentiate between this definition, whose purpose is to describe a system that is to be evaluated for defensibility, and a pure DCO definition, whose purpose is to describe a system that is to be defended from an operational standpoint. An analysis of defensibility needs to include the socio-technical perspective, although these factors are operationally out of scope for a defensive cyber operation.

F. FRAMEWORK OF DEFENSIBILITY

This section is divided into four parts. Initially, dictionary definitions of defensibility are examined to establish foundational definitions. Second, the use of

defensibility in research is examined and mapped to the dictionary definitions. Third, a review of the use of defensibility in discourse concerning cybersecurity and cyber defense examines how decision makers express themselves about defensibility and how their requirements for it can be understood. Finally, based on the use of defensibility in research and decision-maker requirements, a definition of defensibility for the defensive cyber operations context is synthesized using the constructs that have been defined up to this point.

In the *Oxford English Dictionary*, Oxford University Press defines *defensibility* and *defensible* as either the “ability to withstand or repel attack” (n.d.a, definition #1) and to be “able to provide a defence” (n.d.b, definition #1), or “the quality of being defensible in argument” (n.d.a, definition #2) and to be able to be “defended by argument” (n.d.b, definition #2). How can these two sets of definitions be applied to defensive operations? In the first set, it is not necessary for the object itself to provide defensive actions; it can also be a platform that enables or supports defensive actions performed by some defender. As such, the first set of definitions can be understood as the ability of some object to provide a platform for static or active defense measures. In the second definition, defensibility can be understood as the degree to which some action can be justified. This justification can be from one of several different perspectives, for example economy, legal, or moral considerations.

Seeing as there are two distinct meanings ascribed to defensibility, the following paragraphs examine how the term is used in discourse and research in a DCO context.

Cloud (2007) uses defensibility in three situations: when describing that a defensive doctrine framework can be used by tactical commanders to “improve the defensibility and survivability of their assigned portions of cyberspace” (p.72). When applying the concept of fortifications to cyberspace, he says that fortifications “are often used to bolster the defensibility of the existing terrain” (Cloud, 2007, p.18), adding that some examples of fortifications in cyberspace are “firewalls, proxy servers, web and spam filters, mail relays, antivirus/antimalware software, router Access Control Lists (ACLs), cryptography and encryption, user access controls (such as Username/Password authentication, Public Key Infrastructure (PKI), Certificates, access cards, group policies, and digital signatures)” (p.

18). Finally, Cloud (2007) asserts that a failure to reach unity of effort in cyber defense between and within services will result in exploitable areas that “will reduce the defensibility of friendly cyberspace” (p. 69). All of these uses are in line with the first definition, that of an object’s ability to provide a platform for defense measures. Cloud’s (2007) use of defensibility and fortifications has a clear focus on static defense measures.

As described in the literature review, defensibility is used and defined superficially in three separate studies published by the MITRE Corporation (Bodeau & Graubart, 2013; Bodeau et al., 2013; Bodeau et al., 2018). Using definitions of defensibility such as “the ability to address ongoing adversary activities” (Bodeau & Graubart, 2013, p. iii), “causing cyber adversaries to move more slowly, spend more, and take more risks” (Bodeau et al. 2013, p. 1), is consistent with the first definition.

As described in the literature review, Ziring (2015) states that a defensible network “is designed and built to facilitate operations in its own defense” (p. 3), and includes measures to give defenders “accurate and timely knowledge of the operational context” (p. 3). This follows the first definition, as it is all about enabling defensive actions.

Fanelli (2016) also uses defensibility according to the first definition, but with an emphasis on static defense measures. He states:

Effective defense must build upon a strong foundation of static security measures and then extend to include active measures. The defender must attend to static defense techniques, such as secure software configuration and patching, authentication and access control, logging and audit, and secure backup. Although difficult and often unglamorous, the first task for the defender is to build systems, software, and networks to be as secure as possible. In other words, each information resource should have an inherently high and durable level of confidentiality, integrity, and availability. Efforts to ‘maneuver’ or to apply offensive methods for the defense, while appealing, should not get ahead of the fundamental task of optimizing the defensibility of the resources. Attempting to do so is like relying on the purchase of a faster fire engine to make up for neglecting the fundamentals of fire safety. (pp. 60–61)

In a study on how to apply the concept of key terrain in cyberspace, Pantin (2017) uses definitions from military doctrine that include defensibility as a factor. Specifically, it is included in the definitions of the *obstacles* and *cover and concealment* elements in the

OCOKA terrain analysis method, where analysis of these elements can help a commander discover *defensible terrain* (Pantin, 2017). His subsequent discussion of the nature of terrain in cyberspace shows that this definition is in line with the first meaning of defensibility.

In *Time Based Security*, Schwartau (1999) uses defensibility primarily as way to describe how cybersecurity measures could be motivated to decision makers from a cost-benefit perspective. He states that by using his proposed mathematical methodology, “the approach to adequate security is very straightforward, defensible, and measurable” (p. 79). This use of defensibility follows the second definition.

In his study, Medina (2016) also uses defensibility according to the second meaning, as the study examines how to make security policies withstand scrutiny based on best practice and legal standards.

As described in the literature review, Ross et al. (2016) use “defensible and survivable” (p. ii) systems as a desired end state, but they do not define defensibility. However, given that their publication describes perspectives and actions to develop such systems, we can examine its contents to glean a meaning. Ross et al. (2016) state that “the ultimate objective is to obtain trustworthy secure systems that are fully capable of supporting critical missions and business operations while protecting stakeholder assets, and to do so with a level of assurance that is consistent with the risk tolerance of those stakeholders” (p. viii). Following their reasoning, a system that is defensible and survivable embodies those values. With that assumption as a background, we can argue that Ross et al. (2016) use defensibility in a manner aligned with the second definition, as this would best capture the statement that a system should be protected with a level of assurance consistent with risk tolerance. In that interpretation, the defensibility is a matter of security measures being sufficiently aligned with the risk tolerance of stakeholders.

The definition and use of defensibility proposed by Bier and Gutfraind (2019), as described in the literature review, is in keeping with the second definition, as they state that defensibility is “the extent that a modest investment can significantly reduce the damage from an attack or disruption” (p. 626). They link their definition to cost-effectiveness and

cost-benefit calculations, and as such, it can be understood primarily as a tool for motivating efforts rather than enabling actions.

In one study on moving target defense using software-defined networking, Larkin et al. (2021) use defensibility in line with the second meaning, regarding arguments for and against traditional network topologies and the placement of certain network resources.

In a 2011 article, General Keith Alexander is quoted expressing that “the key to stopping any severe piece of malware may lie in the creation of a secure zone [. ...] Establishing this secure zone will entail creating an architecture that is ‘infinitely more defensible’ and limits adversaries’ ability to intrude” (Ackerman, 2011, p. 19). He is also quoted stating that “as communications flow by, you have to look at what are the problems that you see in those communications or in your environment—and is it defensible” (Ackerman, 2011, p. 19). Here, Gen. Alexander connects defensibility with limiting an adversary’s ability to attack a system and monitoring communications and the environment to proactively evaluate if there may be any issues that make it less defensible. This indicates that he is using defensibility as the ability of a system to be protected using active or static measures and also attributing to it the size of the area to be defended.

In 2012, Gen. Alexander, who at the time was the head of both the National Security Agency and the U.S. Cyber Command, told an audience at New York’s Fordham University that the DOD’s networks are “not defensible,” according to an article in *Wired* (Shachtman, 2012). The context in which the term was used refers to defenders being able to perform defensive actions. For example, about the number of networks to be defended, the general reportedly stated that there were “15,000 enclaves: you can’t see ‘em all. You cannot defend them all [. ...] You’ve got to have an infrastructure that is defensible” (Shachtman, 2012). This quote focused on the size of the portion of cyberspace that has to be protected, but the general also raised other concerns, such as visibility and jurisdiction: “what we tell them [Congress] technically is: in order to stop [an attack], you have to see it in real time, and you have to have those authorities” (Shachtman, 2012). In the *Wired* article, Gen. Alexander was also reported as arguing for consolidation of systems and moving towards cloud computing to increase defensibility (Shachtman, 2012). The main points about defensibility in this interview are that it is adversely affected by the size of the

attack surface and area which is to be defended, and it requires visibility and clearly defined authority. The use of defensibility by Gen. Alexander focuses on blue cyberspace as a whole rather than individual systems.

In 2014, Admiral Michael S. Rogers, then chief of U.S. Cyber Command, emphasized defensibility as one of several top priorities, with the comment that it would allow networks to operate under attack and reduce the impact of attacks, as recorded by Gorminsky (2014). As specific initiatives to accomplish this, Adm. Rogers proposed “reducing the number of networks, paying special attention to network [sic] with public interfaces and implementing common IT architecture” (Gorminsky, 2014). In the first part, Adm. Rogers links defensibility with factors related to resilience, and in the second, he relates defensibility to the size of the attack surface and area which is to be defended and degree of standardization.

In 2015, Major General Burke E. Wilson gave a statement on cyber operations before Congress, in which he said that migration of disparate systems into a single architecture had made the Air Force’s networks more defensible (Cyber Operations, 2015). In this context, he was, again, referring to a large portion of blue cyberspace rather than a single system and associated increased defensibility with a reduction of the attack surface, increasing standardization, and shrinking the terrain to be defended.

In the *Cyberspace Solarium Commission Final Report*, King and Gallagher (2020) use defensibility in one desired end state for their concept of *Layered Cyber Deterrence* without giving much context, other than that “critical elements of national power and infrastructure that are secure, resilient, and supported by a defensible digital ecosystem” (p. 30) are desired. The only clear meaning that can be extracted from this use is that it is in the same realm as security and resilience and should thus be interpreted as closer to the first definition—of enabling defensive actions, rather than the second one—to withstand scrutiny from a legal or financial perspective.

Based on the context in which decision makers and researchers have used defensibility, this study uses the first definition as a baseline, that defensibility is about the ability to function as a platform for defense measures. While several decision makers have

emphasized the size of the attack surface as important, this was mainly in the context of blue cyberspace rather than a designated system. As such it will not be included in the definition for this study, but it will be reflected in the operationalization.

Based on the findings just described, the proposed definition for defensibility in defensive cyber operations is the ability of a designated system to facilitate active defense measures performed by a defensive actor in the conduct of defensive cyber operations. This definition is compatible with the first definition from the *Oxford English Dictionary* (Oxford University Press, n.d.a), Bodeau and Graubart (2013), Bodeau et al. (2013), Ziring (2015), and Pantin (2017).

Figure 3 illustrates the relationships between the concepts defined in this chapter—namely, a defensive actor is tasked with conducting a defensive cyber operation in a designated system using active defense measures. The defensive actor has a certain capability to perform active defense measures and the designated system has a certain defensibility, or set of attributes that facilitate active defense measures. How the capability of the defensive actor and the defensibility of the designated system intersect will determine what active defense measures are operationally available and will lead to a potential operational effectiveness for the operation.

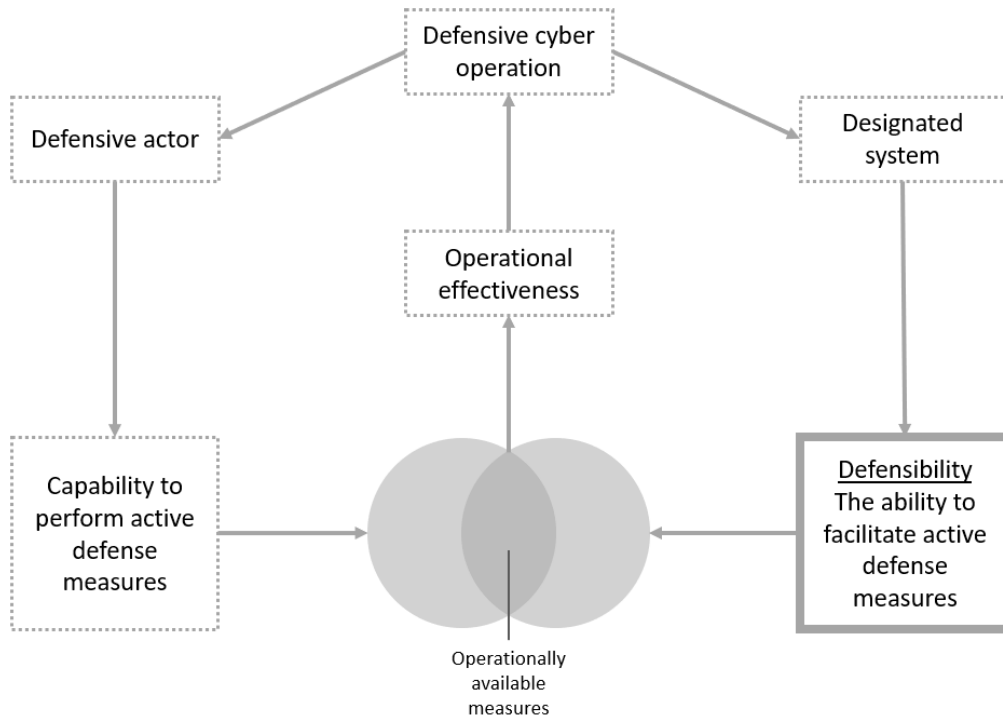


Figure 3. Defensibility framework

There are two types of positive impact that an attribute can have on the defensive actor's capability—allow and amplify. To allow a measure simply means that it is possible to perform it in the system. For example, the defender may be given hands-on access to endpoints, *allowing* for active gathering of data from one device at a time. To amplify a measure means that the system has attributes that result in that same measure having a greater effect. For example, each endpoint in the system may have a preinstalled agent with an array of specialized tools and the capability to perform active gathering in a distributed manner from a central point, greatly increasing the speed and ease with which the defensive actor can execute the measure.

While defensibility has a positive focus, its antithesis must also be considered when assessing a designated system. Thus, when looking for attributes that facilitate active defense measures, we must also highlight attributes that stop or constrain those same measures. At this point, it is necessary to acknowledge that this definition paints a complicated picture, as different defensive measures can have different allowing or amplifying attributes that might be conflicting. There could be situations in which some

attribute of a system allows or amplifies one measure while simultaneously stopping or constraining another.

Now that we have a framework of meaning that defines defensibility, it needs to be operationalized to enable its application in practice. This is done in the following chapter.

V. OPERATIONALIZING DEFENSIBILITY

This chapter builds on the definition of defensibility to establish the observable and measurable attributes of a system that constitute its defensibility. In the previous chapter, defensibility was defined as “the ability of a target system to facilitate active defense measures performed by a defensive actor in the conduct of defensive cyber operations.” To operationalize this definition, we need to answer three key questions:

- What fundamental active defense measures can be performed by a defensive actor when conducting defensive cyber operations in a target system?
- What attributes of a target system will affect those measures?
- How can these system attributes be observed and measured?

Each of these questions is addressed in a separate section, drawing upon doctrine, technical whitepapers, and research to formulate answers.

A. FUNDAMENTAL ACTIVE DEFENSE MEASURES

This section explores what fundamental measures a defensive actor can perform in a target system in the context of defensive cyber operations. In line with the constraints described in the *Limitations* section of Chapter I, this exploration does not go into technical detail and instead maintains a broader, capability-oriented perspective. The categories of active defense measures listed in Chapter IV, section C are used to frame these capabilities. The categories are *detection*, *analysis*, *mitigation*, *response*, *restoration*, and *command and control*.

Saydjari (2004) presents a model of cyber defense with six core elements: “sensors and exploitation; situation awareness; defensive mechanism; command and control; strategy and tactics; and science and engineering” (p. 54). His model does not separate the defender from the target system, but his model can still be analyzed in order to extrapolate defense measure capabilities. The first element, *sensors and exploitation*, is related to

visibility in the system, the ability to detect an attack and gather information about it (Saydjari, 2004). This corresponds to the ability to passively monitor the network and actively gather targeted information from devices, something present in both *detection* and *analysis*.

Situation awareness focuses on placing gathered information into a larger context to aid decision making (Saydjari, 2004). This corresponds to the ability to correlate data from different sources, again present in both *detection* and *analysis*.

Saydjari (2004) describes the *defensive mechanism* element as “technology to counter threats” (p. 54), corresponding to the ability to modify configurations on both network and end devices, alter files, and address system deficiencies. This capability is present in *mitigation*, *response*, and *restoration*.

Saydjari (2004) writes that *command and control* “is the process of making and executing decisions—orchestrating defensive systems, based on input from the situation awareness element” (p. 54), and that it includes both the ability to make decisions based on an understanding of available options and to communicate and execute those decisions throughout the system. These two abilities correspond to the *command and control* supporting function.

Saydjari (2015) defines *strategy and tactics* as “knowledge of what constitutes a good decision in terms of initial defensive policies and configurations as well as changes needed during operations because of attack situations” (p. 54). This element needs to be divided in two parts: (1) the knowledge of the defensive actor’s own capabilities and what constitutes best practice, or self-knowledge, and (2) the knowledge of how those capabilities and practices can and should be applied in the given context of the target system, or system knowledge. Both of these are necessary for decision making and are categorized under *command and control*.

Saydjari (2004) describes *science and engineering* as “the foundation yielding an understanding of design, composition, building, and maintenance of effective defense systems” (p. 54), which can be interpreted as the knowledge of how to make and operate

secure and defensible systems, which is not considered as a part of defensive cyber operations.

Ziring (2015) borrows three of Saydjari's (2004) elements that he argues are core to the future of cyber defense. They are *sensors and data collection*, *situational awareness*, and *defense mechanisms* (Ziring, 2015). For the first element, Ziring (2015) emphasizes not only data gathered from sensors inside the target system but also the correlation of this data with data from outside sources to create both a local and a global context. This corresponds to the ability to passively or actively gather information from the system and to correlate this information to facilitate *detection*. For *situational awareness*, he emphasizes *analysis* to produce "actionable information to support operational decisions" (p. 4). Ziring (2015) mentions system logs and sensors as types of internal sources that produce large amounts of data that needs to be filtered for analysis to be effective. Collecting data from these sources are measures in both *detection* and *analysis*. Concerning the last element—*defense mechanisms*—he states that it "includes specifically designed and deployed mechanisms for controlling the assets that comprise the network, as well as orchestration for applying multiple mechanisms in concert" (p. 4). Controlling assets can be done with the purpose to *mitigate*, *respond*, or *restore*, and orchestration is a supporting function under *command and control*. Ziring (2015) also emphasizes adaptability for defensive cyber operations and gives the example of utilizing software-defined networks "to adapt network topologies to enforce new policy, to douse undesirable dataflows, or even to randomly change networks to defeat attackers" (p. 4). This measure corresponds to *mitigate*, *respond*, and *restore*.

Fanelli (2016) lists three examples of active defense measures as "hunting on defended information resources for indicators of compromise, dynamically altering access controls in response to adversary activity, or deploying decoys to mislead and to redirect attackers" (p. 61). *Hunting* is an activity by which the defender performs targeted searches for signs that indicate an attack in a threat-specific manner, and it fits in the *detection* category. The data gathering can be done using either passive or active methods. *Altering access controls* is done to block access by an attacker, and it fits in the *response* category.

Deploying decoys can be done for different purposes and at different stages in an operation. Thus, it could correspond to *detection*, *analysis*, or *response*.

In *JP 3-12 Cyberspace Operations*, the Joint Chiefs of Staff (2018a) list five categories of defense measures, described as “actions to detect, characterize, counter, and mitigate threats [...], and to restore the system to a secure configuration” (p. II-6). They do not elaborate any further on what measures can be taken to facilitate *detection* or to *characterize a threat*, but both generally consist of gathering and correlating data in relation to a threat and performing *analysis*. The Joint Chiefs of Staff’s (2018a) concept of *counter* can be understood as synonymous with the *response* category of active defense measures and it, together with their *mitigate* and *restore* concepts, are all concerned with modifying different aspects of the system, albeit with different foci. *Mitigation* and *restoration* efforts can be assisted by a defensive actor, but the main responsibility lies with the organization that operates the system on a daily basis (Joint Chiefs of Staff, 2018a).

Cloud (2007) lists three core functions of defensive cyber operations: *posture*, *maneuver*, and *recover*. He writes that “the key principle behind posturing is anticipating cyber-attacks and then planning and implementing measures to ensure the survivability of friendly combat power” (p. 73), adding that the latter part includes “the employment of cover, concealment, dispersal, camouflage, hardening, redundancy, and deception” (p. 73). Although not much further detail is given in his study, *anticipating attacks* could be interpreted as *detection*, i.e., requiring the ability to gather data passively and/or actively from the target system. The latter part of *posturing* as described by Cloud (2007) is more related to cybersecurity and is not considered in this study. On *maneuver*, Cloud (2007) states that it “encompasses proactive and reactive actions taken in response to and during attacks” (p. 74), listing the tasks “attack, defend, relocate, augment, withdraw, delay” (p.75). These tasks can all be categorized into the *mitigate* and *respond* categories, requiring the ability to modify the system at different levels. The *recover* function is straightforward and “includes performing battle damage assessment (BDA), repairs, reconstitution, and emergency containment of extreme damage” (Cloud, 2007, p. 74). This definition includes elements of *mitigate* and *restore*.

In a 2017 paper titled *Next-Generation Defensive Cyber Operations (DCO) Platform*, Brown et al. describe a National Security Agency (NSA) cybersecurity platform for use in active defense measures. Such DCO platforms are used as the interface between the defensive actor and the designated system and serve as the base from which the defender operates. A DCO platform is owned and operated by the defender and is often deployed in the initial phases of a defensive operation. It enables the capabilities of the defender on their side of the demarcation point with the target system. Brown et al. (2017) list the following services of the DCO platform as critical:

Hardening – Implement best-practice guidance for network design and security to include secure configurations for endpoints to reduce a site’s attack surface;

Vulnerability Discovery – Identify weaknesses in the design and implementation of network defenses that can be exploited by an adversary;

Intrusion Detection – Identify activities within the network and on endpoints that are indicative of attempts to compromise or exploit the network;

Continuous Monitoring – Monitor both network traffic and endpoint activities continuously for deviations from a known normal state and behaviors;

Threat Intelligence – Identify and leverage various sources of cyber-threat intelligence that can drive both hunting operations and guide incident-response efforts;

Hunting – Conduct both persistent and on-demand searches for evidence of an adversary’s latest Tactics, Techniques, and Procedures (TTPs) to include new tradecraft;

Incident Response – Rapidly deploy cyber-investigative and cyber-forensic capabilities in response to a known bad activity or intrusion;

Countermeasures – Put into effect mitigation efforts that are the result of the knowledge and understanding of vulnerabilities and adversary TTPs that put a network at risk. (p. 45)

Hardening and *vulnerability discovery* are measures that are aimed at removing avenues through which threats can be realized and correspond to *mitigation*. *Intrusion detection*, *continuous monitoring*, and *hunting* correspond to *detection* using active and

passive methods. *Threat intelligence* is used to inform both *detection* and *analysis*. *Incident response* is a broad field that can cover activities in *analysis*, *mitigation*, *response*, and *restoration*. *Countermeasures* corresponds to the *mitigation* and *response* categories.

The design of the platform is centered on four core functions: *passive sensing*, *active sensing*, *analytic engine*, and *asset management* (Brown et al., 2017). *Passive* and *active sensing* are measures in both *detection* and *analysis*. The *analytic engine* is utilized to filter and correlate data to perform *analysis*. *Asset management* of the DCO platform is a part of *command and control*. Brown et al. (2017) state that the platform, once deployed at a designated system, can be operated either locally or remotely. The mode of operation is a factor in *command and control*.

The measures previously listed illustrate the breadth of activities that can be executed as active defense measures. They have been consolidated and generalized in Table 1. The complete mapping can be found in the appendix.

Table 1. Active defense measure capabilities.

Category	Capability
Detect	Passively gather data from established sensors inside the system
	Correlate data from different sources
	Actively gather data from the system by interacting directly with endpoints and network devices
Analyze	Passively gather data from established sensors inside the system
	Filter and correlate data from different sources
	Actively gather data from the system by interacting directly with endpoints and network devices
Mitigate	Modify aspects of the system
	Actively or passively gather data from the system
Respond	Modify aspects of the system
Restore	Modify aspects of the system
Command and Control	Make decisions
	Execute decisions
	Maintain internal knowledge

As is shown in Table 1, there are several capabilities that are used across different categories of active defense measures. For example, the *respond* and *restore* categories

contain measures that are different and have different goals, but all require the fundamental capability to modify different aspects of the system. Thus, the fundamental active defense measure capabilities are the following:

- Passively gather data from established sensors inside the system

This is accomplished using network sensors such as network traffic monitors; network intrusion detection/prevention systems; IP- or DNS blackholes; honeynets, honeypots, or honeytokens and their monitors; logs from endpoints and network devices (if the system allows them to be gathered passively); and alarms from host-based sensors such as host intrusion detection/prevention systems or other agents. Passive gathering is done by subscribing to data flows without interacting with the system. When done to facilitate detection, the purpose is to find indicators of compromise or anomalies that warrant deeper analysis. When done to facilitate analysis, the purpose is to gather additional information about a detected threat. When done to facilitate mitigation, the purpose is to investigate damages from cyber effects or discover avenues through which threats can be realized.

- Actively gather data from the system

This can be done from a network-centric or host-centric approach. A network-centric approach entails gathering information about the network by using active scanning methods, and the host-centric approach entails interacting directly with hosts to query them for information using different tools. When done to facilitate detection, the purpose is to find indicators of compromise or anomalies that warrant deeper analysis. When done to facilitate analysis, the purpose is to gather additional information about a detected threat. When done to facilitate mitigation, the purpose is to investigate damages from cyber effects or to discover avenues through which threats can be realized.

- Filter and correlate data

This capability uses automation to filter and correlate data from different sources both inside and outside the designated system to support decision making. Correlation is done to assist in detection by making it possible to detect chains of linked events rather

than only singular ones. When used to assist analysis, the filtering and correlation capability is used to single out and discover additional information about a detected threat.

- Modify aspects of the system

Modifying system hardware or software, configuration, or files on end devices or network devices is done to reach some cyber effect. In mitigation, the effect is focused on remediating the effect of attacks or removing avenues through which threats can be realized. In response, the effect is focused on countering an attacker's actions. In restoration, the effect is focused on restoring adequate operational capability to the designated system.

- Make decisions

The ability to make operational decisions requires information about the designated system's cyber terrain and any operational guidelines and restrictions.

- Execute decisions

The execution of decisions includes processes and infrastructure to communicate them and a delivery mechanism to execute them.

- Maintain internal knowledge

This is the ability to possess and leverage tacit and explicit knowledge of the defensive actor of their own capabilities, tools, techniques, and procedures. This capability is primarily a function of the defensive actor and not affected by the designated system and it is therefore not regarded in this study.

B. SYSTEM ATTRIBUTES

This section examines what attributes of a designated system might affect the capabilities necessary to perform fundamental active defense measures. The capabilities of interest are *passive gathering of data*, *active gathering of data*, *filtration and correlation of data*, *modifying aspects of the system*, *making decisions*, and *executing decisions*.

Attributes are considered from a socio-technical perspective using Leavitt's Diamond model (Bostrom & Heinen, 1977; Leavitt, 1965) as a framework to ensure a broad coverage. In doing this, attributes are mapped to either individual elements or connections between elements in the model to illustrate their domain.

The effect of the attributes on the capability of a defender is of interest, regardless of whether it is positive or negative; attributes that stop or degrade a capability are as important to regard as those that enable or amplify it.

1. Passive Gathering of Data

The two main categories of data gathered using this capability are network traffic and logs. As such, these are the areas where the attributes of interest are.

Regarding network traffic, attributes that affect visibility are key to the performance of passive gathering—the number and position of available capture points as well as the capacity of sensors and transparency of traffic at the capture points. Capacity of sensors relates to whether they capture samples of flows, full flows, truncated packet captures or full packet captures and how long they can store capture files before rolling over. Transparency is related to whether traffic content is encrypted at the capture point.

Logs need to be available, i.e., sent to a point where the defender can subscribe to them without interacting with the system to allow passive gathering. If this is not the case, they need to be collected using active gathering. Other attributes that affect passive gathering through logs and events are the type and placement of the sensors. Regular devices that are capable of generating logs should do so. These are devices that are a part of the operational side of the system, such as endpoints and network devices, including firewalls. Devices specifically used for cybersecurity or cyber defense should be positioned to ensure broad coverage and should be tuned to the system. There are several different types of these devices with different purposes, such as IP and DNS blackholes; honeynets, honeypots, honeytokens and their monitors; network intrusion detection/protection systems (NIDS/NIPS); and host intrusion detection/protection systems (HIDS/HIPS). Each of these offer different capabilities but can all be used to generate log flows for passive gathering. Beyond these attributes, there is also a need for a process through which the

defender can make or request configuration changes to network traffic sensors and log sources that generate data for passive gathering.

In the socio-technical model, attributes related to placement and capacity of sensors are primarily in the *technical* domain. Attributes regarding log availability is concerned with the *technical-task* domain, since they rely on technical solutions and the manner in which the organization of the designated system performs tasks related to logs. The process related attribute is in the *task-structure* domain, as it is concerned with both the authority to decide on changes and the actual task of making them.

2. Active Gathering of Data

To perform active gathering, the defender needs to have the appropriate accounts and associated permissions to allow access to the necessary data. Manual interaction with individual systems can be cumbersome and does not scale well in large systems. As such, the coverage and capability of agents on endpoints are two attributes that affect this capacity greatly. Agents offer an interface with which the defender can interact to execute tasks on devices and often contain the tools necessary to perform those tasks, as opposed to the bare-bones method of only having GUI or command-line access to the device and no availability of specialized tools. On the capacity of agents, attributes of importance are, for example, access method, centralized control, and the capabilities of its tools, including the ability to extract and analyze volatile memory, interact with and extract files, read logs, search for IOCs using structured methods such as YARA,² view and interact with processes, run scripts, and configure ad-hoc monitoring and alarms.

The network-centric approach entails sending traffic on the network of the system to gather data, using such methods as port scanning. To perform network-centric active gathering, the defender needs a sufficient number of vantage points to ensure coverage of all relevant segments of the network. The scope of any restrictions to scanning behavior imposed by components of the system is another factor that affects this capability. An

² As described by VirusTotal (n.d.), YARA is a tool that is used to create descriptions, or rules, that are used to identify and classify malware samples or other malicious behavior based on textual or binary patterns. YARA is an acronym for either *YARA: Another Recursive Acronym* or *Yet Another Ridiculous Acronym*.

example of this could be certain devices that are easily overloaded or malfunction when receiving malformed packets. Another area that could affect active gathering is the ability to directly access and interact with network-based sensors, such as the ones described under the section for *passive gathering*. This could allow for active gathering by posing ad-hoc queries and customizing responses using scripts.

The effectiveness of both approaches is affected by the method and capability of the defender's access to the system in the logical layer. The platform from which the defender operates can be offline or connected to the system via one or more links offering different vantage points.

These attributes are primarily in the *technical* domain of the socio-technical model, with scanning behavior restrictions in the *technology-task* domain, as it is concerned with both the technological conditions that are the basis of restrictions and the designated system organization, having performed a sufficient analysis of these conditions to be aware and create the restrictions.

3. Filtration and Correlation of Data

This study assumes that a DCO platform will be utilized to realize analytical tasks, as this is often the standard operating procedure for defensive actors. This means that the actual data correlation is performed on the defender's side of the demarcation and outside of the scope of the designated system. As such, the attributes that affect filtration and correlation of data are primarily concerned with the availability and quality of the data. Data availability is derived from how easy it is to transport and aggregate data from the generating device to a central point for processing. The availability may be different types of sources, such as logs from regular devices that are a part of the operational side of a system, and sensors that are deployed to fill roles in cybersecurity and cyber defense.

The quality of the data concerns its completeness, i.e., does it contain all the necessary data points, if it is enriched with metadata and necessary information to perform correlation—for example session tracking and NAT tracing, if it is normalized to a format that is machine-readable, and if it is necessary. For logs, adherence to an established log

policy solves many of these issues. Other important attributes for correlation are the different types of sensors and retention of historical data.

In the socio-technical model, the quality of the data is primarily in the *technical* domain, with data enrichment also including a *task* connection, as it requires a process to analyze, develop, and maintain necessary enrichments. Data retention is also in the *technical-task* domain, as it depends on technical conditions and the processes of the designated system. Data necessity and adherence to log policy is in the *task* domain, as it is related to the designated system having established processes. Data availability and coverage consist of attributes in the *technology* domain.

4. Modifying Aspects of the System

Modifying the system is a capability that can be done to serve several different purposes in measures that aim to *mitigate*, *respond*, or *restore*, but regardless of the purpose, the basic mechanics and requirements are the same.

The capability is affected by access to accounts and their permissions on necessary devices, the mode of access to different types of devices—remote access or local only, which in turn is partly determined by whether there are designated access points for a DCO platform. The capability is also affected by the presence, coverage, capability, and access method of agents on devices in the system. Agents that facilitate actions on devices in the system—running scripts, killing processes, quarantining files, changing network configuration, etc.—are of interest here. The capability is also affected by the nature of processes to alter network configurations and topology, isolate devices, and perform hardware changes.

In the socio-technical model, most of the attributes that affect this capability also affect active gathering and are described in that subsection. Attributes that relate to access modes are in the *technical* domain. Attributes concerning processes to alter the system are in the *structure-task* domain, as they are related to both the authority to decide on system changes and the process of implementing them.

5. Making Decisions

Attributes that affect the ability to make decisions are concerned with the availability and veracity of two categories of information: technical and operational.

Attributes in relation to technical information about the system are the availability, integrity, and accuracy of different types of documentation. Such documentation includes confirmation lists regarding allowed network flow, devices allowed in the system, users and permissions, and allowed binaries on different devices, and topology maps showing layer 2 of the OSI reference model (i.e., the *data link* layer) and layer 3, the *network layer*. In addition, descriptions of the external attack surface, including all ingress points to and egress points from the system, and use case descriptions are among the necessary information.

Detailed technical information about the system allows the defenders to discern abnormal behavior. Confirmation lists are lists of items that are known and confirmed good. The size of the attack surface was emphasized by decision makers when discussing defensibility, as seen in Chapter IV, section F, and this includes points of ingress to and egress from the system, and what hosts, protocols, and data are involved in exchanges through them. The accuracy of documentation concerns how well it is kept up-to-date and reflects actual conditions in the system.

The integrity of sensor data and log data are also attributes that factor into decision making, as is the availability and capability of a reference environment which can be used to run tests and confirm hypotheses without affecting the production environment.

Attributes of importance for operational information are the availability and comprehensiveness of:

- The designated system's own planning for DCO:
 - Defined mandates and authorities within the designated system
 - Defined responsibilities with regards to DCO
 - Rules of engagement for the defender

- Threat assessments, operational goals and prioritization of services
- Standing orders governing DCO
- Process for deconfliction of activities
- Documentation of all management activities in the system

An important set of attributes that provide an operational context is a DCO plan for the designated system, including rules of engagement and mandates, areas of responsibility for support activities, priorities for defensive actions, and a defined decision maker responsible for making final decisions on defensive actions that will affect the function of the system. An established process for deconfliction and consistent documentation of all management activities in the system are also of importance for decision making.

The technical information attributes are in the *technology-task* domain of the socio-technical model, with the documentation veracity in the *task* domain. Operational information attributes are divided primarily over the *structure* and *tasks* domains, with DCO planning, standing orders in the *structure* domain, documentation of management actions in the *tasks* domain, and defined responsibilities, prioritization, rules of engagement, and deconfliction in both. Defined mandates and authorities is in the *structure-people* domain.

6. Executing Decisions

To communicate and execute decisions, the defender needs to have technical means, formal authority, and practical support.

Attributes affecting technical means include the external access mode for the DCO platform, the number and placement of prepared connection points for the platform, permissions in the system, coverage of network capture points, vantage points for active gathering, and access to tools for modification of the system.

Attributes that affect formal authority are mandates to execute necessary measures and clearance for information stored in the system, as information gathering and analysis might expose defenders to any classified information in the system.

Practical support consists of attributes regarding deconfliction of activities, a dedicated point of contact, and operational information sharing with the designated system organization.

In the socio-technical model, technical means to execute decisions are all in the *technical* domain. Attributes related to formal authority are in the *structure* domain. Deconfliction and operational information sharing are both in the *structure-tasks* domain and the dedicated point of contact is in the *people-task* domain.

7. Summary

Table 2 displays all the defensibility attributes, which fundamental active defense measure capability they affect, and in what domain of the socio-technical model they can be found.

Table 2. Defensibility attributes.

Attribute	No.	Domain	Passive gathering	Active gathering	Filtration and correlation	Modifying aspects of the system	Making decisions	Executing decisions
Access; DCO platform access mode	1	Technology						X
Access; Endpoints	2	Technology				X		
Access; Network devices	3	Technology				X		
Access; Prepared connections for DCO platform	4	Technology		X		X		X
Accounts; Device coverage	5	Technology		X		X		
Accounts; permission levels	6	Technology		X		X		X
Agents; Access method	7	Technology		X		X		
Agents; Automation and centralization	8	Technology		X		X		
Agents; Capability	9	Technology		X		X		X

Attribute	No.	Domain	Passive gathering	Active gathering	Filtration and correlation	Modifying aspects of the system	Making decisions	Executing decisions
Agents; Coverage	10	Technology		X		X		X
Documentation; All management actions in the system are documented	11	Tasks					X	
Documentation; Clearly specified responsibilities	12	Structure, Tasks					X	
Documentation; Confirmation list integrity	13	Technology					X	
Documentation; Confirmation list: allowed binaries on different devices	14	Technology, Tasks					X	
Documentation; Confirmation list: devices that are allowed in the system	15	Technology, Tasks					X	
Documentation; Confirmation list: users and permissions	16	Technology, Tasks					X	
Documentation; Description of allowed network flows	17	Technology, Tasks					X	
Documentation; Description of attack surface – all ingress and egress points	18	Technology, Tasks					X	
Documentation; Layer 2 network map	19	Technology, Tasks					X	
Documentation; Layer 3 network map	20	Technology, Tasks					X	
Documentation; Veracity	21	Tasks					X	
Documentation; Reference environment capability	22	Technology, Tasks					X	
Documentation; Use case description of the system	23	Technology, Tasks					X	
Logs; Adherence to log policy	24	Tasks			X			
Logs; Completeness of data	25	Technology			X			

Attribute	No.	Domain	Passive gathering	Active gathering	Filtration and correlation	Modifying aspects of the system	Making decisions	Executing decisions
Logs; Coverage from regular devices	26	Technology, Tasks	X		X			
Logs; Coverage from special devices	27	Technology, Tasks	X		X			
Logs; Data enrichment	28	Technology, Tasks			X			
Logs; Data format normalized	29	Technology			X			
Logs; Data integrity	30	Technology, Tasks					X	
Logs; Data necessity is considered	31	Tasks			X			
Logs; Data retention	32	Technology, Tasks			X			
Logs; Ease of transport to collection point	33	Technology			X			
Orders; Assets and services are prioritized from an operational perspective	34	Structure, Tasks					X	
Orders; Authority to execute necessary measures	35	Structure						X
Orders; Clearance to information stored and transported in the system	36	Structure						X
Orders; Clearly defined mandates	37	Structure, People					X	
Orders; DCO planning	38	Structure					X	
Orders; Rules of Engagement	39	Structure, Tasks					X	
Orders; Scanning behavior restrictions	40	Technology, Tasks		X				
Orders; Standing orders	41	Structure					X	
Process; Configuration changes for devices that generate data	42	Tasks, Structure	X	X				

Attribute	No.	Domain	Passive gathering	Active gathering	Filtration and correlation	Modifying aspects of the system	Making decisions	Executing decisions
Process; Deconfliction of activities	43	Structure, Tasks					X	X
Process; Altering network topology	44	Structure, Tasks				X		
Process; Designated point of contact	45	People, Tasks						X
Process; Isolating devices	46	Structure, Tasks				X		
Process; Hardware changes	47	Structure, Tasks				X		
Process; Operational information sharing	48	Structure, Tasks						X
Sensors; Capacity of network capture sensors	49	Technology	X					
Sensors; Completeness of data	50	Technology			X			
Sensors; Coverage of network capture points	51	Technology	X		X			X
Sensors; Data enrichment	52	Technology, Tasks			X			
Sensors; Data format normalized	53	Technology			X			
Sensors; Data integrity	54	Technology, Tasks					X	
Sensors; Data necessity is considered	55	Tasks			X			
Sensors; Data retention	56	Technology, Tasks			X			
Sensors; DNS blackhole, capability	57	Technology	X					
Sensors; Ease of transport to collection point	58	Technology			X			
Sensors; HIDS/HIPS, coverage, capability	59	Technology	X					
Sensors; Honeynets, capability	60	Technology	X					

Attribute	No.	Domain	Passive gathering	Active gathering	Filtration and correlation	Modifying aspects of the system	Making decisions	Executing decisions
Sensors; Honeyd, capability	61	Technology	X					
Sensors; Honeytokens and monitors, capability	62	Technology	X					
Sensors; IP blackhole, capability	63	Technology	X					
Sensors; Network vantage points for active gathering	64	Technology		X				X
Sensors; NIDS/NIPS, coverage, capability	65	Technology	X					
Sensors; Transparency of network traffic at capture points	66	Technology, Tasks	X		X			

In the next section, these attributes are examined for potential measurements to finalize the model.

C. MEASURING DEFENSIBILITY

This section defines a measurement, its method of determination, and range of answers for each attribute in the model. The method of determination illustrates whether it is a measure that can be observed quantitatively or if it needs to be assessed qualitatively. The measurements are presented in Table 3, together with their scale, expressed in the *NOIR* scale—*nominal*, *ordinal*, *interval*, or *ratio*.

During the application of this model, the measurements in Table 3 are observed or assessed and given a score in the scale described. The measurement can then be correlated to an attribute in Table 2 by use of the *No.* column, which links measurements to attributes. Based on the information in Table 2, the user can then determine what fundamental capability will be affected and what domain of the designated system contains the attribute.

For example, if an operator was tasked with examining the conditions for executing active defense measures that used *active gathering*, the operator would examine Table 2 and see attributes 4–10, 40, 42, and 64 are of interest and then observe or assess the corresponding measurements.

Table 3. Defensibility measurements.

No.	Measurement	Method	Answers	Scale
1	What is the external access mode of the DCO platform?	Observe	Remote or local	N
2	What is the access mode to endpoints in the system?	Observe	(1) Remote, (2) partly remote, or (3) local	O
3	What is the access mode to network devices in the system?	Observe	(1) Remote, (2) partly remote, or (3) local	O
4	Are there prepared access points for a DCO platform?	Observe	(1) No, (2) Yes, single, or (3) Yes, multiple	O
5	What is the ratio of devices for which there are accounts?	Observe	Percentage	R
6	What permission levels do available accounts have?	Observe	(1) User, (2) User with partial administrative rights, or (3) Administrative rights	O
7	What is the access method to agents in the system?	Observe	Remote or local	N
8	What is the level of automation and centralization associated with agents in the system?	Assess	(1) None, (2) some automation or centralization, (3) partial automation and centralization, or (4) complete automation and centralization	O
9	What capabilities do agents in the system have?	Assess	(1) None, (2) basic, covers a few needed capabilities (3) extensive, covers many needed capabilities or (4) comprehensive, covers all needed capabilities	O
10	What is the ratio of endpoints that contain agents?	Observe	Percentage	R
11	To what degree and detail are management actions documented?	Assess	(1) None, (2) some actions are documented in low detail, (3) acceptable, most actions are covered in sufficient detail, or (4) complete, all	O

No.	Measurement	Method	Answers	Scale
			relevant actions are covered in full detail	
12	To what degree are responsibilities specified and documented?	Assess	(1) None, (2) some, not all responsibilities are specified, many undocumented, (3) acceptable, most responsibilities are specified and documented or (4) complete, all necessary responsibilities are clearly specified and documented	O
13	Can the integrity of confirmation lists be guaranteed?	Observe	Yes or no	N
14	Are there lists of allowed binaries for each type of device?	Observe	(1) No, (2) yes, some, or (3) yes, all	O
15	Are there lists of which devices are allowed in the system?	Observe	Yes or no	N
16	Are there lists of what users are allowed in the system and what permission they should have?	Observe	Yes or no	N
17	Is there a description of all allowed network flows in the system?	Observe	(1) No, (2) yes, partial, or (3) yes, complete	O
18	Is there a description of the system's attack surface showing a specification of all ingress and egress points?	Observe	(1) No, (2) yes, partial, or (3) yes, complete	O
19	Is there a comprehensive network map of layer 2?	Observe	(1) No, (2) yes, partial, or (3) yes, complete	O
20	Is there a comprehensive network map of layer 3?	Observe	(1) No, (2) yes, partial, or (3) yes, complete	O
21	Is the documentation current or are there deviations from the actual state of the system?	Assess	(1) No, there are large deviations; (2) no, and no deviations can be observed; (3) yes, and no deviations can be observed, or (4) yes, confirmed that there are no deviations	O
22	Is there a reference environment available for testing?	Observe	(1) No, (2) yes, with partial usability, or (3), yes, with complete usability	O

No.	Measurement	Method	Answers	Scale
23	Are there use case descriptions of the system	Observe	(1) None, (2) some, (3) acceptable, or (4) complete	O
24	Does the system adhere to an established log policy?	Observe	(1) No, (2) yes, partial, or (3) yes, complete	O
25	Do generated logs cover all necessary data to perform the mission?	Observe	(1) No, (2) yes, partial, or (3) yes, complete	O
26	From what ratio of regular devices are logs being gathered?	Observe	Percentage	R
27	From what ratio of special devices are logs being gathered?	Observe	Percentage	R
28	To what degree are logs enriched with metadata to aid correlation?	Assess	(1) To no degree, (2) to a small degree, or (3) to a large degree	O
29	Are logs normalized to a common format to facilitate automated processing?	Observe	(1) No, (2) yes, partial, or (3) yes, complete	O
30	To what degree can the integrity of log data be guaranteed?	Assess	(1) To no degree, (2) to a small degree, or (3) to a large degree	O
31	To what degree are gathered events motivated by need?	Assess	(1) To no degree, (2) to a small degree, or (3) to a large degree	O
32	Is log data retained for a long enough time to facilitate analysis after-the-fact?	Assess	(1) To no degree, (2) to a small degree, or (3) to a large degree	O
33	To what degree are logs easily transported to a central collection point?	Assess	(1) To no degree, (2) to a small degree, or (3) to a large degree	O
34	To what degree are system assets and services prioritized from an operational perspective?	Assess	(1) To no degree, (2) to a small degree, or (3) to a large degree	O
35	Do the defender have sufficient authority to execute necessary defense measures?	Observe	Yes or no	N
36	Does the defender have clearance to the information stored and transported in the system?	Observe	Yes or no	N

No.	Measurement	Method	Answers	Scale
37	To what degree are mandates clearly defined for decision makers in the designated system?	Assess	(1) To no degree, (2) to a small degree, or (3) to a large degree	O
38	How comprehensive is the DCO planning of the designated system?	Assess	(1) Not at all, (2) basic, (3) extensive, or (4) comprehensive	O
39	Are there clearly defined rules of engagement for operations in the system?	Assess	(1) No, (2) yes, partial, or (3) yes, complete	O
40	Are there restrictions on scanning behavior in the system?	Observe	(1) Unknown, (2) yes, substantial, (3) yes, minor, or (4) no	O
41	Are there standing orders specifically for the system that contain operational guidelines	Observe	(1) No, (2) yes, partial, or (3) yes, complete	O
42	Is there a functioning process for making configuration changes to devices that generate data?	Assess	(1) No, not possible, (2) no, ad-hoc, (3) yes, cumbersome, or (4) yes, effective	O
43	Is there a process for deconflicting activities in the system?	Assess	(1) No, not possible, (2) no, ad-hoc, (3) yes, cumbersome, or (4) yes, effective	O
44	Is there a functioning process for making network changes and altering network topology?	Assess	(1) No, not possible, (2) no, ad-hoc, (3) yes, cumbersome, or (4) yes, effective	O
45	Is there a designated point of contact for DCO?	Observe	(1) No, (2) yes, without mandates, or (3) yes, with mandates	O
46	Is there a functioning process for isolating devices?	Assess	(1) No, not possible, (2) no, ad-hoc, (3) yes, cumbersome, or (4) yes, effective	O
47	Is there a functioning process for making hardware changes?	Assess	(1) No, not possible, (2) no, ad-hoc, (3) yes, cumbersome, or (4) yes, effective	O
48	Is there a process for operational information sharing?	Assess	(1) No, not possible, (2) no, ad-hoc, (3) yes, cumbersome, or (4) yes, effective	O
49	What level of capacity do network capture sensors have?	Observe	(1) subset of network flows only, (2) complete network flow, (3) partial packet capture, or (4) full packet capture	O

No.	Measurement	Method	Answers	Scale
50	How complete is the data capture by other sensors?	Observe	(1) low, (2) medium, or (3) high	O
51	How comprehensive is the coverage of network sensors, from a vantage point perspective?	Observe	Percentage of possible network flows that are visible	R
52	To what degree is data gathered from sensors enriched to facilitate correlation?	Assess	(1) To no degree, (2) to a small degree, or (3) to a large degree	O
53	To what degree is data gathered from sensors normalized to facilitate processing?	Assess	(1) To no degree, (2) to a small degree, or (3) to a large degree	O
54	To what degree can the integrity of sensor data be guaranteed?	Assess	(1) To no degree, (2) to a small degree, or (3) to a large degree	O
55	To what degree is data gathered by sensors motivated by need?	Assess	(1) To no degree, (2) to a small degree, or (3) to a large degree	O
56	Is log data retained for a long enough time to facilitate analysis after-the-fact?	Assess	(1) Not at all, (2) for a short time, not long enough, or (3) yes, long enough	O
57	What is the capability of any DNS blackhole in the system?	Assess	(1) none present, (2) present, low capability, or (3) present, high capability	O
58	To what degree is sensor data easily transported to a central collection point?	Assess	(1) To no degree, (2) to a small degree, or (3) to a large degree	O
59	What is the coverage and capability of any HIDS/HIPS system?	Assess	(1) None present, (2) low coverage/effectiveness, (3) partial coverage/effectiveness, or (4) high coverage/effectiveness	O
60	What is the capability of any honeynets in the system?	Assess	(1) none present, (2) present, low capability, or (3) present, high capability	O
61	What is the capability of any honeypots in the system?	Assess	(1) none present, (2) present, low capability, or (3) present, high capability	O
62	What is the capability of any honeytokens in the system?	Assess	(1) none present, (2) present, low capability, or (3) present, high capability	O
63	What is the capability of any IP blackhole in the system?	Assess	(1) none present, (2) present, low capability, or (3) present, high capability	O

No.	Measurement	Method	Answers	Scale
64	Are there enough vantage points for active gathering to collect necessary data?	Assess	(1) No, none, (2) no, not enough coverage, (3) yes, partially, or (4) yes, full coverage	O
65	What is the coverage and capability of any NIDS/NIPS system?	Assess	(1) None present, (2) low coverage/effectiveness, (3) partial coverage/effectiveness, or (4) high coverage/effectiveness	O
66	Is network traffic encrypted as it passes network capture points?	Observe	(1)Yes, (2) yes, partially, or (3) no	O

Using these measurements, a defender would be able to observe and assess attributes of a designated system and draw conclusions on its defensibility. For internal consumption, in order to inform operational decision making in defensive cyber operations, this granularity might be warranted. However, when communicating results to decision makers and system stakeholders, scores could be combined to highlight areas of importance. This could be from a functional perspective, illustrating defensive capabilities that are of interest, or from a socio-technical systems perspective, using the domains of attributes to find systematic issues.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS AND FURTHER RESEARCH

A. CONCLUSIONS

The research questions that this study set out to answer were (1) how can cyber defensibility be defined in a Defensive Cyber Operations context, and (2) what critical factors and related variables within an analytical framework constitute defensibility for a system in a Defensive Cyber Operations context?

This study uses the constructs *defensive cyber operations*, *active defense measures*, *defensive actor*, and *designated system* to establish a framework of meaning. Based on this framework and the uses of defensibility in other research and in discourse about cybersecurity and cyber defense, this study proposed defining defensibility as *the ability of a designated system to facilitate active defense measures performed by a defensive actor in the conduct of defensive cyber operations*.

To identify critical factors and related variables, this study has proposed a set of seven fundamental active defense measure capabilities that a defensive actor needs to possess to conduct defensive cyber operations: *passive gathering of data*, *active gathering of data*, *filtration and correlation of data*, *modifying aspects of a system*, *making decisions*, *executing decisions*, and *internal knowledge*. These are the active defense measures that a system's defensibility affects. This study then extrapolated a set of 66 attributes of a system that affect these capabilities; i.e., attributes that constitute a system's defensibility. Finally, it proposes a set of measurements for these attributes, allowing defensibility to be measured and analyzed.

B. DISCUSSION

As identified in the literature review, there is a gap in the body of knowledge related to the intersection of the conduct of defensive cyber operations and the attributes of a designated system, i.e., the interaction between fundamental active defense measure capabilities and system attributes. In light of this gap, the analysis in Chapter V, section B, *System Attributes*, is made based on my prior experiences and extensive discussion with colleagues. Similarly, in section C, *Measuring Defensibility*, of the same chapter where the

literature review indicated that metrics developed to assess aspects of systems that touch defensibility are often developed from an internal perspective rather than from the perspective of an external defensive actor. The proposed metrics are therefore also a result of my own experience in the field and on independent analysis; they represent a first step on which expand, detail, and build a more robust model. The next step is to test these attributes and examine to what extent they affect the conduct of defensive cyber operations. Furthermore, both the measurements and the attributes identified can be expanded, given more detail, and weighed to gain more precision and accuracy in the model. The model also lacks a defined method to combine the results from the measurements to facilitate communication with decision makers and system stakeholders, but this is something that could be done from several perspectives, adding versatility to the model.

This study takes the perspective of a defender who is external to the organization that owns, operates, and uses the system, which also means that the defender is not an established stakeholder when prioritizing system changes. Many of the proposed attributes represent, similarly to cybersecurity measures, tradeoffs among defensibility, useability, and cost, meaning that defensibility might not be a priority unless ordained so by decision makers.

C. RECOMMENDATIONS FOR FURTHER RESEARCH

To continue the work of this study, I propose that defensibility should be further operationalized and that experiments with measuring defensibility in quantitative studies should be performed. One such study could use simulations to test the relationships between attributes and defensive action effectiveness and apply the results to improve the precision of the model. This would be a first step toward automated system evaluation that can provide recommendations for improving defensibility and proposing the most effective defensive actions in a given situation.

Another interesting area of future research is examining the relationship between system defensibility and defender capabilities. This would create a combined measurement of system defense status that reflects both what actions defenders are capable of performing and to what degree, as well as how those actions will be affected by the attributes of the

designated system. This measurement could then be used by decision makers to prioritize efforts to reinforce the defensive posture at a larger scale by focusing efforts either on the systems that are to be defended or on the actors performing the defense.

Finally, a future experiment could develop and test a measure of effectiveness for defensive cyber operations in general and for individual active defense measures, which could then be used to examine the correlation between changes in effectiveness and variations in the attributes of defensibility of the designated system to establish causal models and aid in analysis.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX. MAPPING FROM MEASURE TO CAPABILITY

Table 4 shows each measure described in Chapter V, section A, *Fundamental Active Defense Measures*, and how they can be combined into broader fundamental capabilities.

Table 4. Measure to capability.

Category	Measure	Source	Capability	Description
Detect	Actions to detect threats	Joint Chiefs of Staff (2018a)	Passively gather data from established sensors inside the system	This can be done using network sensors such as network traffic monitors; network intrusion detection/prevention systems; IP or DNS blackholes; honeynets, honeypots, or honeytokens and their monitors. Logs from endpoints and network devices (if the system allows them to be gathered passively). Alarms from host-based sensors such as host intrusion detection/prevention systems or other agents. When done to facilitate detection, the purpose is to find indicators of compromise or anomalies that warrant deeper analysis.
	Anticipate attacks	Cloud (2007)		
	Continuous monitoring	Brown et al. (2017)		
	Deploy decoys	Fanelli (2016)		
	Hunting	Brown et al. (2017)		
	Hunting for indicators of compromise	Fanelli (2016)		
	Intrusion detection	Brown et al. (2017)		
	Passive gathering	Saydjari (2004)		
	Passive sensing	Brown et al. (2017)		
	Utilize sensors inside the system	Ziring (2015)		
	Correlate data	Saydjari (2004)	Correlate data from different sources	Using automation, this process correlates data from different sources, both inside and outside the
	Correlate data	Ziring (2015)		

Category	Measure	Source	Capability	Description
	Threat intelligence	Brown et al. (2017)	Actively gather data from the system by interacting directly with endpoints and network devices	designated system to support decision making. Correlation is done to assist in detection by making it possible to detect chains of linked events rather than only singular ones.
	Actions to detect threats	Joint Chiefs of Staff (2018a)		This can be done from a network-centric or host-centric approach. Network-centric entails gathering information about the network by using active scanning methods, and host-centric entails interacting directly with hosts to query them for information. When done to facilitate detection, the purpose is to find indicators of compromise or anomalies that warrant deeper analysis.
	Active gathering	Saydjari (2004)		
	Active sensing	Brown et al. (2017)		
	Hunting	Brown et al. (2017)		
	Hunting for indicators of compromise	Fanelli (2016)		
Analyze	Deploy decoys	Fanelli (2016)	Passively gather data from established sensors inside the system	This can be done using network sensors such as network traffic monitors; network intrusion detection/prevention systems; IP or DNS blackholes; honeynets, honeypots, or honeytokens and their monitors. Logs from endpoints and network devices (if the system allows them to be gathered passively). Alarms from host-based
	Gather data from sensors	Ziring (2015)		
	Gather data from system logs	Ziring (2015)		
	Incident response	Brown et al. (2017)		
	Passive gathering	Saydjari (2004)		

Category	Measure	Source	Capability	Description
	Passive sensing	Brown et al. (2017)	Filter and correlate data from different sources	sensors such as host intrusion detection/ prevention systems or other agents. When done to facilitate analysis, the purpose is to gather additional information about a detected threat.
	Analytic engine - filter and correlate	Brown et al. (2017)		Using automation, this process filters and correlates data from different sources, both inside and outside the designated system to support decision making. When used to assist analysis, filtering and correlation is used to single out and discover additional information about a detected threat.
	Analyze data to produce actionable information	Ziring (2015)		
	Characterize threats	Joint Chiefs of Staff (2018a)		
	Correlate data	Saydjari (2004)		
	Filter data	Ziring (2015)		
	Incident response	Brown et al. (2017)		
	Threat intelligence	Brown et al. (2017)		
	Active gathering	Saydjari (2004)	Actively gather data from the system by interacting directly with endpoints and network devices	This can be done from a network-centric or host-centric approach. Network-centric entails gathering information about the network by using active scanning methods, and host-centric entails interacting directly with hosts to query them for information. When done to facilitate analysis, the purpose is to gather additional information about a detected threat.
	Active sensing	Brown et al. (2017)		
	Gather data from sensors	Ziring (2015)		
	Gather data from system logs	Ziring (2015)		
	Incident response	Brown et al. (2017)		

Category	Measure	Source	Capability	Description
Mitigate	Attack, defend, relocate, augment, withdraw, delay	Cloud (2007)	Modify aspects of the system	Modifying system hardware or software, configuration, or files on end devices or network devices to reach some cyber effect. In mitigation, the effect is focused on remediating the effect of attacks or removing avenues through which threats can be realized.
	Control assets	Ziring (2015)		
	Countermeasures	Brown et al. (2017)		
	Emergency containment of extreme damage	Cloud (2007)		
	Hardening	Brown et al. (2017)		
	Incident response	Brown et al. (2017)		
	Mitigate threats	Joint Chiefs of Staff (2018a)		
	Modify configuration of end devices	Saydjari (2004)		
	Modify configuration of network devices	Saydjari (2004)		
	Modify files	Saydjari (2004)		
	Modify system hardware	Saydjari (2004)		
	Modify system software	Saydjari (2004)		
	Battle damage assessment (BDA)	Cloud (2007)	Actively or passively gather data from the system	Gathering data from the system to facilitate mitigation by investigating damages from cyber effects or discovering avenues through which threats can be realized.
	Vulnerability discovery	Brown et al. (2017)		
Respond	Altering access controls	Fanelli (2016)	Modify aspects of the system	Modifying system hardware or software,

Category	Measure	Source	Capability	Description
	Attack, defend, relocate, augment, withdraw, delay	Cloud (2007)		configuration, or files on end devices or network devices to reach some cyber effect. In response, the effect is focused on countering an attacker's actions.
	Control assets	Ziring (2015)		
	Counter threats	Joint Chiefs of Staff (2018a)		
	Countermeasures	Brown et al. (2017)		
	Deploy decoys	Fanelli (2016)		
	Incident response	Brown et al. (2017)		
	Modify configuration of end devices	Saydjari (2004)		
	Modify configuration of network devices	Saydjari (2004)		
	Modify files	Saydjari (2004)		
	Modify system hardware	Saydjari (2004)		
	Modify system software	Saydjari (2004)		
Restore	Control assets	Ziring (2015)	Modify aspects of the system	Modifying system hardware or software, configuration, or files on end devices or network devices to reach some cyber effect. In mitigation, the effect is focused on restore adequate operational capability to the designated system.
	Incident response	Brown et al. (2017)		
	Modify configuration of end devices	Saydjari (2004)		
	Modify configuration of network devices	Saydjari (2004)		
	Modify files	Saydjari (2004)		

Category	Measure	Source	Capability	Description
	Modify system hardware	Saydjari (2004)		
	Modify system software	Saydjari (2004)		
	Reconstitution	Cloud (2007)		
	Repairs	Cloud (2007)		
	Restore to secure configuration	Joint Chiefs of Staff (2018a)		
Command and control	Make decisions	Saydjari (2004)	Make decisions	Making decisions is the ability to make operational decision, which requires information about the designated system's cyber terrain and any operational guidelines and restrictions.
	System knowledge	Saydjari (2004)		
	Communicate and execute decisions	Saydjari (2004)	Execute decisions	Executing decisions is the execution of decisions, which includes processes and infrastructure to communicate them and a delivery mechanism to execute them.
	Local or remote deployment of DCO platform	Brown et al. (2017)		
	Orchestrate measures	Ziring (2015)		
	Asset management	Brown et al. (2017)	Maintain internal knowledge	Having the ability to possess and leverage the tacit and explicit knowledge of the defensive actor about their own capabilities, tools, techniques, and procedures.
	Self-knowledge	Saydjari (2004)		

LIST OF REFERENCES

- Ackerman, R. K. (2011). Cyber command confronts evolving environment. *Signal*, 65(6), 18–21.
- Ackerman, R. K. (2019). Army defensive cyber operations maintain balancing act. *Signal*, 73(12), 17–19.
- Antonucci, D. (Ed.). (2017). *The cyber risk handbook: Creating and measuring effective cybersecurity capabilities*. John Wiley and Sons, Inc.
- Applegate, S. D., Carpenter, C. L., & West, D. C. (2017) Searching for digital hilltops: A doctrinal approach to identifying key terrain in cyberspace. *Joint Force Quarterly*, 1st quarter 2017(84), 18–23. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-84/jfq-84_18-23_Applegate-Carpenter-West.pdf
- Aziz, B., Malik, A., & Jung, J. (2017). Check your blind spot: A new cyber-security metric for measuring incident response readiness. In J. Großmann, M. Felderer, & F. Seehausen (Eds.), *Risk assessment and risk-driven quality assurance* (pp. 19–33). Springer. https://doi.org/10.1007/978-3-319-57858-3_3
- Bernier, M., Leblanc, S., & Morton, B. (2012). *Metrics framework of cyber operations on command and control*. Reading: Academic Conferences International Limited. <http://libproxy.nps.edu/login?url=https://www-proquest-com.libproxy.nps.edu/conference-papers-proceedings/metrics-framework-cyber-operations-on-command/docview/1035293477/se-2?accountid=12702>
- Bier, A. B. (2014). *A cognitive and economic decision theory for examining cyber defense strategies* (SAND2014-0442). Sandia National Laboratories. <https://doi.org/10.2172/1147206>
- Bier, V., & Gutfraind, A. (2019). Risk analysis beyond vulnerability and resilience: characterizing the defensibility of critical systems. *European Journal of Operational Research*, 276(2), 626–636. <https://doi.org/10.1016/j.ejor.2019.01.011>
- Bodeau, D., & Graubart, R. (2013). *Characterizing effects on the cyber adversary: a vocabulary for analysis and assessment* (MTR130432). The MITRE Corporation. <https://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf>

- Bodeau, D., Graubart, R., & Heinbockel, W. (2013). *Mapping the cyber terrain: Enabling cyber defensibility claims and hypothesis to be stated and evaluated with greater rigor and utility* (MTR130433). The MITRE Corporation. <http://www.mitre.org/sites/default/files/publications/mapping-cyber-terrain-13-4175.pdf>
- Bodeau, D. J., Graubart, R. D., McQuaid, R. M., & Woodill, J. (2018). *Cyber resiliency metrics, measures, of effectiveness, and scoring: enabling systems engineers and program managers to select the most useful assessment methods* (MTR180314). The MITRE Corporation. <https://apps.dtic.mil/sti/pdfs/AD1108019.pdf>
- Bostrom, R. P. & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective; Part 1: The causes. *MIS Quarterly*, 1(3), 17–32. <https://www.jstor.org/stable/248710>
- Brown, S., Carlin, S., & Torres-Negron, I. (2017). Next-generation defensive cyber operations (DCO) platform. *Journal of Information Warfare*, 16(2), 43–55.
- Cloud, D. W. (2007). *Integrated cyber defenses towards cyber defense doctrine* [Master's thesis, Naval Postgraduate School]. NPS Archive: Calhoun. <https://calhoun.nps.edu/handle/10945/3059>
- Cyber operations: Improving the military cybersecurity posture in an uncertain threat environment: Hearing before the Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services, 114th Cong. (2015). <https://www.govinfo.gov/content/pkg/CHRG-114hhrg94221/html/CHRG-114hhrg94221.htm>
- Denning, D. (1999). *Information warfare and security*. ACM Press.
- Denning, D. (2013). *Framework and principles for active cyber defense*. Naval Postgraduate School. <http://doi.org/10.1016/j.cose.2013.11.004>
- Department of the Army. (2019a). *Offense and defense* (ADP 3–90). https://irp.fas.org/doddir/army/adp3_90.pdf
- Department of the Army. (2019b). *Operations* (ADP 3–0). https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN18010-ADP_3-0-000-WEB-2.pdf
- Dewar, R. S. (2014). The “triptych of cyber security”: A classification of active cyber defence. *2014 6th International Conference on Cyber Conflict (CyCon 2014)*, 7–21. <https://doi.org/10.1109/CYCON.2014.6916392>
- Encyclopædia Britannica. (n.d.) *Defense definition and meaning*. The Britannica Dictionary. Retrieved February 24, 2022, from <https://www.britannica.com/dictionary/defense>

- Fanelli, R. (2016). Cyberspace offense and defense. *Journal of Information Warfare*, 15(2), 53–65. <https://www.jstor.org/stable/26487531>
- Fruhlinger, J. (2020, February 10). The CIA triad: Definition, components and examples. *CSO Online*. <https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html>
- Gorminsky, L. (2014, May 29) Defensible networks, C2 among CYBERCOM chief's plans to operationalize cyberwar. *Defense Daily*. <https://libproxy.nps.edu/login?url=https://www.proquest.com/trade-journals/defensible-networks-c2-among-cybercom-chiefs/docview/1700347629/se-2?accountid=12702>
- Hobbs, D. (2007). *Application of OCOKA to cyberterrain*. White Wolf Security. https://web.archive.org/web/20131022035519/http://www.whitewolfsecurity.com/pdf/Application_of_OCOKA_to_Cyberterrain.pdf
- Joint Chiefs of Staff. (2017). *Doctrine for the Armed Forces of the United States* (JP 1). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf?ver=2019-02-11-174350-967
- Joint Chiefs of Staff. (2018a). *Cyberspace operations* (JP 3-12). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf
- Joint Chiefs of Staff. (2018b). *Joint operations* (JP 3-0). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf
- Kallberg, J. (2017). Traditional military thinking in cyberspace: The need for adaptation. In D. Van Puyvelde & A. F. Brantly (Eds.), *U.S. National Cybersecurity* (1st ed., vol. 1, pp. 81–90). Routledge.
- King, A. & Gallagher, M. (March 2020). *Cyberspace solarium commission final report*. U.S. Cyberspace Solarium Commission. <https://www.solarium.gov/>
- Lachow, I. (2013). *Active cyber defense: A framework for policymakers*. Center for a New American Security. <http://www.jstor.org/stable/resrep06088>
- Larkin, R., Jensen, S., Koranek, D., Mullins, B., & Reith, M. (2021). Towards dynamically shifting cyber terrain with software-defined networking and moving target defense. *International Conference on Cyber Warfare and Security*, 535–540. <https://doi.org/10.34190/IWS.21.056>
- Leavitt, H. J. (1965). Applied organizational change in industry: Structural, technological and humanistic approaches. In J. G. March (Ed.), *Handbook of organizations* (1st ed., pp. 1144–1170). Rand McNally.

- Llanso, T., McNeil, M. (2021). Towards an organizationally-relevant quantification of cyber resilience. *Proceedings of the 54th Hawaii International Conference on System Sciences*, 7065–7074. <http://hdl.handle.net/10125/71470>
- Medina, D. (2016). Defensible cybersecurity: tailoring an organization’s security posture to applicable legal standards. *The Computer & Internet Lawyer*, 33(11), 11–17.
- Morin, M. (2016). *Protecting networks via automated defense of cyber systems*. [Master’s thesis, Naval Postgraduate School]. NPS Archive: Calhoun. <http://hdl.handle.net/10945/50600>
- Oxford University Press. (n.d.a). Defensibility, n. In *Oxford English Dictionary*. Retrieved March 31, 2022, from <https://www-oed-com.libproxy.nps.edu/view/Entry/48803>
- Oxford University Press. (n.d.b). Defensible, adj. In *Oxford English Dictionary*. Retrieved March 31, 2022, from <https://www-oed-com.libproxy.nps.edu/view/Entry/48804>
- Pantin, N. P. (2017). *Key terrain: Application to the layers of cyberspace*. [Master’s thesis, Naval Postgraduate School]. NPS Archive: Calhoun. <http://hdl.handle.net/10945/53030>
- Raymond, D., Cross, T., Conti, G., Nowatkowski, M. (2014). Key terrain in cyberspace: Seeking the high ground. *2014 6th International Conference on Cyber Conflict (CyCon 2014)*, 287–300. <https://doi.org/10.1109/CYCON.2014.6916409>
- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (SP 800–207). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-207>
- Ross, R., McEvilly, M., & Carrier Oren, J. (2016). *Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems* (SP 800–207). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-160v1>
- Shachtman, N. (2012, January 12). Military networks ‘not defensible,’ says general who defends them. *Wired*. <https://www.wired.com/2012/01/nsa-cant-defend/>
- Saydjari, O. S. (2004). Cyber defense: Art to science. *Communications of the ACM*, 47(3), 52–57. <https://doi.org/10.1145/971617.971645>
- Snyder, D., Mayer, L. A., Weichenberg, G., Tarraf, D. C., Fox, B., Hura, M. ... Welburn, J. W. (2020). *Measuring cybersecurity and cyber resiliency*. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2703/RAND_RR2703.pdf

- Schwartau, W. (1999). *Time based security*. Interpact Press.
- Thomas, J. E., Eisenberg, D. A., Seager, T. P., & Fisher, E. (2019). A resilience engineering approach to integrating human and socio-technical system capacities and processes for national infrastructure resilience. *Journal of Homeland Security and Emergency Management*, 16(2), 1–17. <https://doi-org.libproxy.nps.edu/10.1515/jhsem-2017-0019>
- U.S. Cyber Command. (April 2018). *Achieve and maintain cyberspace superiority: Command vision for U.S. Cyber Command*. <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf>
- U.S. Strategic Command, U.S. Transportation Command, and U.S. Cyber Command, U.S. Senate Committee on Armed Services, 114th Cong. (2015) (testimony of Michael S. Rogers). https://www.armed-services.senate.gov/imo/media/doc/Rogers_03-19-15.pdf
- VirusTotal. (n.d). *YARA: The pattern matching Swiss knife for malware researchers*. VirusTotal. Retrieved May 17, 2022, from <https://virustotal.github.io/yara/>
- Von Clausewitz, C. (1918). *On war* (third imprint). E. P. Dutton and Co.
- Wagner, N., Şahin, C. Ş., Winterrose, M., Riordan, J., Hanson, D., Peña, J., & Streilein, W. W. (2017). Quantifying the mission impact of network-level cyber defensive mitigations. *Journal of Defense Modeling and Simulation*, 14(3), 201–216. <https://doi.org/10.1177/1548512916662924>
- Wang, L., Jajodia, S., & Singhal, A. (2017). *Network security metrics* (1st ed. Springer International Publishing. <https://doi.org/10.1007/978-3-319-66505-4>
- Ziring, N. (2015). The future of cyber operations and defense. *Journal of Information Warfare*, 14(2), 1–6.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California