



Calhoun: The NPS Institutional Archive
DSpace Repository

NPS Scholarship

Theses

2020-06

REDUCING INFORMATION OVERLOAD VIA AN ANALOG MODEL FOR CYBER RISK

Breuer, Pablo C.

Monterey, CA; Naval Postgraduate School

<https://hdl.handle.net/10945/65458>

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

Downloaded from NPS Archive: Calhoun



Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>



**NAVAL
POSTGRADUATE
SCHOOL**

MONTEREY, CALIFORNIA

DISSERTATION

**REDUCING INFORMATION OVERLOAD VIA AN
ANALOG MODEL FOR CYBER RISK**

by

Pablo C. Breuer

June 2020

Dissertation Supervisor:

Dan C. Boger

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 2020	3. REPORT TYPE AND DATES COVERED Dissertation	
4. TITLE AND SUBTITLE REDUCING INFORMATION OVERLOAD VIA AN ANALOG MODEL FOR CYBER RISK			5. FUNDING NUMBERS
6. AUTHOR(S) Pablo C. Breuer			
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) Cybersecurity relies on Security Operations Center (SOC) personnel to conduct data triage on large numbers of automated alerts to identify true threats to networks. To achieve this goal, SOC personnel must not only filter out false positives in data streams but also coalesce disparate pieces of data to generate information that yields a conclusion of an existing exception condition in the desired state of cybersecurity and requires action. Additionally, false negatives in data streams may later be identified when a compromise is discovered via human reporting or other means. Limitations of Turing machines used as automated sensors, ever-increasing network size and speed of transmission, limited numbers of qualified personnel, and the necessity to work in uncertainty all serve to exacerbate the continual condition of information overload for network defenders. This research will attempt to address information overload by reducing the information that is presented to personnel working in a SOC. The goal is to propose a new framework for determining cybersecurity risk as a time-dependent function, which will allow for reduced information overload and at least maintain equivalent cybersecurity posture. Our findings indicate that the quantity of information presented to cybersecurity personnel can be reduced, in some cases by more than half, while maintaining the cybersecurity posture required for the completion of mission-essential tasks.			
14. SUBJECT TERMS cyber, security, information, overload, CND, defense, cybersecurity, information overload			15. NUMBER OF PAGES 127
			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.

**REDUCING INFORMATION OVERLOAD VIA AN ANALOG MODEL
FOR CYBER RISK**

Pablo C. Breuer
Commander, United States Navy
BS, U.S. Naval Academy, 1998
MS, Computer Science, Naval Postgraduate School, 2008

Submitted in partial fulfillment of the
requirements for the degree of

DOCTOR OF PHILOSOPHY IN INFORMATION SCIENCES

from the

**NAVAL POSTGRADUATE SCHOOL
June 2020**

Approved by: Dan C. Boger
Department of
Information Sciences
Dissertation Supervisor

Alex Bordetsky
Department of
Information Sciences

Raymond R. Buettner
Department of
Information Sciences

George W. Dinolt
Department of
Computer Science

Douglas J. MacKinnon
Department of
Information Sciences

Dan C. Boger
Department of
Information Sciences
Dissertation Chair

Approved by: Thomas J. Housel
Chair, Department of Information Sciences

Orrin D. Moses
Vice Provost of Academic Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Cybersecurity relies on Security Operations Center (SOC) personnel to conduct data triage on large numbers of automated alerts to identify true threats to networks. To achieve this goal, SOC personnel must not only filter out false positives in data streams but also coalesce disparate pieces of data to generate information that yields a conclusion of an existing exception condition in the desired state of cybersecurity and requires action. Additionally, false negatives in data streams may later be identified when a compromise is discovered via human reporting or other means. Limitations of Turing machines used as automated sensors, ever-increasing network size and speed of transmission, limited numbers of qualified personnel, and the necessity to work in uncertainty all serve to exacerbate the continual condition of information overload for network defenders. This research will attempt to address information overload by reducing the information that is presented to personnel working in a SOC. The goal is to propose a new framework for determining cybersecurity risk as a time-dependent function, which will allow for reduced information overload and at least maintain equivalent cybersecurity posture. Our findings indicate that the quantity of information presented to cybersecurity personnel can be reduced, in some cases by more than half, while maintaining the cybersecurity posture required for the completion of mission-essential tasks.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	CURRENT CYBERSECURITY CHALLENGE.....	1
B.	HYPOTHESIS, RESEARCH QUESTION, AND POTENTIAL CONTRIBUTIONS.....	4
II.	COMPUTER SCIENCE AND CYBERSECURITY	7
A.	THE UNDECIDABLE NATURE OF SECURITY	7
B.	COMPUTER ARCHITECTURE CHALLENGES TO SECURITY	8
C.	TRADITIONAL AUTOMATION OF CYBERSECURITY	9
D.	ARTIFICIAL INTELLIGENCE IN CYBERSECURITY.....	10
III.	INFORMATION OVERLOAD.....	15
IV.	CYBERSECURITY FRAMEWORKS.....	23
A.	OVERVIEW OF EXISTING CYBERSECURITY FRAMEWORKS.....	23
B.	CYBERSECURITY FRAMEWORKS.....	24
C.	RISK FRAMING IN PRACTICE.....	30
V.	METHODS	33
A.	RESEARCH DESIGN	33
B.	RESEARCH QUESTION AND HYPOTHESIS.....	33
C.	PARTICIPANTS AND SETTINGS.....	34
1.	Subject Matter Experts	34
2.	Scenarios / Tasks	35
D.	INSTRUMENTATION AND PROCEDURES	36
VI.	DATA ANALYSIS	37
A.	FRAMEWORK DESCRIPTION	37
B.	TASK 1: TRANSPORT AND/OR PROVIDE FOR CASUALTY / PATIENT EVACUATION	38
1.	Operations Department.....	38
2.	Supply / Logistics Department.....	41
3.	Combined Analysis	43
C.	TASK 2: CONDUCT DAY HELICOPTER OPERATIONS	43
1.	Operations Department.....	43

2.	Supply / Logistics Department.....	46
3.	Combined Analysis	47
D.	TASK 3: MAINTAIN READY COMBAT AIR PATROL (CAP)	47
1.	Operations Department.....	48
2.	Supply / Logistics Department.....	49
3.	Combined Analysis	51
E.	TASK 4: DETECT, LOCALIZE, AND TRACK SUBSURFACE CONTACTS WITH ACTIVE/PASSIVE SONOBUOYS	51
1.	Operations Department.....	52
2.	Supply / Logistics Department.....	53
3.	Combined Analysis	54
F.	TASK 5: PLAN / DIRECT ATTACK OF SUBMARINES	55
1.	Operations Department.....	55
2.	Supply / Logistics Department.....	56
3.	Combined Analysis	58
G.	TASK 6: EMERGENCY REPAIRS TO EQUIPMENT CRITICAL TO SHIP'S MISSION.....	58
1.	Operations Department.....	58
2.	Supply / Logistics Department.....	59
3.	Combined Analysis	61
VII.	RESEARCH CONTRIBUTIONS TO THEORY AND PRACTICE.....	63
VIII.	CONCLUSIONS AND FUTURE WORK.....	65
A.	CONCLUSIONS	65
B.	GENERALIZABILITY.....	66
C.	RESEARCH LIMITATIONS.....	66
D.	FUTURE WORK	67
1.	Task Deconstruction and Integration Analysis.....	67
2.	Mission System Analysis.....	67
3.	Graph Mapping and Reduction.....	68
4.	Framework Automation.....	68
APPENDIX A.	MEASUREMENT INSTRUMENT	69
APPENDIX B.	EXPERIMENTAL DATA	77
A.	TASK 1: TRANSPORT AND / OR PROVIDE FOR CASUALTY / PATIENT EVACUATION	77
1.	Operations Department.....	77
2.	Supply/ Logistics Department.....	79

B.	TASK 2: CONDUCT DAILY HELICOPTER OPERATIONS	81
	1. Operations Department.....	81
	2. Supply / Logistics Department.....	83
C.	TASK 3: MAINTAIN READY COMBAT AIR PATROL (CAP)	85
	1. Operations Department.....	85
	2. Supply / Logistics Department.....	87
D.	TASK4: DETECT, LOCALIZE, AND TRACK SUBSURFACE CONTACTS WITH ACTIVE / PASSIVE SONOBUOYS	89
	1. Operations Department.....	89
	2. Supply / Logistics Department.....	91
E.	TASK 5: PLAN / DIRECT ATTACK OF SUBMARINES	93
	1. Operations Department.....	93
	2. Supply / Logistics Department.....	95
F.	TASK 6: EMERGENCY REPAIRS TO EQUIPMENT CRITICAL TO SHIP'S MISSION.....	97
	1. Operations Department.....	97
	2. Supply / Logistics Department.....	99
	LIST OF REFERENCES	101
	INITIAL DISTRIBUTION LIST	107

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1.	Risk management process. Source: National Institute of Standards and Technology (2011).	25
Figure 2.	Multitiered organization-wide risk management. Source: National Institute of Standards and Technology (2011).	26
Figure 3.	Risk Mitigation Framework Security Life Cycle. Source: National Institute of Standards and Technology (2013).	30
Figure 4.	Operations department cybersecurity requirements for task 1 by percentage of a month's time (uncorrected).	39
Figure 5.	Operations department cybersecurity requirements by percentage of a month's time (corrected).	39
Figure 6.	Task 1 operations requirements by percentage.	40
Figure 7.	Task 1 operations requirements by hours/month.	41
Figure 8.	Task 1 supply/logistics requirements by percentage.	42
Figure 9.	Task 1 supply/logistics requirements by hours/month.	42
Figure 10.	Task 2 operations requirements by percentage.	45
Figure 11.	Task 2 operations requirements by hours/month.	45
Figure 12.	Task 2 supply/logistics requirements by percentage.	46
Figure 13.	Task 2 supply/logistics requirements.	47
Figure 14.	Task 3 operations requirements by percentage.	49
Figure 15.	Task 3 operations requirements by hours/month.	49
Figure 16.	Task 3 supply/logistics requirements by percentage.	50
Figure 17.	Task 3 supply/logistics requirements by hours/month.	51
Figure 18.	Task 4 operations requirements by percentage of time.	52
Figure 19.	Task 4 operations requirements by hours/month.	53
Figure 20.	Task 4 supply/logistics requirements by percentage of time.	54

Figure 21.	Task 4 supply requirements by hours/month.	54
Figure 22.	Task 5 supply requirements by percentage.	56
Figure 23.	Task 5 operations requirements by hours/month.	56
Figure 24.	Task 5 supply/logistics requirement by percentage of time.....	57
Figure 25.	Task 5 supply/logistics requirement by hours/month.	57
Figure 26.	Task 6 operations requirement by percentage of time.	59
Figure 27.	Task 6 supply/logistics requirement by hours/month.	59
Figure 28.	Task 6 supply/logistics requirements by percentage of time.	60
Figure 29.	Task 6 supply/logistics requirements by hours/month.....	60

LIST OF TABLES

Table 1. Security control identifiers and family names. Adapted from National Institute of Standards and Technologies (2013).....29

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AI	Artificial Intelligence
ATO	Air Tasking Order
CAP	Combat Air Patrol
CASREP	Casualty Report
CIA	Confidentiality, Integrity, and Availability
FIPS	Federal Information Processing Standards
HCI	Human-Computer Interaction
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronic Engineers
IL	Information Load
IPC	Information Processing Capacity
ISO	International Standards Organization
JP	Joint Publication
NIST	National Institute of Standards and Technology
OSI	Open Source Interconnect
PCI	Payment Card Industry
PCI-DSS	Payment Card Industry Digital Security Standards
POE	Projected Operational Environment
MIT	Massachusetts Institute of Technology
RMF	Risk Management Framework
ROC	Required Operational Capabilities
SC	Security Category
SIEM	Security Information Event Management
SME	Subject Matter Expert
SOC	Security Operations Center
SP	Special Publication
TTP	Tactic, Techniques, and Procedures

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The completion of an advanced degree is not possible without the support and assistance of mentors, friends, colleagues, and family. I would like to thank my committee for their guidance and support. I'd like to particularly call out the tireless support and guidance of Dr. Dan Boger and Dr. Douglas MacKinnon. I would like to thank my friends, Dr. Michael Klipstein, Dr. Lydia Kostopoulos, and Ms. Natasha Cohen for their friendship and constant encouragement. Ms. Sara-Jayne Terp deserves special thanks for not only cheerleading, but more importantly, kicking me when I needed it. Finally, I'd like to thank my family for enduring my long absences and interminable editing sessions, and for providing their enduring love.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. CURRENT CYBERSECURITY CHALLENGE

This dissertation demonstrates that there is a better methodology to assess cybersecurity risk and incorporates this risk model to reduce the information overload of cybersecurity personnel by addressing a gap in existing information overload theory and providing a method for selectively filtering information based on relevance prior to processing. This is especially important as societal reliance on connected information systems increases while the size and scope of interconnected networks continue to outgrow both the number of qualified cybersecurity personnel and the ability of those cybersecurity personnel to adequately analyze sensor data to be able to defend those networks. While great strides have been made in using automation to correlate log entries, there has been little effort in updating operational cybersecurity risk models or addressing the human information overload situation for cybersecurity directly.

Information security, computer security, and cybersecurity are functionally equivalent terms used to describe the presence of three security principles: confidentiality, integrity, and availability (Harris, 2003; Stallings, 2014). These three principles are colloquially known as the CIA triad. Confidentiality is that principle that guarantees that only the initiator and authorized recipients are capable of accessing information. Integrity is that principle which guarantees only authorized personnel are capable of modifying information, and that the information received is the same information transmitted. Finally, availability is that principle which guarantees timely and reliable access to information. Historically, cybersecurity has required the simultaneous and continuous presence of all three principles of the CIA triad.

On Department of Defense Networks, the cybersecurity posture of a network is monitored by personnel in a Security Operations Center (SOC). SOC personnel monitor the state of the network via the use of an integrated Security Information Event Management (SIEM) system whose function is to accept, integrate, and display a variety of logs from sensors throughout the network. A nominal SOC composition will consist of three tiers of analysts and a SOC manager (Torres, 2015). Tier 3 alert analysts monitor the

SIEM system on a continuous basis and triage security alerts. In some cases, the alert will result in the initiation of a standardized process. In other cases, the alert may lead to an exception condition which requires further guidance. Upon detection of an exception, Tier 3 analysts may contact a Tier 2 analyst. Tier 2 analysts are more experienced and knowledgeable and can conduct a more thorough investigation into the exception condition. By correlating data from various sources, they can determine if an exception has occurred and what, if any, impact there is to the security posture and state of the network. If necessary, a Tier 1 analyst may be contacted to bring specific subject matter expertise on a particular portion of the network or particular piece of equipment. Tier 1 analysts are also called upon to direct corrective action to address exception conditions. Overseeing the SOC is the SOC manager who is responsible for managing resources including personnel, technology, and budget.

SOC personnel work in a constant state of information overload. The size and speed of networks has outpaced the growth of cybersecurity talent by orders of magnitude. In 2014, the number of systems connected to the internet exceeded the number of humans on the planet. Depending on the source, the number of devices on the internet is predicted to be between four and five times the number of people on the planet in 2020. In addition to the massive number of devices, the number of alerts and log entries is tremendous. In 2012, the Institute of Electronics and Electrical Engineers' (IEEE) Visual Analytics Science and Technology challenge included forty hours of firewall and intrusion detection system (IDS) logs totaling over 23 million firewall entries and almost 38 thousand IDS alerts (Zhong, Yen, Liu, & Erbacher, 2016). Currently, a SOC responsible for managing a network of thousands of computers on a U.S. Navy aircraft carrier will normally have fewer than ten personnel on shift at any given time. That network will support off-ship connectivity of several gigabits per second, normal information technology, propulsion systems, engineering systems, and weapon systems supporting over four thousand personnel. Put more simply, assuming ten personnel on a U.S. Navy Carrier SOC, each would have to read, analyze, and incorporate 67,000 pages of text per second to have total information awareness of the state of the network. These expectation are unrealistic and expected to

worsen as more devices are added to the network and the speed of transmission of those networks continues to increase.

As the quantity of information we've asked SOC personnel to analyze has increased, there has not been a corresponding increase in the workforce. The current gap of cybersecurity personnel in the United States is estimated to be half a million and will be required to grow by sixty-two percent this year to keep up with demand in the United States ((ISC)², 2019). Within the United States, the cybersecurity workforce is estimated to be less than half a percent of the total workforce. The projected increase in cybersecurity personnel is projected to be a significant shortfall over the growth in requirements.

To compound the situation, organizational theory suggests that working in states of uncertainty and dealing with exceptions exacerbate information overload (J. Galbraith, 1973). Due to the nature of their task, SOC personnel must specifically monitor for exceptions in a state of relative uncertainty as to the actual state of cybersecurity on the network. This puts cybersecurity in an intractable situation.

To summarize, there are insufficient cybersecurity personnel; the personnel in cybersecurity are in a constant state of information overload; and the shortfall of required cybersecurity personnel will continue to widen as the size of networks continue to grow. Computer science and organizational theory have attempted to address these issues through automating human processes or through the creation of slack resources. Neither of these solution sets have been able to independently keep pace with the rapid rate of information overload in cybersecurity. To improve the current situation, a framework must be developed that integrates organizational theory and computer science theories with the socio-technical system formed by considering computer networks, their operational intent, and their intended users. This combined approach will allow for optimization of human analysts' time by selectively reducing the quantity of information they are asked to analyze (Veeramachaneni, Arnaldo, Korrapati, Bassias, & Li, 2016).

B. HYPOTHESIS, RESEARCH QUESTION, AND POTENTIAL CONTRIBUTIONS

This research attempts to answer the question: *Can a new risk framework reduce information overload for cyber defenders while providing at least equivalent security?* This dissertation advances the hypothesis that a framework built on subject matter expert (SME) knowledge and the uncertainty that the SME acknowledges will allow decision makers to more accurately assess risk, and, consequently, better decide what information may be ignored by network defenders while providing at least equivalent security monitoring.

This research proposes a framework that gives organizations a more comprehensive understanding as to the minimum network security posture and baseline security principles required to meet mission essential tasks. This framework considers the network and organization as its operational context changes over time, and therefore recognizes not only the tasks required but the time period for which they are required. This will challenge the long-held assumption that all three security principles of the CIA triad must always be present for all computing assets. The proposed framework will apply existing information overload theory to the cybersecurity problem and challenge assumptions held by network defenders and information security professionals.

The proposed framework will allow for the extension of information overload theories introducing the concept of efficiency, in which efficiency is re-defined as decreasing false positive rates while reducing data analyzed by SOC personnel, based upon mission essential tasks and security requirements. Simply restated, the desired goal of this framework is to reduce the amount of information that requires human analysis, while providing a more accurate assessment of the state of the network. This increase in efficiency is achieved by a priori decisions on the relevance of information based upon the requirements associated with essential operational tasks. Previous efforts on the use of efficiency have concerned themselves with better use of all available data as opposed to actually reducing data (Heylighen, 2004). Existing theory acknowledges that organizations may choose to process less information, thereby reducing utilization of information processing capacity, creating slack resources, to address information overload. Existing theory recognizes the one method to reduce information overload is to simply process less

information leading to a lower utilization of existing information processing capacity (J. R. Galbraith, 1995). Additional theory has recognized that decision makers often request more information than necessary to make a decision, and that this tendency results simultaneously in poor decisions and more confidence in those decisions (O'Reilly, 1980). This tendency also serves to exacerbate information overload. Finally, existing theory suggests selectively filtering information based on relevance prior to processing, but acknowledges that filtering systems may be brittle with respect to context (Woods, Patterson, & Roth, 2002).

This research potentially adds the following contributions to the existing body of knowledge:

- It incorporates subject matter expert (SME) mental models of risk and security requirements based on mission task.
- It proposes a risk model for the required cybersecurity posture of a network as a function of time and tasks along the three axes of confidentiality, integrity, and availability
- It suggests a method for filtering cybersecurity information based on an a priori analysis of information relevance to baseline requirements of mission tasks performed on the network
- It suggests a method for the visualization of unacceptable risk as a surface map of confidentiality, integrity, and availability over time, thereby allowing for informed discussions of acceptable risk

The proposed framework assesses cybersecurity risk based upon a needs-based analysis of mission essential tasks performed on the network. By assuring that requirements for mission essential tasks are met, information can be filtered on relevance prior to requiring human information processing. Combined with existing studies on decision-making and information overload, we show that this framework could result in a significantly improved cybersecurity posture by reducing information overload, false

positives, and false negatives, while simultaneously improving decision-making performance.

Chapter II discusses the current state of cybersecurity, the cybersecurity workforce, computer science efforts to address cybersecurity, and the limitations of computers to resolve cybersecurity challenges. Chapter III presents the concept of information overload, the negative effects of information overload, the motivations that inadvertently place decision makers and organizations in information overload, and organizational theory attempts to mitigate information overload. Chapter IV introduces the current concept of cybersecurity frameworks and mission essential tasks. Chapter V describes the methods undertaken in this research, the method of quantifying unacceptable risk, and the method of reducing information overload based on unacceptable risk. Chapter VI presents data analysis and acknowledges the limitations of this research. Chapter VII includes the conclusion and suggestions for future work.

II. COMPUTER SCIENCE AND CYBERSECURITY

A. THE UNDECIDABLE NATURE OF SECURITY

Increasing information processing capacity has been the primary effort of computer scientists in cybersecurity since Dorothy Denning (1987) first suggested the use of an automated intrusion system in 1987. Continued improvement in processing power and techniques for anomaly detection has increased the rate at which cybersecurity information may be processed by Turing machines. Artificial intelligence techniques have been implemented to automate human tasks and automate decision making; however, these techniques still face hard limits on accurate security decisions.

The theoretical study of using computers to solve certain types of problems is a field of mathematics called automata. Before developing an algorithm to solve a problem, a computer scientist must classify the problem to determine if it can be solved by a computer. In the broadest terms, problems are decidable (can be solved by a computer) or undecidable (cannot be solved by a computer). In computer science, a problem is decidable if an algorithm can be devised for which a definitive answer of “yes” or “no” can be reached for any input (Kelley, 1995). If a problem is undecidable, it cannot be completely solved regardless of the amount of computing resources available. The Halting Problem asks if, given an arbitrary program and input for that program, a Turing machine can determine if the program halts on that input. The Halting problem is one of many problems provably undecidable. The Halting problem can be represented as this:

“Let M be an arbitrary Turing machine with input alphabet Σ . Let $\omega \in \Sigma^*$.¹
Will M halt when begun on the input string ω ?” (Kelley, 1995, p. 192)

It is important to note, that for the Halting problem to be decidable, a single algorithm must be able to decide for all programs and all inputs to those programs. Algorithms can “cheat” a solution by reducing the universe of inputs or making assumptions. Either of the above will result in some rate of erroneous results represented as some combination of false positives or false negatives.

¹ If Σ is an alphabet, Σ^* is the set of all possible strings of length zero or more in Σ (Igarashi et al., 2014)

In automata, a reduction is a proof by contradiction where a question of interest can be shown to be a subset of an undecidable problem. In the case of cybersecurity, we can ask, “Given an arbitrary input to our network, is that input a violation of cybersecurity (i.e., confidentiality, integrity, or availability)?” This question is analogous to the question posed by the Halting problem. The reduction of the cybersecurity question would read as such:

Assume that the cybersecurity violation is a decidable problem, and the algorithm that solves the cybersecurity question could be encoded on a computer chip. A system could now be built for which a program and the input to the program are provided and we can redefine “halt” as “in compliance of cybersecurity” and “doesn’t halt” as “in violation of cybersecurity policy.”

If the above were possible, we could solve the Halting problem. This creates a logical fallacy: since the Halting problem is undecidable, deciding whether an arbitrary input violates policy must also be undecidable. Many of the questions of interest in security are reducible to known undecidable problems.

B. COMPUTER ARCHITECTURE CHALLENGES TO SECURITY

The undecidable nature of security is exacerbated by current computer architecture. Most general purpose computers use the Von Neumann architecture (Intel Corporation, 2011; Silberschatz & Galvin, 1995). In the Von Neumann architecture, there is a single shared memory space for both code and data. Since both code and data are represented in binary, any given sequence of binary digits could arbitrarily be code or data. The root cause of most software exploits takes advantage of this duality (Anley, Heasman, Linder, & Richarte, 2007; BlackAngel, 2009; Harper et al., 2011; Ligh, Case, Levy, & Walters, 2014). When a computer is exploited, it is convinced to run code other than that intended by the original software author. This is typically done by convincing the computer that data input from the user is actually code to be executed, or by convincing the computer the data input from the user points to a memory location that contains code that should be executed (Anley et al., 2007; BlackAngel, 2009; Harper et al., 2011).

C. TRADITIONAL AUTOMATION OF CYBERSECURITY

While the Von Neumann architecture makes it difficult to detect exploits, and the Halting Problem guarantees that the problem is undecidable, computers are not completely incapable of detecting cybersecurity problems. Current solutions can provide some answers to cybersecurity questions by being willing to accept errors in the form of type I errors (false positive) and type II errors (false negative). False positives present as log entries in network sensors which then require a person to decide if the log entry represents a cybersecurity event or a false positive. A false negative would be the failure to alert on a real cybersecurity incident. As the false positive rate increases, the number of incidents that humans must analyze increases. If the false negative rate increases, the number of undetected incidents increases. Network owners must carefully balance their acceptable risk based upon mission and available resources. The best-known automated detection rate is roughly eighty-five percent. That detection rate currently belongs to AI², a Massachusetts Institute of Technology developed supervised machine-learning model that is paired with humans to “learn” which identified incidents are real incidents, and which are false positives. Detection and prevention of cybersecurity incidents via automated methods alone cannot solve our network security problems (Shim, 2010).

Implementation of detection and countermeasures on networks comes at a cost. Clearly there is a financial cost in development, deployment, and maintenance of automated security measures. Due to the limitations on accuracy, there is a personnel cost required to monitor the output of these security systems. Additionally, there are numerous operational costs to implementation of such countermeasures. Operational costs may include reduced functionality, reduced interoperability, reduced ease of use, reduced output, and time delays (Buckshaw, 2005).

Despite the known limitations of Turing machines, computer scientists have endeavored to reduce both false positive and false negative errors through the use of various automated algorithms (Denning, 1987; Harris, 2008; Kewley & Bouchard, 2001; Qin & Lee, 2004; Ramaki, Khosravi-Farmad, & Bafghi, 2015; Veeramachaneni et al., 2016). Automation has focused on various heuristic methods for attack prediction or attack detection. The detection of an unwanted indicator is often referred to as “blacklisting” and

assumes an open world view that anything not previously identified as bad is good (Harris, 2008). The opposite “closed world” view, assumption that something is unwanted unless it has previously been identified as “good,” is “white-listing,” and has proven too costly in most cases (Harris, 2008). While white-listing systems are in use, those systems tend to have a very limited scope. Using a white-listing system tends to have very high cost of reduced interoperability and ease-of-use.

Static systems are those systems for which heuristic signatures are not automatically created. In this case, signatures are a distinctive pattern or characteristic by which something, such as a piece of malware, can be identified. Most commercial systems are static and require signatures to be created, updated, and prioritized to detect an activity. This is obviously problematic in the cases where a previously unknown attack is used. Without prior knowledge, a static heuristic system will not have a signature with which to detect previously unknown malicious activity and will therefore result in a false negative error (Harris, 2008). To reduce the likelihood of a false negative, most organizations are willing to accept significantly more false positives, but these false positives must be then investigated by personnel, thereby increasing the analysis workload for personnel. Additionally, many heuristics match on “anomalous” behavior, but rarity is not an indication of malice. Finally, static heuristic models tend to identify information without context. That’s because context requires knowledge of what occurred before and what occurs next. In networks, this usually means information across several devices that have different reporting mechanisms, standards, and signatures.

D. ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

Plan recognition in cybersecurity has been an active research area for artificial intelligence (AI) and follows either keyhole recognition or intended recognition depending on the agent being observed (Buckshaw, 2005; Kewley & Bouchard, 2001). In intended recognition, the agent is aware of being observed and is a willing participant. The human training of an AI system to recognize a task for automation is an example of intended recognition. Intended recognition is used for applications such as expert systems. In keyhole recognition, the agent is not aware of being observed, but does not attempt to

impact or thwart the detection. While keyhole recognition might be appropriate for a legitimate user who inadvertently conducts an action that violates cybersecurity policy, a truly malicious actor will purposefully implement techniques, tactics, and procedures (TTPs) to avoid detection (Buckshaw, 2005). This kind of adversarial action adds a layer of complexity making plan detection far more difficult.

Plan recognition adds some context, but like other static heuristic methods, requires that a valid signature exist in the library. Research into development of a library of these attack trees has shown that while the search for the correct signature has a linear time complexity, there is a quadratic memory requirement (Buckshaw, 2005). The number of combinations that must be tracked for every eventuality make the creation of a complete library intractable even if every possible combination were known and could be enumerated. The alternative is to allow for partial matches, which will result in false positive and false negative errors. Additionally, it is not reasonable to assume that all actions can be monitored. Network architecture, encryption, and the simple financial cost of placing sensors to measure everything limit what may be observed. Another paradox to consider is that the monitoring tool is the point of intrusion. There are numerous historical cases in which the intrusion leveraged a vulnerability in anti-virus software or a hardware firewall. Each one of the above challenges results in errors that require personnel to review information to make a final determination.

Dynamic heuristics allow for any AI system to learn from previous instances. The two primary methodologies for learning AI are unsupervised learning and supervised learning. In unsupervised learning, rules for classification are provided and then a large amount of data is fed to the learning system for analysis and the measurement of results from its classification (O'Neil, 2016; Veeramachaneni et al., 2016). The learning occurs without human intervention or evaluation of performance until after the heuristics have been built from the learning data. In supervised learning, there is a human "in the loop" who assesses the learning algorithms classification and provides feedback as it learns. This ostensibly allows for better learning by providing corrective actions as the system learns (O'Neil, 2016; Veeramachaneni et al., 2016).

A comprehensive discussion of the strengths and weaknesses of AI systems is beyond the scope of this research; however, Cathy O’Neil’s book, *Weapons of Math Destruction* is an excellent source. A short explanation of some of the perils of AI is warranted and the examples are largely based on the aforementioned book. One of the challenges with AI systems is that they are not explainable. By explainable, what is meant is that no auditable trail is created that explains how the AI arrived at a particular classification decision (O’Neil, 2016). This leads to numerous challenges in validating the heuristic model that is used to learn AI classification signatures.

A trivial example of a classification error might be the “Black Swan” problem. The Black Swan problem describes an unexpected event. If an AI algorithm were trained to characterize swans in an unsupervised fashion, it might conclude that all swans were white and misclassify a black swan as not being a swan (Godfrey-Smith, 2003). On the surface, it seems that this type of anomaly detection would be good thing for a cybersecurity monitor, but it can lead to large numbers of either false positives or false negatives. Not only would these errors exacerbate the information overload problem for network defenders, they lead to user frustration as the user is blocked from doing a task that should be allowed. Without the introduction of malice, this occurs because a heuristic model is poorly defined. Usually this poor definition is due to bias in the researcher who created the classification heuristic. There is, however, another way for bias to lead an AI awry. If the data used to train the heuristic is biased, the results will also be biased. In the aforementioned case, maybe all of the pictures fed to the AI were of white swans and there were no instances of black swans included in the training set. In cybersecurity, that data is virtually guaranteed to be biased as not all attacks are known, and, therefore, there is a significant probability of a previously unknown attack being misclassified as normal behavior.

In supervised learning, humans are “in the loop” and can validate or invalidate the classification results of the AI. This serves as a feedback loop that the model can integrate into future classification decisions and allows for detection of a bad heuristic model after fewer classification decisions. A supervised learning model necessitates a much longer time to train, as humans must validate the decisions. This can lead to a different issue, as

the humans conducting verification may maliciously provide false feedback to the learning algorithm. Even without malice, humans grow tired and bored. After repetitive tasks and decisions, a human will inadvertently (or sometimes consciously) provide the wrong feedback. Additionally, two different humans, both acting in good faith, could also provide contradictory feedback.

MIT's AI² system uses a supervised learning model to classify cybersecurity validations in an attempt to triage the amount of information that must be analyzed by humans (Veeramachaneni et al., 2016). The maximum classification accuracy of AI² was seventy-five percent before supervised training and eighty percent with supervised learning when analysts were shown 1000 alerts a day. Unfortunately, this is insufficient, and Veeramachaneni et al. (2016) found that analysts could only be expected to handle only about 0.00001% of overall event volume. To add another measure of scope, the MIT team had access to three months of logs totaling 3.6 billion log entries—an average of 40 million log entries per day. This means that at a maximum of 1000 alerts per day, 40,000 analysts would be needed.

Computer science has been unable to find a solution to the cybersecurity problem. Static heuristics require far more computing resources than will ever be available and require a complete catalog of every possible signature. Artificial intelligence is able to help with data triage; however, there are hard limits on any algorithm running on a Turing machine. For the time being, human analysts must be relied upon to identify the vast majority of incidents and discern true events from false positives. Even state-of-the-art supervised learning systems provide an inadequate level of protection and require humans to analyze a massive quantity of information, placing them in a continuous state of information overload.

THIS PAGE INTENTIONALLY LEFT BLANK

III. INFORMATION OVERLOAD

The term “information overload” has been used in various disciplines including organizational theory, psychology, and marketing, but has rarely been addressed using a multi-disciplinary approach (Anderson & de Palma, 2012). To address information overload, it is important to first define the concept. Once information overload is defined, it must be explained why being in a condition of information overload is undesirable as well as why an individual or organization might subject themselves to a condition of information overload. Finally, a summary of current tactics, techniques, and procedures for addressing information overload will be presented.

Numerous authors have suggested that organizations can be viewed as information processing systems (J. R. Galbraith, 1995; O’Reilly, 1980), and traditionally, there has been an assumption that information is good (Himma, 2007). While a discussion of information theory and knowledge management is beyond the scope of this paper, it is helpful to examine a few definitions of information. Himma (2007) defines information as “true propositional content.” Claude Shannon provides a mathematical definition of information as an object whose content value measured by how many questions it answers (Himma, 2007). Colin Cherry defines three levels of analysis: “Information consists of symbols generated using a limited range of characters according to certain rules (syntax), which have a concrete, abstract or objective meaning (semantics), and the content of which is interpreted by the sender and recipient of the information in a certain way (pragmatics)” (Klausegger, Sinkovics, & Zou, 2007; Schram & Cherry, 1957).

While useful, these definitions require a bit of clarification within the context of cybersecurity. The first challenge is clarifying the concept of truthfulness. In the above section, the concepts of false positives and false negatives were introduced. In the case of a false negative, no propositional statement is made, and therefore there is no statement to evaluate for truthfulness. In the case of a false positive, a propositional statement is made, but it must still be true to be considered information. On first glance, it may seem that a false propositional statement was made, but this would be incorrect. A log entry generated by a Turing machine says that a condition requiring a log entry has been found. This

condition is the result of a signature or heuristic and it must have been met to generate an entry. The “falseness” of the statement comes from the interpretation of the semantics (meaning) of that entry. As an example, in the case of a firewall, network defenders create and employ signatures meant to identify indicators (e.g., a pattern of bytes in network traffic) from which an inference of an event can be made (e.g., identification of a virus signaling infection). A log entry is made when traffic traverses the firewall that exactly matches that signature, but it is up to a system administrator to determine if that match identifies the intended ascribed meaning. The truth of the match is not in question. This may happen for several reasons including choosing a characteristic that is not unique to the artifact or event of concern. In this sense, all entries generated in logs by network sensors and other Turing machines on the network are, in fact, true propositional statements and therefore information. It is important to note, however, that content cannot be valued simply for its truth; there are plenty of propositions that are true and yet not valuable within a given context (Kastenmüller et al., 2014).

The Oxford English Dictionary Online defines information overload as “Exposure to or provision of too much information; a problematic situation or state of mental stress arising from this” (Himma, 2007). Whether someone is in a state of information overload requires a comprehensive socio-scientific analysis and requires a multivariate analysis of numerous factors affecting an individual that go beyond what is needed to clarify the concept (Himma, 2007). From a mathematical standpoint, the descriptive claim is that: “(1) P has an excessive amount of x relative to some defined standard or an appropriate amount; and (2) P incurs some negative effect E” (Himma, 2007, p. 265). “The normative claim is that the effect E on P from too much x is undesirable or problematic” (Himma, 2007, p. 265).

The descriptive claim is easy to address. It can be stated that “information overload occurs when the information processing demands on time (information load, IL) to perform interactions and internal calculations exceed the supply or capacity of time available (information processing capacity, IPC) for such processing” (Bergamaschi, Guerra, & Leiba, 2010). Restated mathematically, information overload occurs when $IL > IPC$. All information processing requires resources. At a minimum, all information processing

requires attention (Himma, 2007). Attention is, at the individual level, a fixed resource. While that resource may be optimized by reducing tasks, minimizing distractions, ensuring proper rest, or other methods, no more attention may be created in an individual.

Thus far, we have defined only that there is more information that can usefully processed, but the negative effect required for our definition of information overload has not been identified. If information is excessive simply because it cannot be processed, it is qualitatively equivalent to not having the excess information (Himma, 2007). Regardless, processing information to decide what is useful is paramount as incorrect or incomplete information can yield a decision with negative consequences (Bergamaschi et al., 2010). Numerous fields have identified negative effects to humans in information overload conditions, including stress and poor decision making (Anderson & de Palma, 2012; Himma, 2007). Some studies have also suggested that increased quantities of irrelevant information reduce decision making performance by reducing the ability to identify relevant information (O'Reilly, 1980). Furthermore, these studies have shown that while increased information may reduce decision making accuracy, it has simultaneously increased a subject's confidence in their decision.

Even without intentionally processing additional information, simple awareness that there is more content than can be processed leads to techno stress, which may manifest with typical symptoms associated with other physiological stress: depression, anxiety, or panic (Himma, 2007). Another idea proposed suggests that having to process too much information leaves less time that would be better spent on thinking, analysis, and contemplation to arrive at a correct decision (Levy, 2005). These combined effects can lead to increased cognitive friction and cognitive easing which may reduce the likelihood of recognizing and correcting a previous error, lead to additional bias, and further reduce decision making performance.

From a cybersecurity perspective, we must measure the negative effect of information overload on the security of the network. Per the discussion in the previous section, for a given amount of information I that is logged by a Turing machine on a network, there will be some subset that represents false positives (FP) such that $FP \in I$. There is also a subset of I that represents true positives (TP) such that $I = \Sigma FP + \Sigma TP$. It

stands to reason that if $IL > IPC$, there is some subset of I that is not evaluated. It also follows that while some of the unevaluated information may consist of false positives, some may also consist of true positives. The inability to process a true positive detection of a network security incident is a negative and undesired effect. Additionally, there may be some number of false negatives that are incidents not logged by computing machines at all. In some cases, these incidents may be identified by significant processing of what appear to be unrelated log entries or outside information (e.g., a phone call by a user describing unexpected behavior in a network device). At best, the inability to appropriately process indicators that may infer a false negative yields the negative effect of not having detected a cybersecurity incident. In a case that proves even more problematic, false negatives incur an additional cost on limited attention resources, further reducing the ability to appropriately process false positives or true positives, yielding a possible situation in which both false positives and false negatives are incorrectly addressed.

As the overarching concept of information overload and its negative effects is now understood, it's important to understand why an individual or an organization may find themselves in an information overload condition. As previously discussed, the lack of sufficient resources, whether insufficient time or attention to process information, is the dominant factor in whether an information overload condition will exist (Kock, 2000). Any condition or requirement that reduces time or attention serves to exacerbate the information overload condition. Some of these conditions are situational, but some are also sociological or psychological.

Some job functions and processes create conditions that exacerbate information overload. Cybersecurity, by its very nature, works in uncertainty. Uncertainty creates a need for more information for disambiguation, but it does so without necessarily adding the resources required to process the additional information requirement (O'Reilly, 1980). The number of information exchanges required of a team necessarily increases interruptions of information processing, thereby lowering processing efficiency (Kock, 2000). These information exchanges also allow for a chance of miscommunication, which increases uncertainty. In either case, these conditions increase the time pressure and therefore the overload condition. In cybersecurity managing the operational context of log

entries is paramount to decision making. Managing operational context requires constant cognitive context switches, and these switches reduce information processing capacity (Simperl et al., 2010). These conditions exacerbate the information overload condition for cybersecurity practitioners, yet are inseparable from their duties.

Beyond situational conditions, there are interesting phenomena in psychology that will drive people to willingly seek more information, even when in an information overload condition. The first psychological condition affecting information overload is the inability to perceive one's own information processing limits objectively (O'Reilly, 1980). People tend to over-estimate their own capabilities and seek information far beyond what they can accurately process. This leads to a paradox: subjects who are overloaded with information are more confident and satisfied with their decisions and communication; however, they perform more poorly than those given less information (O'Reilly, 1980). Previous efforts have identified several reasons why decision makers obtain so much information as to self-induce an information overload condition (Anderson & de Palma, 2012). One reason is that they receive unsolicited information. While this can be somewhat remedied through the institution of standard procedures, it can never really be eliminated. The other reasons are existentially harder to correct. Decision makers collect information because they want to demonstrate a commitment to rationalism and need to be able to justify the logic of their decisions (Anderson & de Palma, 2012). Additionally, decision makers may seek additional information to confirm previous information to provide feelings of safety. Finally, decision makers seek additional information in the case that it might prove useful in the future or to use as a type of currency to avoid falling behind colleagues (Anderson & de Palma, 2012). While none of these psychological conditions are surprising, self-identification of biases remains challenging even for those formally trained on the subject.

Organizational theory has provided some insight into dealing with information overload in complex organizations. The recommended methods of reducing information overload are to limit the need to process information or to increase the capacity to process it (J. Galbraith, 1973). Galbraith suggests that increasing the capacity to process information may include investment in vertical information systems or the creation of lateral relations (1973). According to Galbraith, reducing the need for information

processing can be accomplished through the creation of slack resources and/or the creation of self-contained tasks (1973).

As previously discussed, increasing information processing capacity has been the primary effort in cybersecurity; however, Turing's Halting problem guarantees that no automated information system will be able to do this sufficiently (Martin, 1996; Kelley, 1995). This serves to increase uncertainty in its own way as personnel must determine if an alert is relevant to the current security posture of the network.

To increase detection rate without slowing down the speed of transmission, a defense-in-depth approach has historically been implemented. This is exactly what is meant by investment in vertical information systems. Devices at various points in the network will only monitor information within a subset of the Open Sources Interconnection (OSI) protocol layers. For example, intrusion detection systems may monitor the transmission and network layers of the OSI model, while application proxies may monitor the network and application layers. By limiting analysis to a subset of the available information and providing overlap in analysis, increased accuracy and resiliency may be obtained without unacceptable slowing of network traffic. Unfortunately, each of these devices also produces its own logs and in its own format. These logs must inevitably be analyzed by SOC analysts to determine the state of the network.

According to organizational theory proposed by Galbraith, reducing the need for processing may be accomplished via the creation of slack resources or the creation of self-contained tasks (1973). Reducing the information that must be processed has been suggested by others (Bergamaschi et al., 2010; O'Reilly, 1980). The creation of slack resources in the case of SOCs is conducted by adding additional information processing capacity in the form of personnel or the introduction of additional computing power. The use of additional processing power may reduce computational overhead for automated sensors but does nothing to address information overload in the humans nor to reduce the uncertainty inherent within cybersecurity. As for adding personnel, the lack of a sufficient pool of qualified candidates is a well-known fact in industry. There simply aren't enough qualified personnel to fill positions even at current staffing levels (Chant, 2017).

The creation of self-contained tasks (J. Galbraith, 1973) has also been tried. By creating different tiers of analysts, as well as allowing for specialization and defined incident response procedures, some amount of overload reduction has been achieved. Unfortunately, the reduction in overload via these types of efforts has been insignificant compared to the increase in information that has come with increased network size and speed. An increase in network size equates to an increase in devices on the network; each additional device on the network creates additional logs, alerts, and other information which should be processed by SOC personnel. Similarly, an increase in network speed allows for more information to be transmitted over the network. This additional information is examined by network devices, which likely results in additional alerts which must be analyzed by cybersecurity personnel. Additionally, the fact that SOC analysts must specifically deal with exceptions limits their ability to create self-contained tasks a priori. Self-contained tasks require knowledge of not only what is to be done, but also of how to do it. Due to the complex nature of current networks and network attacks, the number of types of incidents and the corresponding techniques, tactics, and procedures required to appropriately address every security violation can be described by a factorial function. Additionally, new attack techniques are developed on a continual basis, and the discovery of a previously unknown technique after a compromise, known as a zero-day attack, is a routine occurrence that identifies a previous false negative and increased uncertainty.

Clay Shirky, a New York University professor, provides an interesting viewpoint when he states that information overload equates to a filter failure (Bergamaschi et al., 2010). Historically filters have acted on information. This research proposes a new paradigm, specifically, that information be filtered on context prior to processing. If this could be accomplished, it would reduce information load, ensure that only relevant information is presented, and reduce uncertainty.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CYBERSECURITY FRAMEWORKS

A. OVERVIEW OF EXISTING CYBERSECURITY FRAMEWORKS

Chapters II and III introduced the theoretical underpinnings of the challenges faced by cybersecurity practitioners. Chapter IV will introduce the practical application of that theory in the form of cybersecurity risk mitigation frameworks. Risk is defined as “a measure of the extent to which an entity is threatened by a potential circumstance or event” (National Institute of Standards and Technology, 2011, p. B-7). Risk mitigation is defined as, “prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process” (National Institute of Standards and Technology, 2011, p. B-8). The purpose of risk mitigation frameworks is to provide a structured, repeatable approach for managing cybersecurity risk through data and risk categorization, mitigating risk through the selection and implementation of appropriate controls, and the use of best practices (National Institute of Standards and Technology, 2018). As information systems are used to conduct critical business/mission functions, information security becomes a required operational capability (National Institute of Standards and Technology, 2013). Executing a cybersecurity framework allows organizations to link risk management processes at the system and organizational level (National Institute of Standards and Technology, 2013). While some frameworks are general purpose and over-arching, others are industry sector specific. The National Institute of Standards and Technology (NIST) *Risk Management Framework* (RMF) and International Standards Organization (ISO) *27001:2013 Information Security Management Systems* are examples of general-purpose cybersecurity frameworks. The Payment Card Industries (PCI) *Payment Card Industry Digital Security Standards* (PCI-DSS) and Department of Defense Instruction 8510.01 *Risk Management Framework* are industry sector specific frameworks. These standards are greater than 90% similar (Office of the DOD Chief Information Officer [DODCIO] 2014 ; PCI Security Standards Council LLC., 2019) with industry-specific frameworks providing more detailed implementation guidance based on industry best practices. The DOD has made particular efforts to ensure minimum differences between their RMF implementation, DOD Instruction 8500.01, and

NIST's implementation (DODCIO, 2014). The primary differences in these two implementations are due to DOD's requirements to deal with classified information and thus require additional guidance for implementation of cryptographic standards. The rest of this chapter will use NIST's RMF as an exemplar, but similar language and recommendations are found in all standard general-purpose and industry-specific cybersecurity frameworks.

B. CYBERSECURITY FRAMEWORKS

Cybersecurity risk mitigation frameworks seek to provide a standardized approach for risk management. As illustrated in Figure 1, according to NIST, risk management requires that an organization: frame risk, assess risk, respond to risk, and monitor risk to provide a feedback loop for continuous improvement (National Institute of Standards and Technology, 2011). This activity should be carried out holistically at the strategic, operational, and tactical levels as illustrated in Figure 2 (National Institute of Standards and Technology, 2011). The rest of this chapter uses the definition of SOC tiers as described in NIST standards. While not prescriptive in nature, the NIST standards serve as a model on which other SOCs can be based. In order to differentiate NIST definitions of SOC tiers from the generic term, this section will capitalize "Tier" as is done in the NIST documentation.

Tier 1 is responsible for presenting a strategic view of the organizations and provides a list of business/mission functions and their relative priorities. This prioritization serves to inform risk acceptance and promote effective implementation of cybersecurity controls consistent with an organization's strategic goals (National Institute of Standards and Technology, 2013). Tier 2 is responsible for identifying mission and business processes that support the the accomplishment of those strategic goals. Additionally, Tier 2 personnel are responsible for "determining the security categories of the information systems needed to execute those business functions" (National Institute of Standards and Technology, 2013, p. 8). Finally, Tier 2 must incorporate information security requirements into those business processes and monitor their effectiveness.

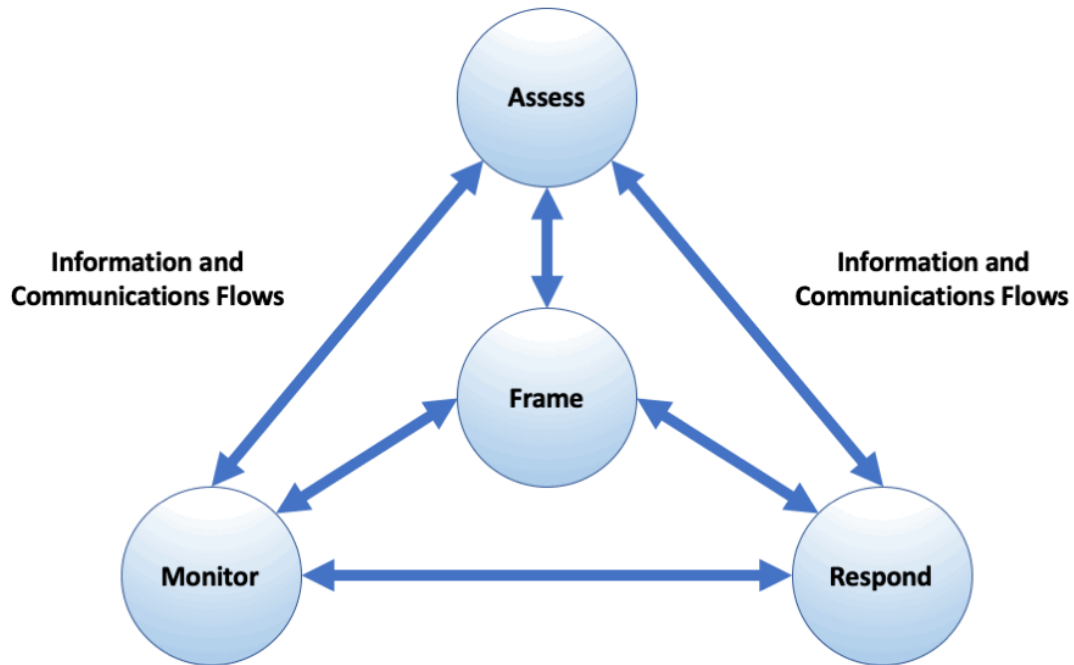


Figure 1. Risk management process. Source: National Institute of Standards and Technology (2011).

The first step in framing risk requires that organizations establish a context by describing the operational environment. Risk framing is, in many ways, the most critical step in risk management. In this step, an organization must recognize and validate assumptions about the operational environment at the strategic, operational, and tactical levels. These include assumptions about threats, vulnerabilities, likelihood of occurrence and severity, degrees of risk uncertainty, and risk tolerance, to name a few (National Institute of Standards and Technology, 2011). Recognizing and validating these assumptions provides a realistic view from which the importance of business/mission functions can be assessed and prioritized, and trade-offs can be made based upon constraints in time or other resources.

Having reconciled the operational environment and validated environmental assumptions, the organization can begin to assess their own organizational risk in the environment. This requires identifying vulnerabilities and risks to the organization's operations, assets, and personnel. During this step, it is critical that the organization understands any constraints in the information gathering phase that may insert additional

assumptions or bias into the process. Once the risks are identified, they are examined for likelihood of occurrence and impact, should they occur.



Figure 2. Multitiered organization-wide risk management. Source: National Institute of Standards and Technology (2011).

To determine the operational impact of a risk, information systems and information must be categorized. As previously discussed, the security objectives are confidentiality, integrity, and availability (Harris, 2008; Information & Standards, 2007). The overall impact of a vulnerability is defined in the Federal Information Processing Standards 199 (FIPS) as a security category. The impact of the loss of any of the security objectives can be described as low, moderate, or high. A potential impact is defined as low if the loss of the security objective will have a limited adverse effect (National Institute of Standards and Technology, 2004). FIPS 199 defines moderate impact as when the loss of confidentiality, integrity, or availability will have a serious adverse effect. Finally, a high severity impact is one in which the loss of a security objective results in catastrophic adverse effects (National Institute of Standards and Technology, 2004). The generalized representation of security category (SC) is expressed as:

$SC_{Information\ Type} = \{(confidentiality, impact), (integrity, impact), (availability, impact)\}$ (NIST, 2004, p. 3)

The overall security category is determined as a ceiling function; the highest impact of any subcomponent determines the overall security category. Hence, if two categories have low impacts and one has a high impact, the overall security category is considered high.

A critical Tier 1 action during this phase is the determination of risk tolerance. NIST defines risk tolerance as “the level of risk that organizations are willing to accept in pursuit of strategic goals and objectives” (National Institute of Standards and Technology, 2011, p. 37). Strategic leadership must clearly communicate acceptable risk assessment methodologies, response strategies, monitoring approaches, and organizational constraints (National Institute of Standards and Technology, 2011). Risk tolerance will vary according to business mission and function as not all functions carry the same priority. As the importance of a function increases, there must be a corresponding degree of risk management. This mission prioritization occurs at Tier 1, is enacted at Tier 2, and directs the actions at Tier 3 (National Institute of Standards and Technology, 2011).

At Tier 2, operational level managers may have different risk tolerances. According to NIST, conflicts can be resolved by applying the security category formula and applying a ceiling function. In practice, it is not uncommon for Tier 1 to accept additional risk and refuse to resource a more restrictive solution recommended by lower tiers.

The third component of risk management examines how an organization responds to a risk. This effort requires organizations determine the appropriate risk response (i.e., accept, mitigate, avoid, share, or transfer) (National Institute of Standards and Technology, 2011). Determining risk response is an organization-wide responsibility that requires the creation and evaluation of alternate courses of action based upon organizational risk framing and risk acceptance. Additional considerations when evaluating courses of action may include resource cost, effectiveness, legal and regulatory requirements, and organizational culture. Tier 3 personnel will implement security controls on specified systems based upon guidance from Tier 1 and Tier 2. If the level of residual risk and implementing controls is deemed acceptable by Tier 1 and Tier 2, risk mitigation may move

on to the next phase. If the level of residual risk is deemed unacceptable, the previous steps are repeated until the level of residual risk is deemed acceptable.

To aid in the selection of controls and mitigations, cybersecurity frameworks routinely include a catalog of baseline security controls. In the NIST RMF, this catalog is in Special Publication (SP) 800–53: Security and Privacy Controls for Federal Information Systems and Organizations. The catalogs list compensating controls by functional families. Table 1 shows the security control family names per SP 800–53. An interesting detail to notice is that the controls are not categorized by the security principle met. Cybersecurity frameworks also suggest or direct the implementation of a baseline set of controls based upon a system’s security category. NIST SP 800-60 Volume II provides a guide for mapping types of information systems to security categories (National Institute of Standards and Technology, 2008); however, NIST SP 800-60 notes that DOD national security systems fall under a different recommended baseline due to their processing of classified information. As previously stated, in most cases the DOD implementation of the RMF matches the NIST implementation. The primary difference is that DOD implementation requires specific cryptographic algorithms be implemented to protect classified information. As the name implies, these baselines recommend only the bare minimum required controls. While these baselines may represent regulatory compliance, they do not represent the needs of a secure system, and may fail to meet an organization’s risk tolerance.

Table 1. Security control identifiers and family names. Adapted from National Institute of Standards and Technologies (2013).

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Service Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

The remaining phase is that of monitoring effectiveness. By monitoring effectiveness, organizations can verify that planned controls and response measures have been implemented correctly and are traceable to a business function, laws, or directives (Department of Defense, 2011). Additionally, monitoring allows for verification that of correct implementation, operation, and desired operational effect of controls (National Institute of Standards and Technology, 2013). The steps of assessing risk, responding to risk, and monitoring the effectiveness of response is a cycle that is continuously executed. NIST’s RMF encourages automated monitoring as more efficient and less prone to human error, but does recognize that not all monitoring can be conducted in an automated fashion. Chapter II explains the limitations of automated monitoring for the purposes of cybersecurity.

Cybersecurity frameworks provide a standardized process by which organizations may tie risk management to business/mission objectives and regulatory requirements. As part of the process, organizations must conduct their own risk framing and risk tolerance. Based upon the risk framing and risk tolerance, a framework may suggest compensating controls that must be selected, implemented, monitored and assessed. Figure 3 summarizes the process as delineated in the RMF. The successful implementation of a risk mitigation framework is predicated on an organization’s ability to understand and describe core

organizational business/mission functions, and to design and implement a set of security capabilities to protect such functions to a level of acceptable risk.

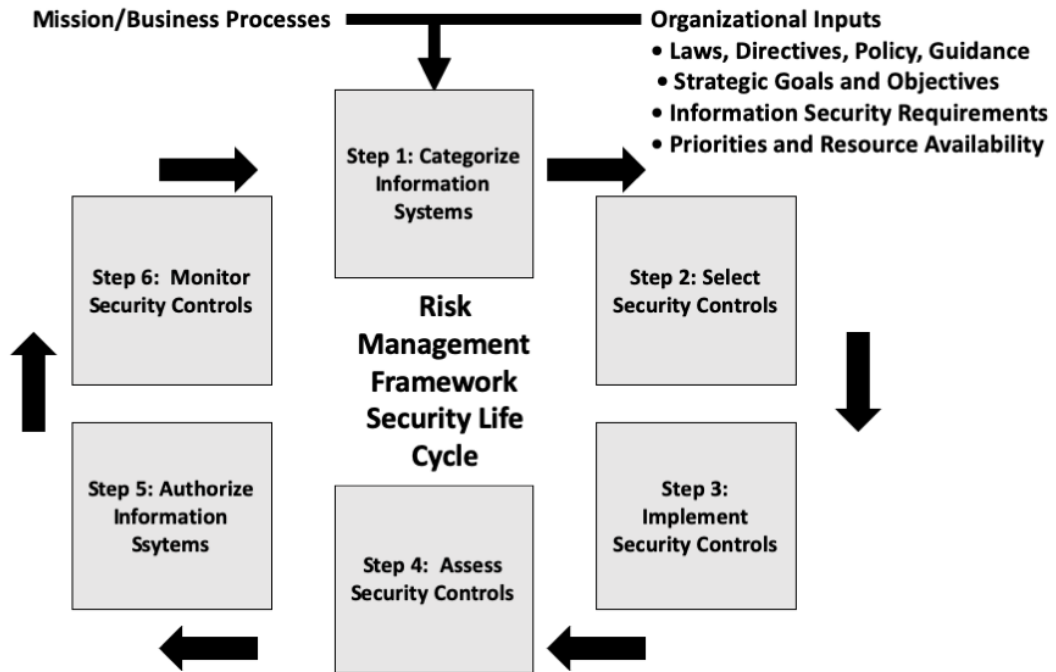


Figure 3. Risk Mitigation Framework Security Life Cycle. Source: National Institute of Standards and Technology (2013).

C. RISK FRAMING IN PRACTICE

To determine appropriate protections, an organization must be able to understand the environment, its core business/mission tasks, and reconcile assumptions. Few organizations have invested as much time and rigor into formalizing this process as the U.S. DOD. The DOD, as an organization, has expended tremendous effort to develop doctrine that links strategic level goals, to operational requirements, and tactical actions. While explaining the whole of the DOD’s joint planning process and U.S. national security strategy is outside the scope of this document, a synopsis linking strategic goals to core business/mission requirements is in order. In U.S. military parlance, “joint” refers to guidance, direction, or operations covering more than one armed service. The DOD and Joint Chiefs of Staff promulgate Joint Publications (JP) to provide strategic-level guidance

to those services. The services implement guidance provided in joint publications in their own service-specific instructions. JP 5-0 is DOD's joint publication for joint planning. Joint planning is "the deliberate process of determining how (the ways) to use military capabilities (the means) in time and space to achieve the objectives (the ends) while considering the associated risks" (Joint Chiefs of Staff, 2017, p. I-1). To accomplish the desired ends in military plans, commanders must decide on core mission functions. These core mission functions are referred to as mission essential tasks by the joint force. The *Joint Mission Essential Task List (JMETL) Development Handbook* states, "joint force commanders must identify the tasks most essential to their assigned or anticipated missions, with priority given to wartime missions" (Joint Chiefs of Staff, 2002, p. 2).

As an organization, DOD must be able to execute assigned missions. Unlike most commercial organizations, DOD must be able to resource unplanned missions. To allow for proper resourcing and capabilities, armed services publish instructions to inform unit commanders of their expected capabilities based on unit type. In the U.S. Navy, these documents are promulgated as instructions by the Chief of Naval Operations and titled *Projected Operational Environment and Required Operational Capabilities (ROC/POE)*. A ROC/POE document provides risk framing (projected operational environment), core mission/business functions (required operational capabilities), and a duration of time that a unit is expected to provide a capability within a core environment. Some capabilities (e.g., employment of weapon systems) are executed only in a wartime environment. Some capabilities are employed in both a peacetime and wartime environment (i.e., safe navigation of a naval vessel), but may require different resourcing due to environment assumptions.

THIS PAGE INTENTIONALLY LEFT BLANK

V. METHODS

This research effort utilized operations and supply/logistic SME expertise to determine the cyber security requirements of assigned mission essential tasks as designated by the United States Navy. The task timelines were divided into preparation, execution, monitoring, and steady-steady state phases, and presented to SMEs for them to determine what cybersecurity principles were required, at which phase, and for how long. These results were compared to the null hypothesis:

Ho: No risk framework can reduce information overload for cyber defenders without negatively affecting security.

A. RESEARCH DESIGN

This research used a correlation design to elicit from SMEs what cybersecurity principles are required to complete mission essential tasks over the lifetime of each task. Any instance that would endanger a required principle for a mission essential task is deemed an unacceptable risk. SMEs were chosen from the operations and logistics departments aboard U.S. Navy nuclear aircraft carriers, and mission essential tasks were chosen from the Required Operational Capability and Project Operational Environment for Multi-purpose Nuclear-powered Aircraft Carrier Instruction (Office of the Chief of Naval Operations, 2014). These SME elicitation were used to calculate the amount of time a security principle is required for a department to complete given task with a 95% confidence interval.

B. RESEARCH QUESTION AND HYPOTHESIS

This research attempts to answer the question: Can a new risk framework reduce information overload for cyber defenders without negatively affecting security? This research advances the hypothesis that a new risk framework built on SME knowledge of requirements can allow cybersecurity defenders to eliminate information less relevant to the completion of essential mission tasks, allowing for a reduction in information overload without negatively affecting mission completion.

This effort proposes creating a framework that does not consider cybersecurity as an atomic state in perpetuity, but instead considers cybersecurity as a time-and-task dependent state based upon one or more cybersecurity principles required to complete a mission essential task. The proposed framework acknowledges that any given task is not completed on a continuous basis, that required cybersecurity principles may change based upon the task as well as on their current phase of execution, and that the presence of any information about security principles beyond what is required is less relevant than required information.

C. PARTICIPANTS AND SETTINGS

This study included two types of participants: aircraft carrier SMEs in the supply/logistics department and aircraft carrier SMEs in the operations department. All SMEs had over five years' experience in the U.S. Navy and were serving or had served in managerial positions (paygrade E7-E9, or O3-O6) aboard a nuclear-powered aircraft carrier within twenty-four months of solicitation.

1. Subject Matter Experts

Expertise was solicited from mid-career and senior officers and enlisted aboard aircraft carriers. While SMEs from any unit type could have been selected, nuclear-powered aircraft carriers are the largest current military asset, employ some of the most senior and experience personnel in the Navy, and have the widest range of missions and mission essential tasks of any Navy unit. This combination of factors makes it more likely that results from these subject matter experts is generalizable. Managerial positions aboard aircraft carriers require more experienced personnel than other units. Enlisted crew with leadership and managerial positions are at paygrades of E7-E9, with officer positions at the O3-O6, paygrades typically with a decade or more experience in the Navy. The deep experience allows for a broader understanding of mission essential tasks of various units, the supporting tasks required for completion, completion timeline, and the security principles required to complete them. All SMEs were currently serving as a nuclear-powered aircraft carrier crew, or had completed a tour within twenty-four months of solicitation.

Expertise was solicited from the two largest Navy concentration areas in the continental United States: San Diego, CA, and Norfolk, VA. There is a total of eleven nuclear-powered aircraft carriers in current service of the U.S. Navy. The data gathered is represents insight from three different nuclear-powered aircraft carriers. When considered over the professional careers of all participating SMEs the experience of seven carriers over multiple tours is represented. It is acknowledged that this is a very finite population; therefore, quantitative analysis required the use of a finite population correction factor.

Communications and networks personnel were specifically excluded to ensure that task owners could provide feedback as to what is needed to complete the mission task without the bias of current cybersecurity implementation. The intent was to ascertain the requirements of the mission essential task, rather than the requirements of the information networks. The operational requirements can then be interpreted into cybersecurity requirements to ensure that cybersecurity requirements truly support what is required to meet mission essential tasks.

2. Scenarios / Tasks

Six mission essential tasks were selected from the Navy's Required Operational Capability (ROC) and Projected Operational Environment (POE) document for nuclear-powered aircraft carriers, OPNAV 3501.65F. This document defines the Navy's risk-framing and mission essential tasks for an aircraft carrier. In addition, this document lists how long a unit is expected to be able to support completion of a task under various risk scenarios. While some tasks are only employed in a wartime environment (e.g., employment of kinetic weapon systems), others are employed throughout the risk spectrum (e.g., medical evacuation of injured personnel). Tasks were chosen to include those that are completed both in the wartime only environment as well as tasks that are completed in both the peacetime and wartime environment. For tasks that are completed across the spectrum of operations, SMEs were asked to consider only peacetime completion of the task. Additionally, tasks were chosen that increased the likelihood of requiring involvement from both logistics and operations departments to complete. Finally, tasks chosen were

meant to limit variation in execution based upon situational specifics such as geographic location or local commander guidance.

D. INSTRUMENTATION AND PROCEDURES

This section discusses the data collection processes and procedures. Data was collected via paper questionnaire with the researcher available to answer questions at the time of data collection. Participant demographic data was collected simultaneously to ensure data was collected from the desired population. At the time of collection, surveys were reviewed for completeness and to ask any follow-up questions arising from either the survey or the responses. The results of some of these questions will be addressed under the research limitations and conclusions section of this dissertation.

All tasks were divided into four phases of completion: preparation, execution, monitoring, and steady-state. The preparation phase was defined as including all preparations and subtasks that must be accomplished prior to execution of the mission essential task. The execution phase includes the actual performance of the task. The monitoring phase is defined as the phase after which active tasks have been conducted and when monitoring may be required to ensure the task has been completed and requires no further action. The steady-state phase is the time period that is not described by one of the aforementioned phases.

For each phase, SMEs were asked to consider a period of thirty days. Tasks have different periodicities and using a uniform time window allows for a normalized comparison of the resources required to complete each task. Within the specified thirty-day time window, SMEs were asked how long their department spends in the preparation, execution, monitoring, and steady-state phase of each task. For each phase of task completion, they were asked what percentage of the time confidentiality, integrity, and availability were required to accomplish the that phase.

VI. DATA ANALYSIS

A. FRAMEWORK DESCRIPTION

This research proposes a framework that reduces information overload for cybersecurity defenders without negatively affecting the cybersecurity of a network. The framework centers around the concept that mission essential tasks are not static and that cybersecurity is not an atomic principle. To that end, it suggests that the required security principles for any mission essential task depends not just on the nature of the task, but also on the current state of task completion at a specific instance in time. As previously stated, tasks are considered in the preparation, execution, monitoring, and steady-state phases. Task owners define the minimum-security principles required for the completion of each phase as well as how long those principles must be present in that phase.

Once data is collected, each principle may be graphed as a curve. The x-axis for such a curve represents time and the y-axis represents what percentage of a given principle must be present at that instant in time. As this curve represents the absolute minimum required to complete the process, any point below the curve results in task failure and therefore represents unacceptable risk. Thus, the acceptable risk is represented by value of the curve and unacceptable risk by any value under the curve. If the curve for representing the requirements for confidentiality is represented by the function f_c , the amount of resources required to mitigate unacceptable risk could be represented by for confidentiality could be calculated by $\int_0^T f_c \frac{dc}{dt}$. Any area above the curve, but below 100% represents excess capacity. It is up to the leadership to frame risk for their organization and decide if excess capacity represents acceptable risk, or if excess capacity can be used to provide a buffer beyond the minimum requirements. The same procedure may be followed to calculate the requirements for integrity and availability represented by f_i and f_a respectively.

B. TASK 1: TRANSPORT AND/OR PROVIDE FOR CASUALTY / PATIENT EVACUATION

Task one required that SMEs consider the task of transporting and/or providing for casualty and patient evacuation. This task is carried out in both wartime and peacetime, with the expectation that the task is carried out more frequently in times of active conflict. SMEs were asked to consider this task during a normal peacetime operation. Under normal peacetime conditions, this task is not a planned event and occurs on an ad-hoc, as-needed basis.

1. Operations Department

One respondent was anomalous in that their confidentiality requirement was more than ten times larger than the average. Although this difference seems catastrophically large, it represents a difference of merely fourteen hours over the mean for a month. Figure 4 shows a zoomed in version of the operations requirements for the CIA triad during preparation, execution, monitoring, and steady-state phases with the anomalous data point. Figure 5 shows the same analysis without the anomalous SME. It's interesting to note that the shape of the curve does not significantly change, nor does the maximum effort required to successfully complete the task. Figures 6 and 7 have been standardized to show a full month's requirements. Figure 6 shows the percentage of time a security principle is required per month to complete task 1. Figure 7 illustrates the number of hours a security principle is required per month to complete task 1.

At no point is there a need for a requirement to exceed five percent and with a z-score of 0.39 at a confidence interval of 95% there is statistical support for the conclusions drawn from this data. This is likely due to a few factors. The anomalous SME in question was in a departmental leadership position with greater insight into operations throughout the ship and not just within their department. This led to a much higher reported amount of time spent preparing for this task as well as a greatly increased confidentiality requirement. The inclusion of this lone data point shifted the standard deviation by more than three-fold, and when, considered along with the SME's knowledge, was discarded as anomalous for this task.

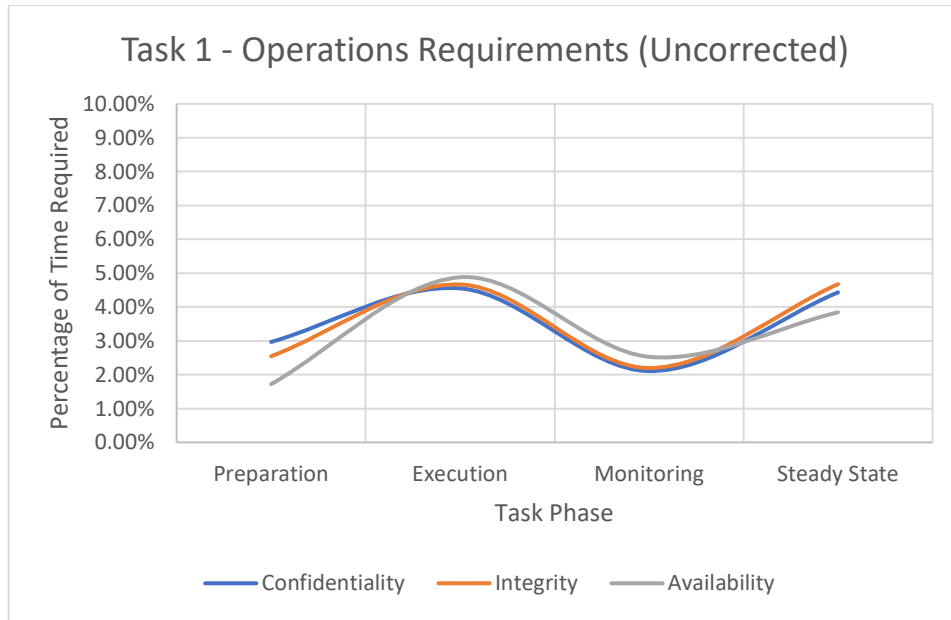


Figure 4. Operations department cybersecurity requirements for task 1 by percentage of a month's time (uncorrected).

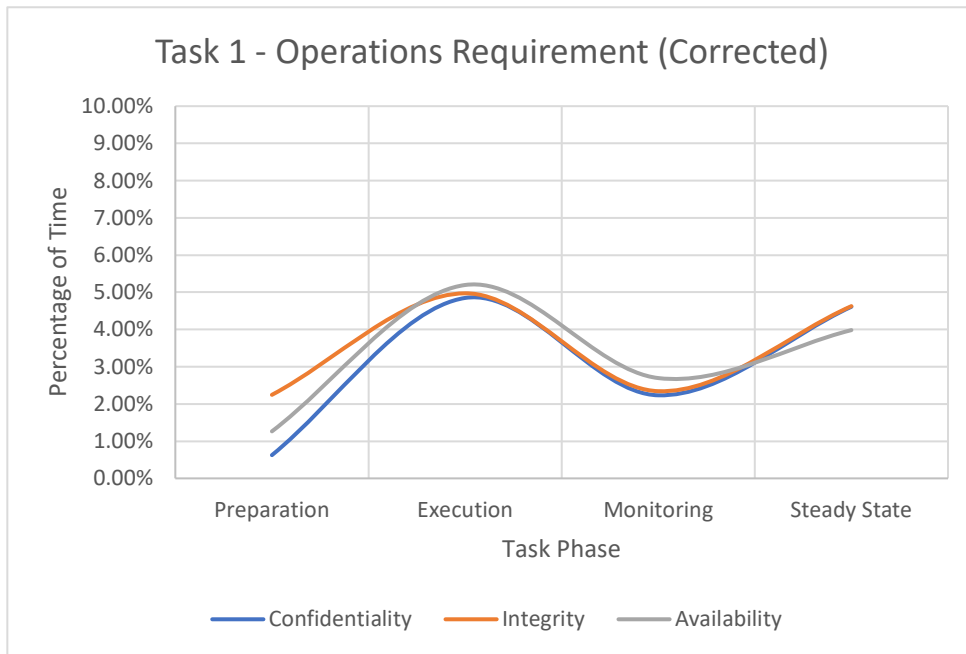


Figure 5. Operations department cybersecurity requirements by percentage of a month's time (corrected).

In the preparation phase, there is little need for confidentiality. Preparatory tasks occur primarily on-ship. Typical concerns about protecting the confidentiality of a flight plan are not a present due to very limited time windows between planning and execution. Additionally, the need for integrity is minimal, as communications with off-ship entities requires little more than basic flight and injury information. As the task moves to the execution phase, limited medical data and operational specifics must be timely and correct with a modicum of protection. The rise in requirements during steady-state does seem anomalous, but can be explained by the phenomena of leaders asking for more information than what is needed for decision making. Although it's curious that a steady-state phase requires more resources than a preparation phase, it does not require significantly more resources, and is a very low threshold to meet. It is promising to note that the data suggests that in the case of accomplishing task 1, significantly over half of information that might be available on the state of cybersecurity can be ignored without endangering task completion.

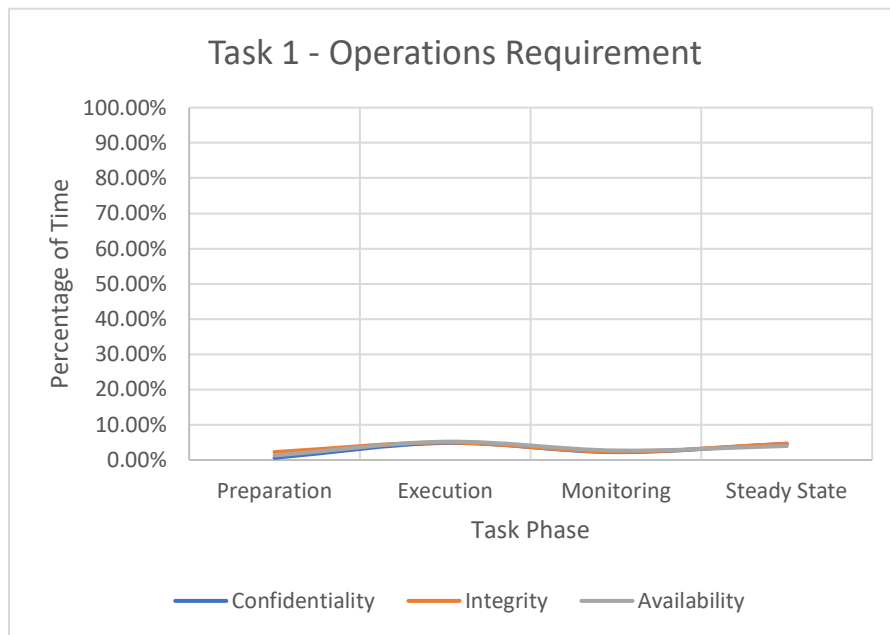


Figure 6. Task 1 operations requirements by percentage.

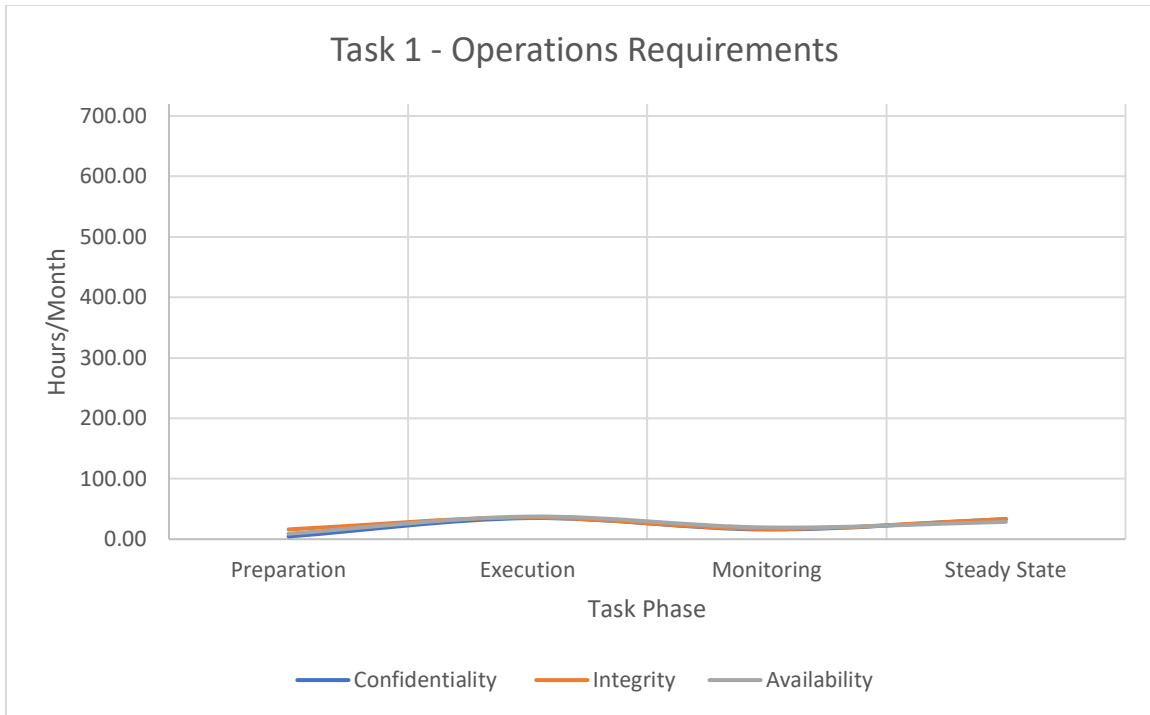


Figure 7. Task 1 operations requirements by hours/month.

2. Supply / Logistics Department

Supply and logistics departments have no direct action in a medical evacuation. Additionally, the logistics department encompasses very diverse activities from the ordering of aviation fuel to laundry services. It is not surprising to find a large standard deviation among the collected data. Even so, the calculated value for a 95% confidence interval has a z-score of 0.42 is less than half a standard deviation from the mean. As a medical evacuation is an exigent circumstance, no additional actions are conducted by the logistics department in anticipation of completion of that task. To the logistics department, the reason for the launch of an aircraft is not important; the department will simply order fuel, repair parts, and other supplies based on the number of aircraft missions. Figures 8 and 9 graph the CIA triad requirements for the logistics department to support execution of task 1 by phase.

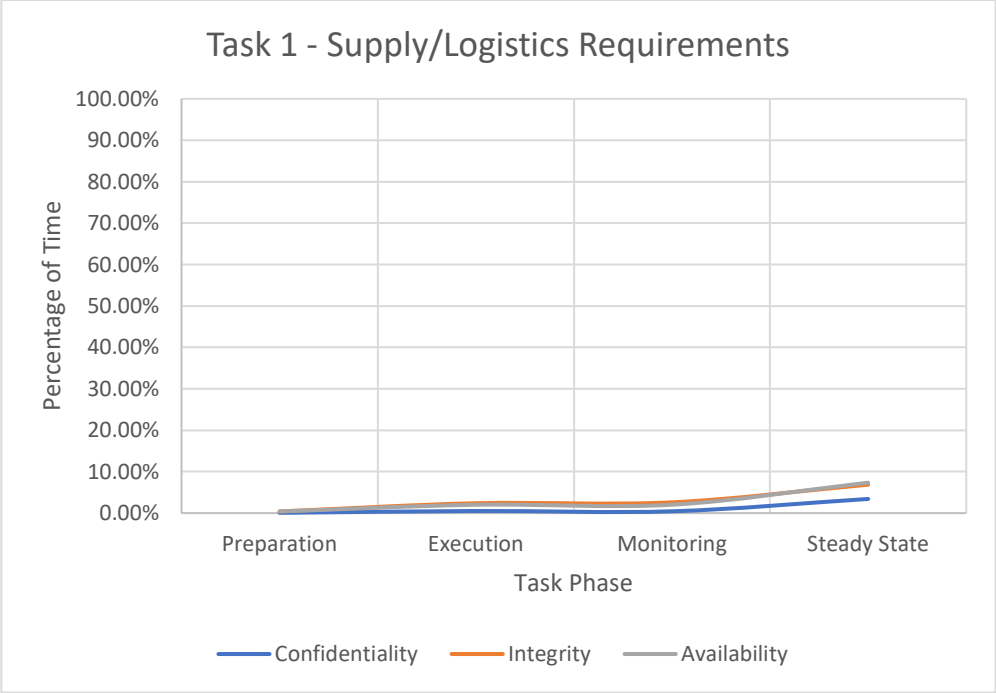


Figure 8. Task 1 supply/logistics requirements by percentage.

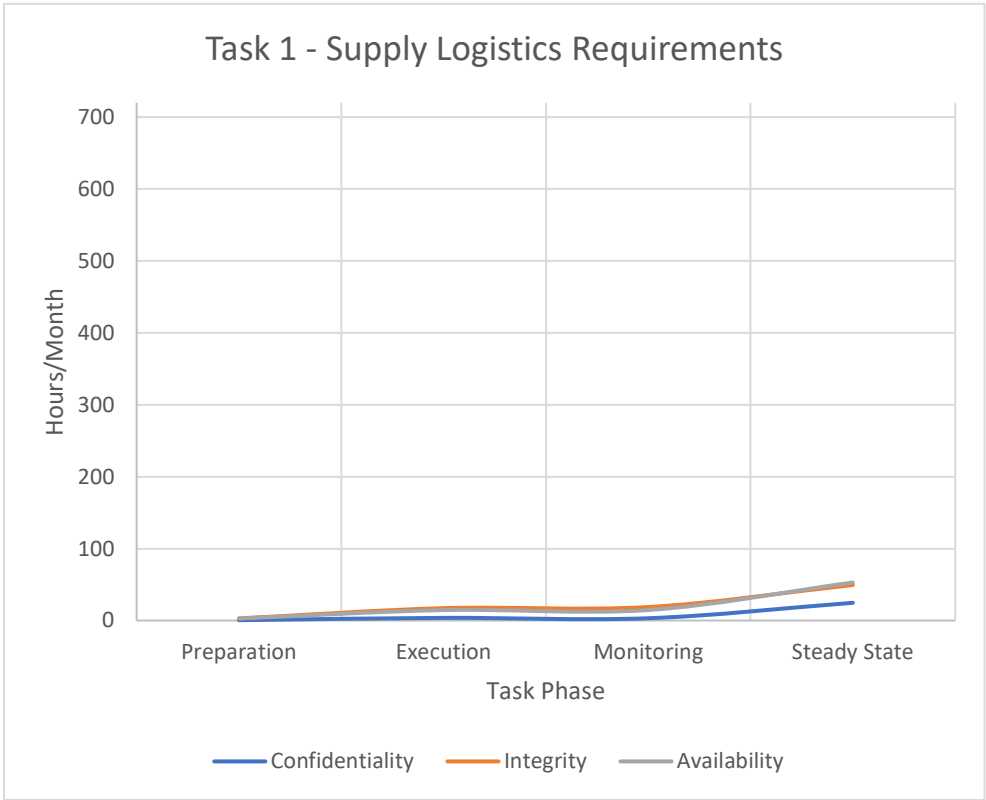


Figure 9. Task 1 supply/logistics requirements by hours/month.

3. Combined Analysis

Task one required that SMEs consider the task of transporting and/or providing for casualty and patient evacuation in a peacetime environment. Medical evacuations in a peacetime environment are exigent circumstances and are executed a-periodically. This mission is usually executed by small boats or aircraft and crew already aboard the carrier. As these resources are used for a multitude of other missions, the task presents no unique resource requirements. Furthermore, the amount of collaboration that must be done via network systems is minimal. Due to the short message length, the amount of network availability required is also minimal. Due to a lack of secret or private data, the need for confidentiality is also minimized. Any lapses in integrity on the network can easily be addressed by voice reports or simply ignored as few details transmitted would result in a critical failure of the task.

C. TASK 2: CONDUCT DAY HELICOPTER OPERATIONS

Task two required that SMEs consider the task of conducting daytime helicopter operations. This task is carried out in both wartime and peacetime for a variety of purposes. SMEs were asked to consider this task during a normal peacetime operation. Under normal peacetime conditions, this task is carried out on a recurring and roughly periodic timeline.

1. Operations Department

There are two data points within the operations department that, on the surface, seem anomalous and claim that preparation for launching daytime helicopter operations requires a completion time of sixteen days per month. These personnel include parts of the aircraft handling team and are responsible for taxiing helicopters to and from their launch position, to and from their maintenance positions, and generally moving aircraft so that other aircraft that need to transit can do so. This represents a very high requirement, but upon inspection, the data is valid. Physical space on an aircraft carrier is at a premium and constant activity with multi-million-dollar aircraft in a time and space constrained activity can lead to a lot of chaos, damage, and injury if not properly managed. As such, it is critical for aircraft handlers to be aware of their current situation during execution. A loss of availability during execution could result in a missed message announcing an aircraft

emergency and result in mission failure. However, network requirements drop off rapidly after execution.

Aircraft mission are governed by a daily order deemed the Air Tasking Order (ATO). This document pairs aircraft with missions and is classified. It is impossible to conduct aircraft operations without accessing this classified document, and this drives the confidentiality requirement. Even so, the requirement for confidentiality never reaches 45%, meaning that over half of the security information logged on systems supporting completion of this task can be ignored while still meeting the baseline requirements of the mission task.

It's useful to compare the requirements for task 3 to task 1. Whenever possible, evacuation of wounded personnel is conducted via aircraft. While it may be conducted via fixed wing or rotary wing aircraft, it's interesting to consider how difference in requirements. As the flight for an emergency isn't planned, the need to access a classified document isn't required. While the requirements for integrity and availability do increase, that increase does not appear to be a linear correlation with the number of flights nor the amount of time required. The reasons for this are not currently understood, although it is suspected that repeating tasks and re-using information leads to efficiencies. Figures 10 and 11 illustrate operations department requirements for the conduct of day helicopter operations. The data shows the maximum need is for confidentiality at maximum requirement of forty percent with a z-score of 0.37 supporting the conclusion that almost sixty percent of the available cybersecurity information can be ignored.

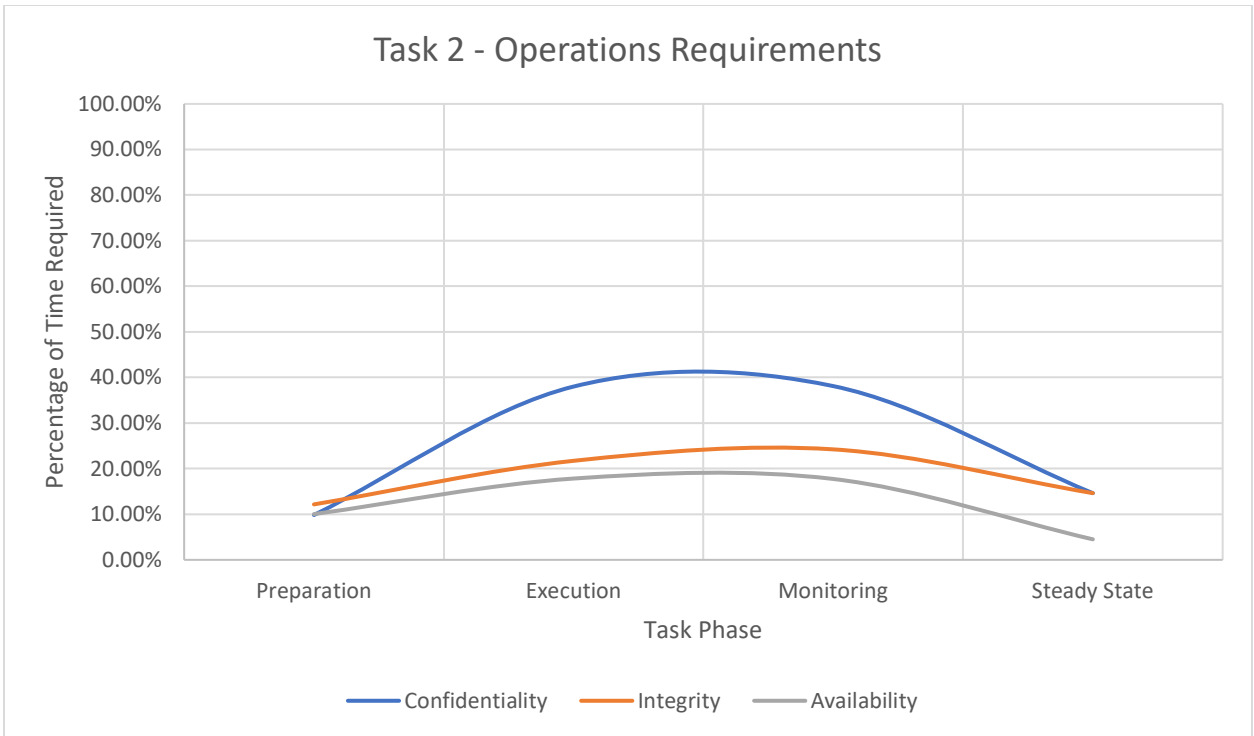


Figure 10. Task 2 operations requirements by percentage.

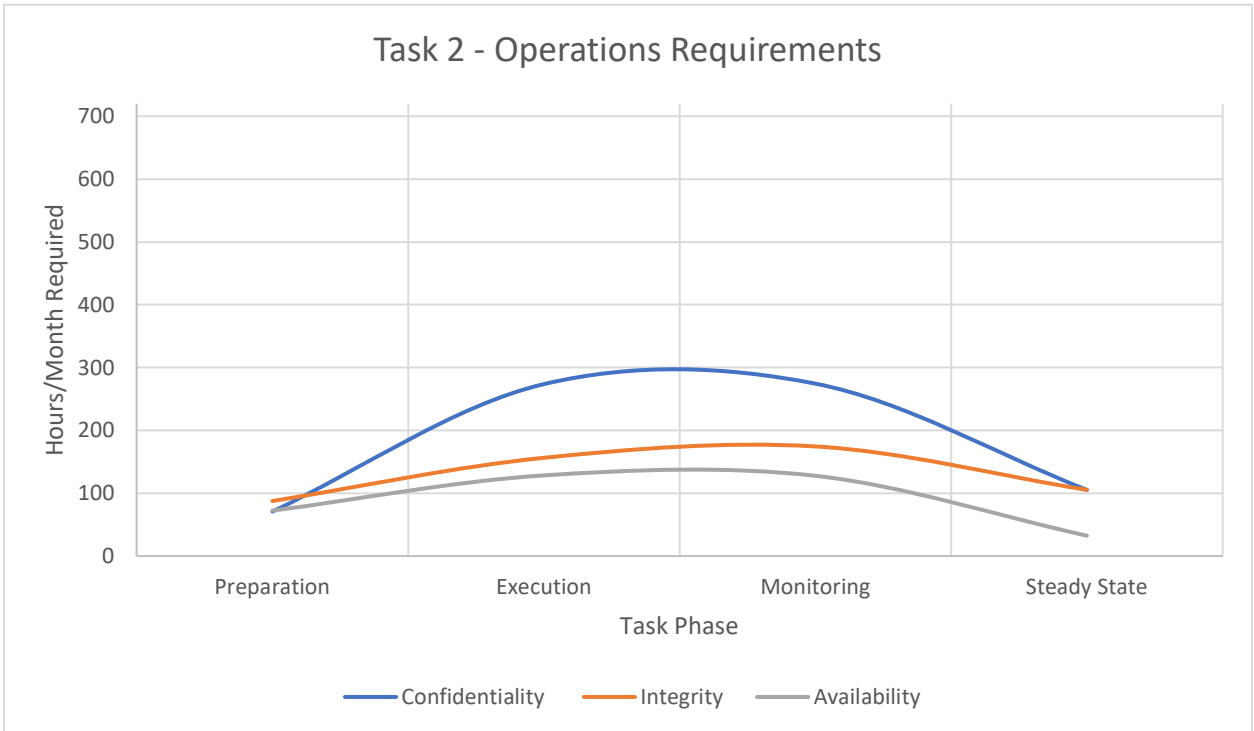


Figure 11. Task 2 operations requirements by hours/month.

2. Supply / Logistics Department

The supply and logistics department conducts a very wide range of support activities onboard. Some activities such as food and laundry service are either unaffected or only marginally affected by the mission tasks being conducted. Other supporting actions, such as ordering of spare parts, munitions, or fuel, are affected, depending on which tasks are conducted and how often. The variance in duties and their effect on this task accounts for a larger value of 0.39 than in the analysis of the operations department, but is still within acceptable norms for statistical relevance. Regardless of the task, supply must usually communicate with off-ship commercial vendors to provide the necessary supplies. This requires availability, so that orders can be made, and integrity, so that orders can be correct, but not confidentiality. The supply department must constantly monitor the state of mission tasks, as the actual execution of tasks requires them to order fuel and parts. Planned tasks may not execute and tasks that were not planned for (e.g., an equipment casualty that is not part of scheduled maintenance) may need to be executed; both will affect the need for logistics to ensure that the necessary resources are available. Figures 12 and 13 show the supply/logistics required security principles for their support to launching daytime helicopter operations.

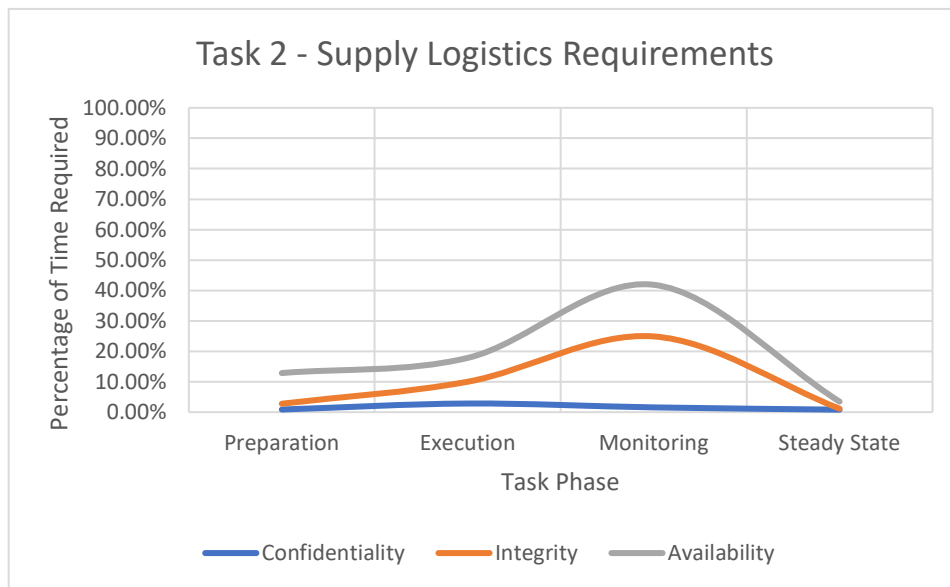


Figure 12. Task 2 supply/logistics requirements by percentage.

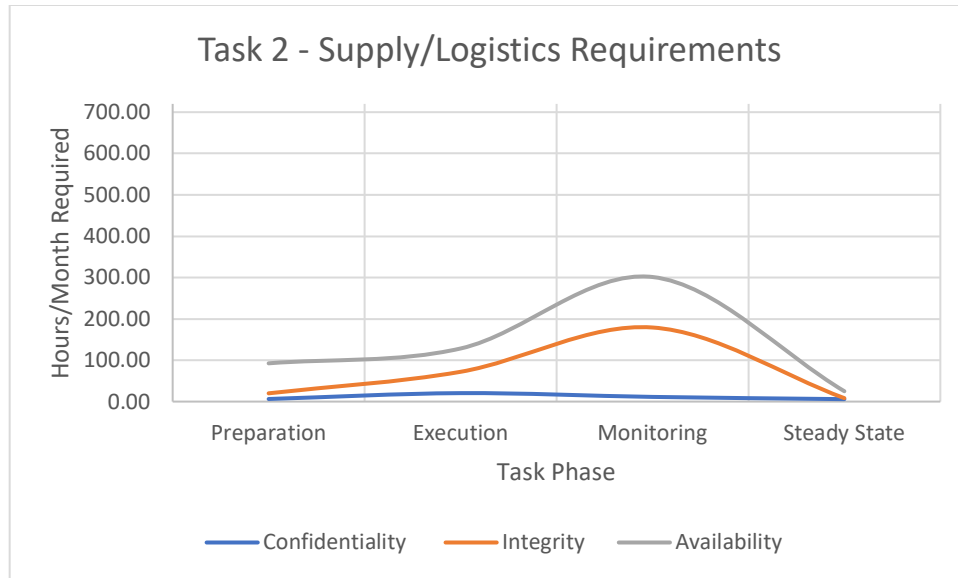


Figure 13. Task 2 supply/logistics requirements.

3. Combined Analysis

The execution of daytime helicopter missions is a complex task that occurs on a routine basis aboard an aircraft carrier. The different needs of operations and logistics becomes evident as operations requirements tend to be front-loaded on preparation and execution while supply/logistics concentrate on the monitoring phase. In addition, the nature of the tasks conducted by each department require different security principles: operations requires primarily confidentiality while logistics requires availability. Even in a complex evolution that occurs on a reasonably continuous basis, no requirement exceeds 50%. This means that at least half of the security information logs on systems supporting this mission essential task can be ignored without negatively affecting task completion.

D. TASK 3: MAINTAIN READY COMBAT AIR PATROL (CAP)

Maintaining a combat air patrol requires the coordination of a number of different types of aircraft, including fighter jets, tanker aircraft, command and control aircraft, and search and rescue aircraft, just to name a few. All of these aircraft must coordinate with each other and the ship. If there are no unexpected events during the patrol, the phase requiring the most coordination is the execution phase. Specifically, the start of the execution phase requires the most resources, as this is when a largest number of aircraft

are launched and controlled. As one CAP launches, another must prepare to land. This leads to a large number of dynamic changes, increases uncertainty and, therefore, increases in information requirements.

1. Operations Department

The maintenance of a CAP is, in many ways, similar to the task of conducting daytime helicopter operations. Aircraft must be launched, controlled, and landed. In a CAP, however, multiple aircraft must be launched and controlled simultaneously. Having multiple aircraft means that it's possible for one aircraft to report another aircraft's status if the called aircraft is unavailable. It is also expected that some efficiencies are gained as repetitive tasks are conducted in a short time using the same information. Statistical calculations give us a z-score of 0.29 suggesting that the actual value is less than one-third a standard deviation from the calculated value and statistical significance. A point for which an explanation could not be discerned is the 5% reduction for confidentiality for launching a CAP over a helicopter for daytime operations. Standard operating procedures for both CAP and helicopters fall under the standards of Naval Air Systems Command and no difference in operating requirements could be found in documentation. It is suspected that more data would reduce this variance. Figures 14 and 15 show operations requirements for maintenance of a ready CAP.

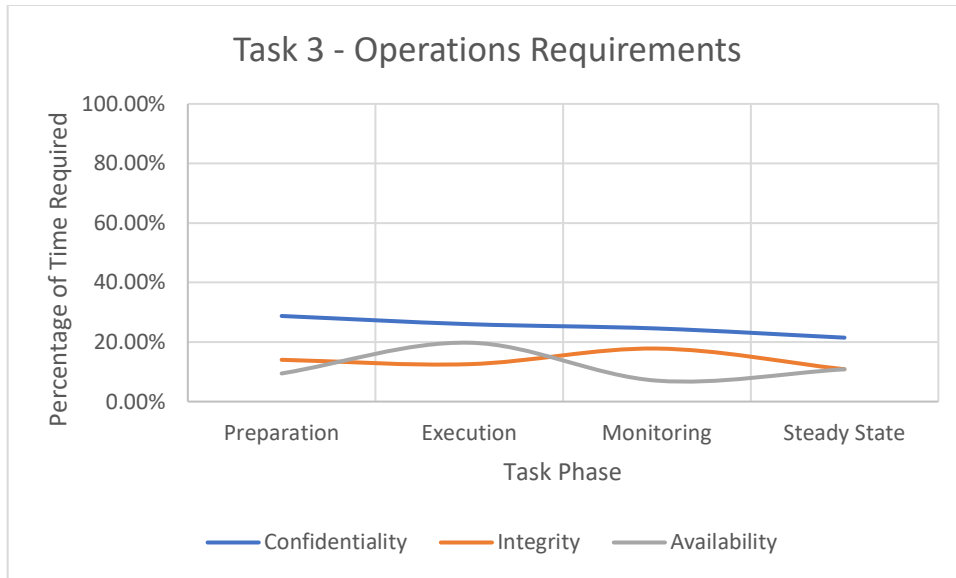


Figure 14. Task 3 operations requirements by percentage.

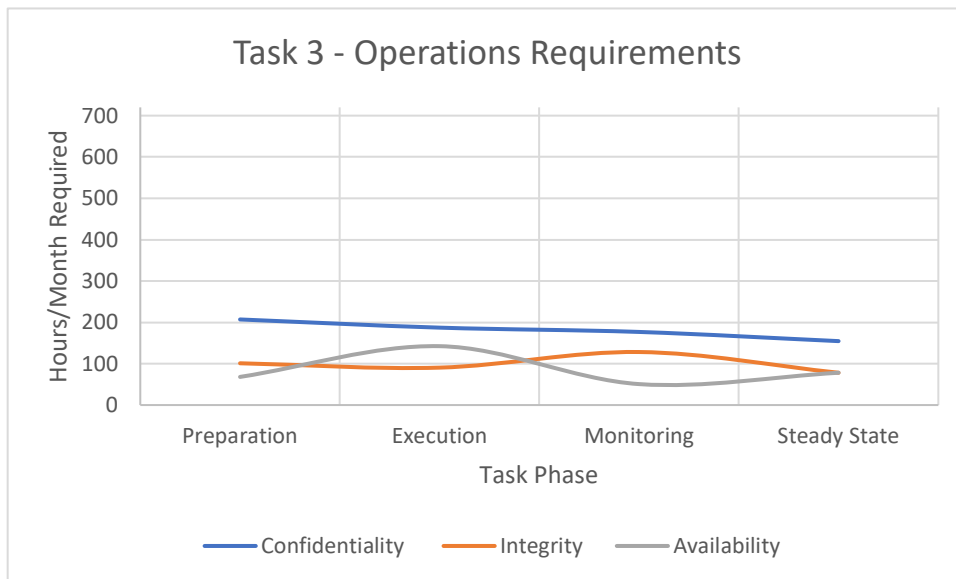


Figure 15. Task 3 operations requirements by hours/month.

2. Supply / Logistics Department

The requirements for maintenance of a ready CAP by the supply/logistics department closely mirror their requirements for helicopter flight operations. As previously stated, the tasks accomplished by the logistics department will vary by the mission task they are supporting and how often it is conducted, but not by the size of the task. While a

ready CAP launches more aircraft and therefore burns more fuel and more aircraft will require more repair parts, this simply requires that the logistics department order more fuel and more parts, but does not necessitate making more orders. Additionally, services provided by supply/logistics such as food service and laundry do not change based on the number of aircraft launched. This consistency in requirements is supported by similar requirements and a z-score of 0.39, very similar to that of task 1. Figures 16 and 17 illustrate the logistics requirements for the networks supporting maintenance of a ready CAP and are very similar to Figures 12 and 13, which illustrate logistic requirements for helicopter day operations.

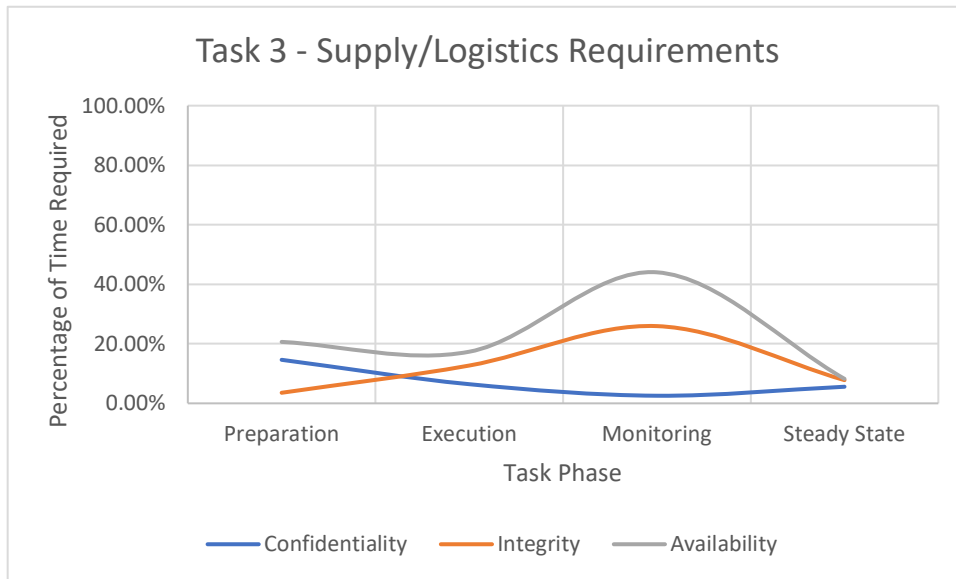


Figure 16. Task 3 supply/logistics requirements by percentage.

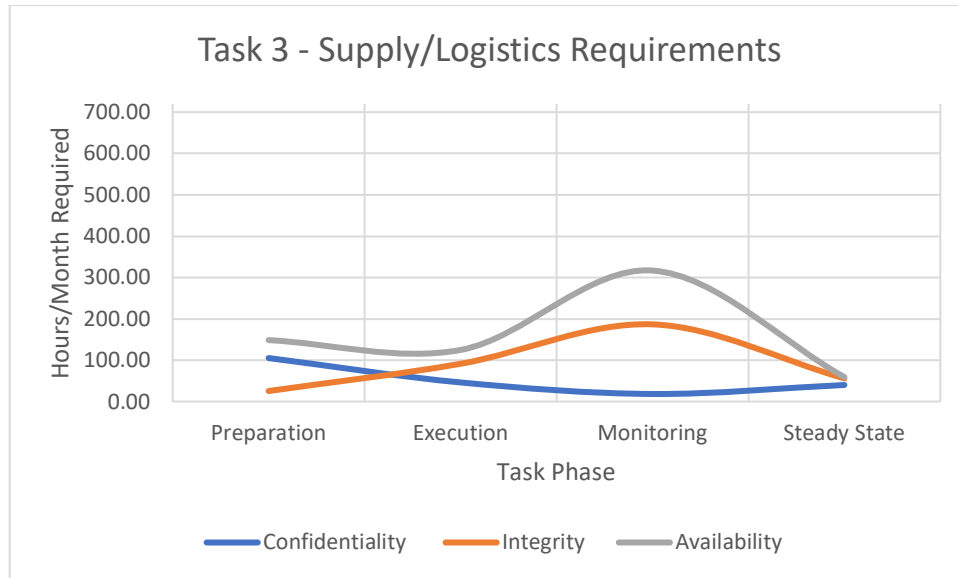


Figure 17. Task 3 supply/logistics requirements by hours/month.

3. Combined Analysis

When it comes to supporting the maintenance of a ready CAP, we’re able to discern that the operations department has more front-loaded requirements and primarily requires confidentiality. In support of the same, the supply/logistics department is more back-loaded and primarily requires availability. Once again, no requirement breaks the 50% threshold.

By combining the results of tasks one, two, and three some patterns begin to emerge. There is evidence in the first three tasks to reject the null hypothesis. The cybersecurity requirements of a mission essential task seem to be driven by the nature of the task and varies based upon the phase of execution as well as the entity conducting the action. This is sufficient to reject the null hypothesis and suggest the emergence of this pattern for at least peacetime tasks.

E. TASK 4: DETECT, LOCALIZE, AND TRACK SUBSURFACE CONTACTS WITH ACTIVE/PASSIVE SONOBUOYS

Task four examines SME requirements for detecting, localizing, and tracking subsurface contacts with active/passive sonobuoys. Sonobuoys are remote sensors that are dropped from aircraft into the water to detect submarines. Passive sonobuoys consist of one or more hydrophones, and active buoys make use of an active sonar. Both active and

passive sonobuoys are wireless and use radio frequencies to transmit their status. This task is a wartime active which is conducted in peacetime only for the purposes of training and readiness. SMEs were asked to consider this task during a wartime operation. Under normal peacetime conditions, this task is carried out on a recurring and roughly periodic timeline.

1. Operations Department

Once sonobuoys are deployed, requirements are relatively static. Submarine hunting is, at best, an art, and even under the best of circumstances, contact is intermittent. The need for confidentiality is driven by the need to communicate any submarine contacts to friendly forces. Sonobuoys are employed in groups; it is never the case that a single sonobuoy is deployed. As such, intermittent availability to any sonobuoys is not problematic. Figures 18 and 19 show operations department requirements for task 4. Despite the perceived importance of conducting a wartime task, cybersecurity requirements peak at under thirty percent and a z-score of 0.32 supports the calculated values of this research.

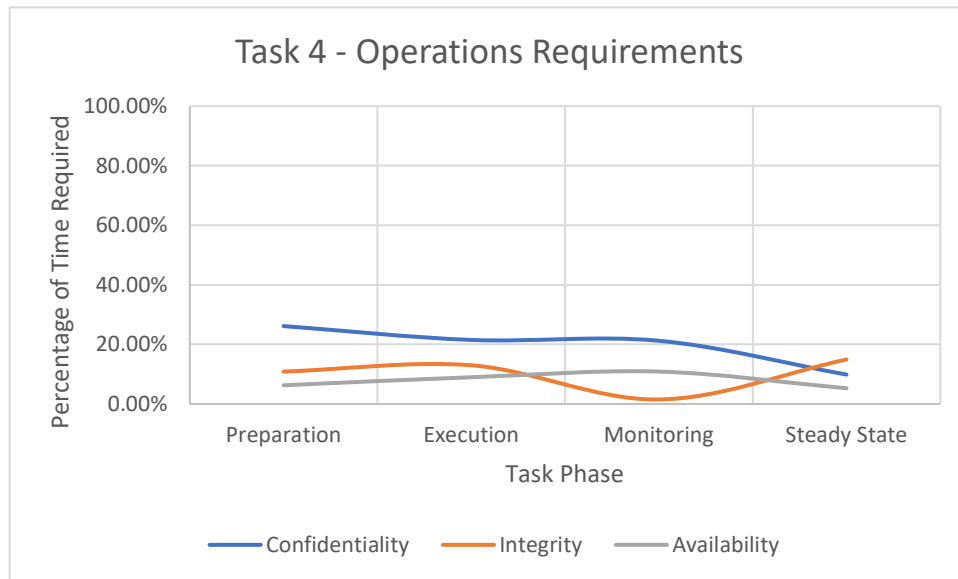


Figure 18. Task 4 operations requirements by percentage of time.

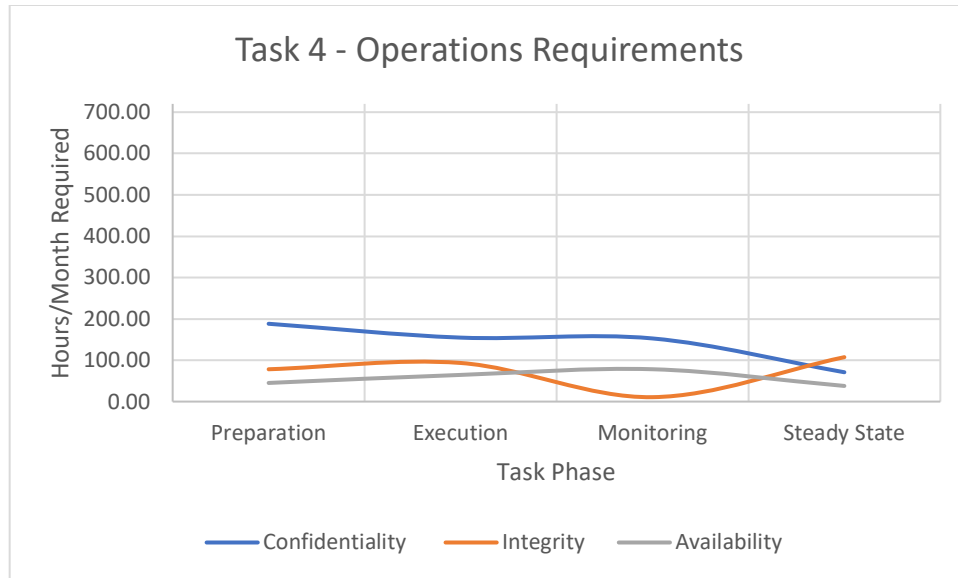


Figure 19. Task 4 operations requirements by hours/month.

2. Supply / Logistics Department

As in the previous tasks, supply/logistics department needs primarily concentrate on the need to re-order expended supplies. The high variance in responses from the supply/logistics department can be explained by the breadth of activities in the department. Once again, it is understandable that food and laundry services would have no additional needs to support the successful completion of this task. Expended ordinance and sonobuoys need to be ordered via the use of classified systems increasing the need for confidentiality; however, integrity and availability remain relatively the same as the previously examined tasks. Figures 20 and 21 show supply/logistics department requirements for task 4. The z-score is 0.42, similar to other tasks for supply/logistics department and supporting this analysis.

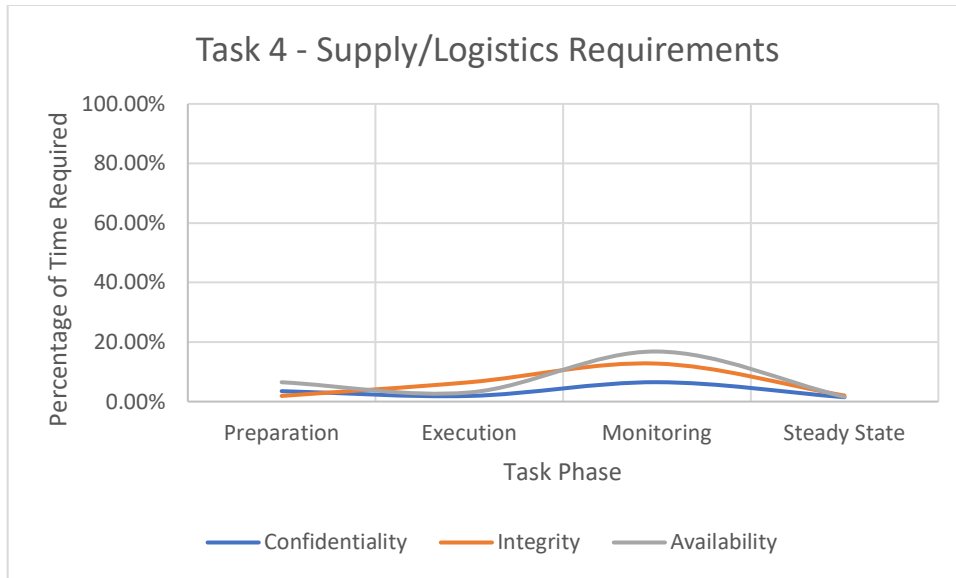


Figure 20. Task 4 supply/logistics requirements by percentage of time.

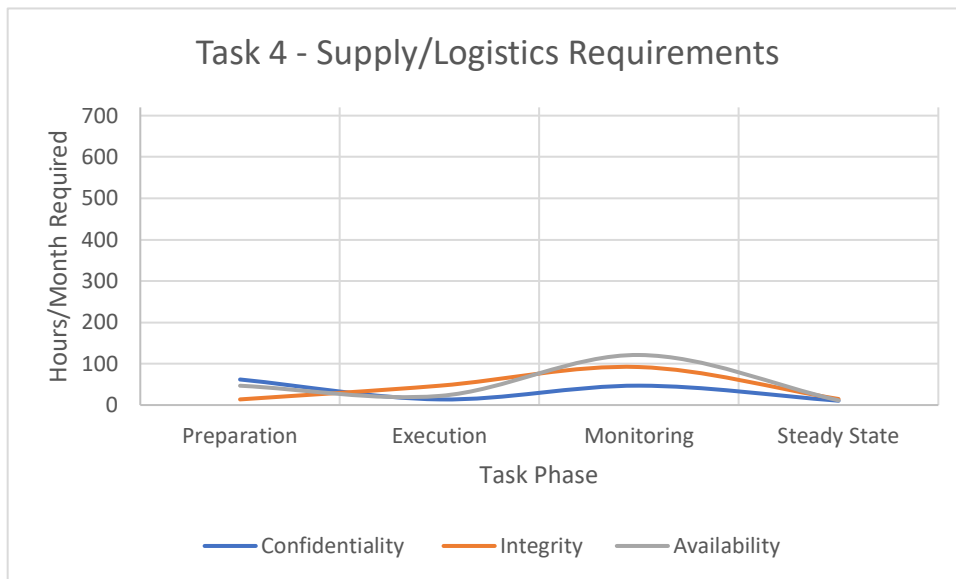


Figure 21. Task 4 supply requirements by hours/month.

3. Combined Analysis

Task 4 is the first task examined that is considered primarily a wartime activity. Failure to successfully complete a wartime mission essential task can, without a doubt, have catastrophic results. The failure to adequately find and track an enemy submarine contact could result in the loss the aircraft carrier and the thousands of lives aboard. Even

with such dire consequences, the cybersecurity requirements are limited to a maximum of 20% of the information available. This again support rejection of the null hypothesis. In all four of the previously examined tasks, the cybersecurity information requirements are far less than what is available.

F. TASK 5: PLAN / DIRECT ATTACK OF SUBMARINES

Task five asked the SME to consider the wartime action of planning and directing an attack on submarines. This task is the second wartime task examined and the first which requires the employment of lethal force. Once a decision is made to attack, the window of execution for this task is comparatively short. If not conducted correctly, weapon systems may malfunction or destroy the wrong target. The situations in which this task is completed are high stress, full of relative uncertainty, and of high consequence.

1. Operations Department

Figures 22 and 23 illustrate the requirements of the operations department to complete task 5. To complete this task, an aircraft carrier will either employ its own weapon system or direct another asset to employ a weapon system. The launch of a weapon becomes apparent instantly and the need to provide confidentiality after weapon system deployment is not present. The low rate of availability and integrity is surprising. In a high stress, high consequence environment, it would be expected that availability would approach 100% so that a weapon system would be available the instant it's needed. Likewise, a loss of integrity could result in improper employment of the weapon system and either missing a threat, or possibly striking a friendly unit. It is possible that since there are multiple redundant weapon and communications systems available operators felt comfortable with low figures, and, with a z-score of 0.32, these values are well supported.

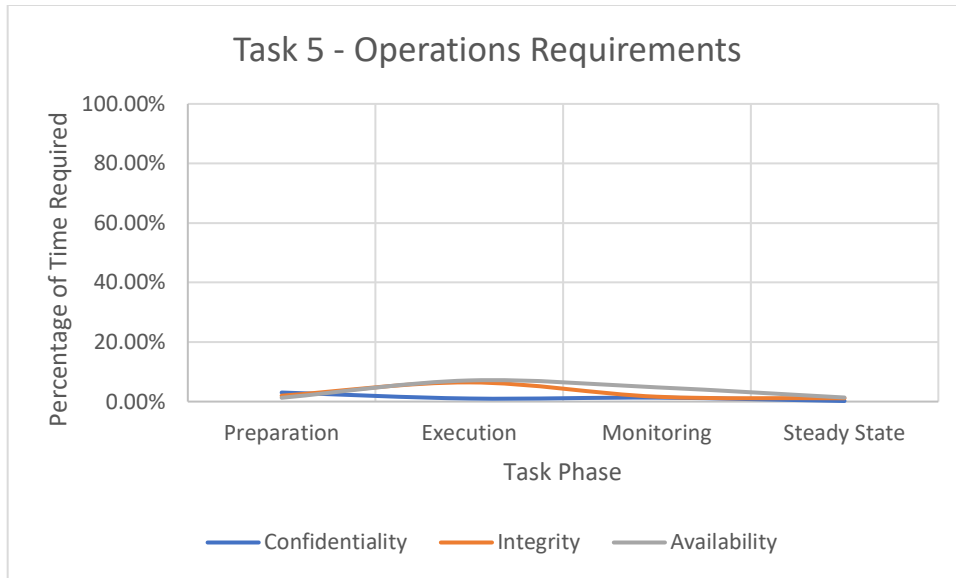


Figure 22. Task 5 supply requirements by percentage.

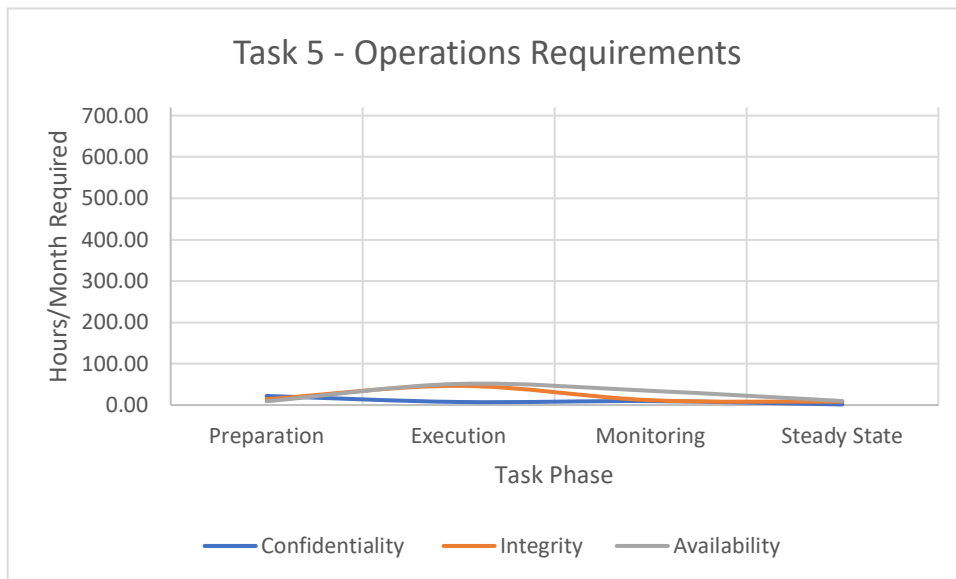


Figure 23. Task 5 operations requirements by hours/month.

2. Supply / Logistics Department

As in previous tasks, the supply/logistics department's primary efforts are during the monitoring phase. Figures 24 and 25 show that availability is the primary concern, and is roughly the same as the requirement for maintaining a ready CAP. The requirements for supply is again shown to be relatively regardless of which mission essential task is being

supported. A maximum need of well below 30% for availability. A z-score of 0.39 supports these values and is consistent with other values calculated for the supply/logistics department.

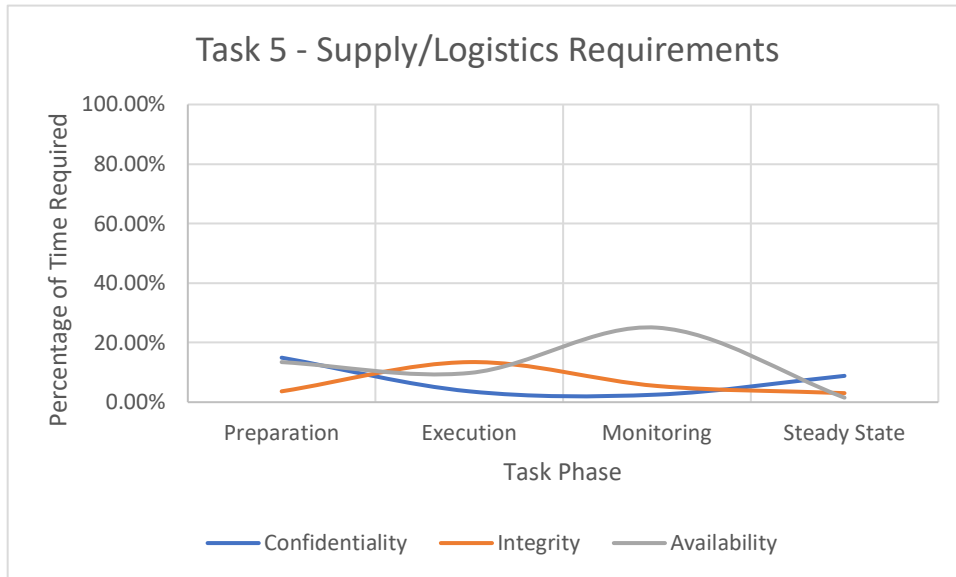


Figure 24. Task 5 supply/logistics requirement by percentage of time.

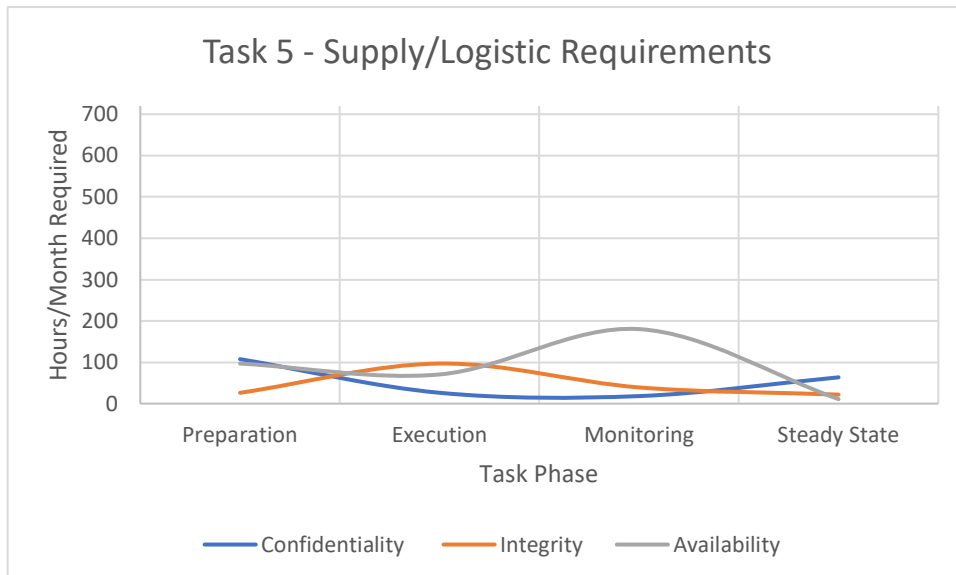


Figure 25. Task 5 supply/logistics requirement by hours/month.

3. Combined Analysis

Directing an attack is an action that is not taken lightly as the consequences are lethal and errors catastrophic. Even in the case of this mission essential task, the security requirements are rather paltry. Once again, more than half of the cybersecurity information can be ignored and the task successfully completed. In all five of the examined tasks, cybersecurity requirements have remained well below the 50% threshold. Once again, H_0 can be rejected.

G. TASK 6: EMERGENCY REPAIRS TO EQUIPMENT CRITICAL TO SHIP'S MISSION

Task 6 required SMEs to consider emergency repair to equipment critical to ship's mission and is equally likely to occur in wartime or peacetime. While an aircraft carrier carries a large amount of repair parts carrying every feasible part is simply not possible. Additionally, many parts require specific certifications or tolerances that must be verified immediately before installation. As suggested by the name, emergency repairs are unplanned maintenance. When accomplishing this task, ships require parts and/or expertise to be delivered. These requests for assistance are governed by a Casualty Report (CASREP) whose status briefed at least daily to the Chief of Naval Operations. Equipment that is critical to the ship's mission severely limit its ability to perform mission essential tasks and are of primary concern to national command authority.

1. Operations Department

As in previous tasks, Figures 26 and 27 illustrate that the operations department's primary effort is during execution. In the case of repairs, understanding the equipment casualty and its effects is critical to ensuring a successful repair. Additionally, constant status updates and ensuring the integrity of all tool readings and system logs is critical to understand what happened, why, and if a repair has been successfully implemented. Unsurprisingly, integrity and availability are more highly desired than confidentiality.

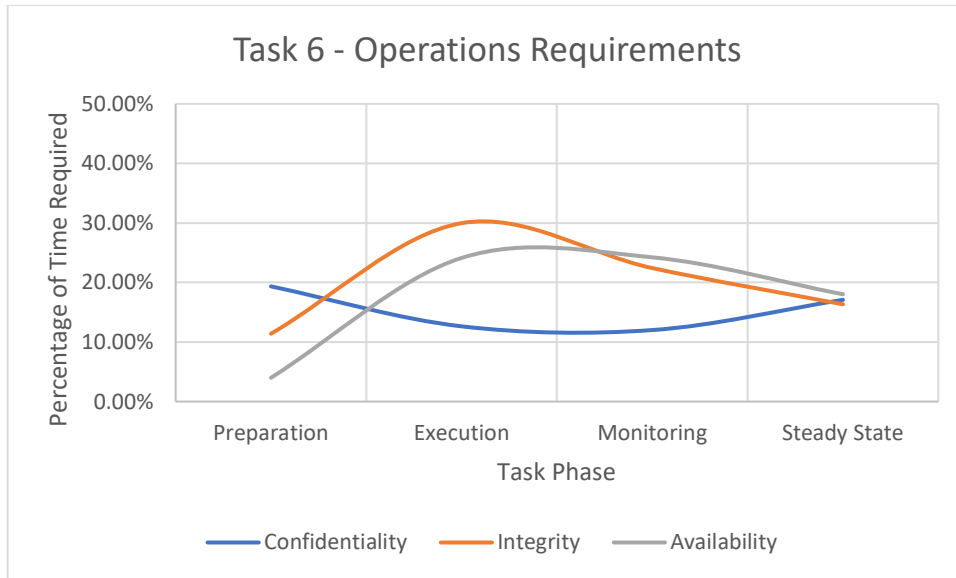


Figure 26. Task 6 operations requirement by percentage of time.

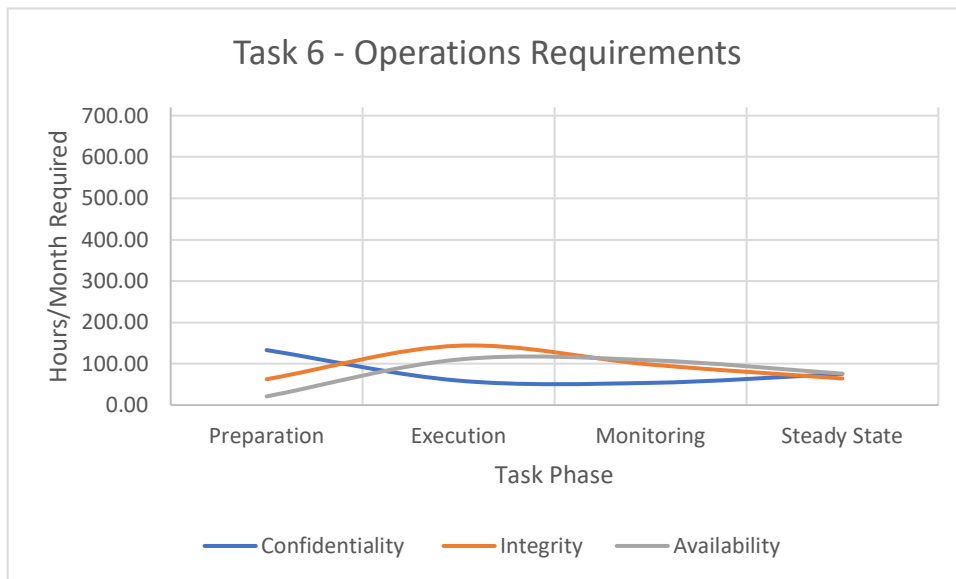


Figure 27. Task 6 supply/logistics requirement by hours/month.

2. Supply / Logistics Department

Figures 28 and 29 demonstrate that the supply and logistics department have a more critical role in enabling the completion of this task. Emergent orders for repair parts and method of delivery need to be planned and executed. In many cases, additional expertise may be needed to support the onboard crew. The need for the network to be available is

not surprising. Although CASREPs are classified documents, transmission of these reports is usually surrounded by a series of phone calls. By the time a CASREP is transmitted, it's common for all parties involved to already be aware of the contents of the message.

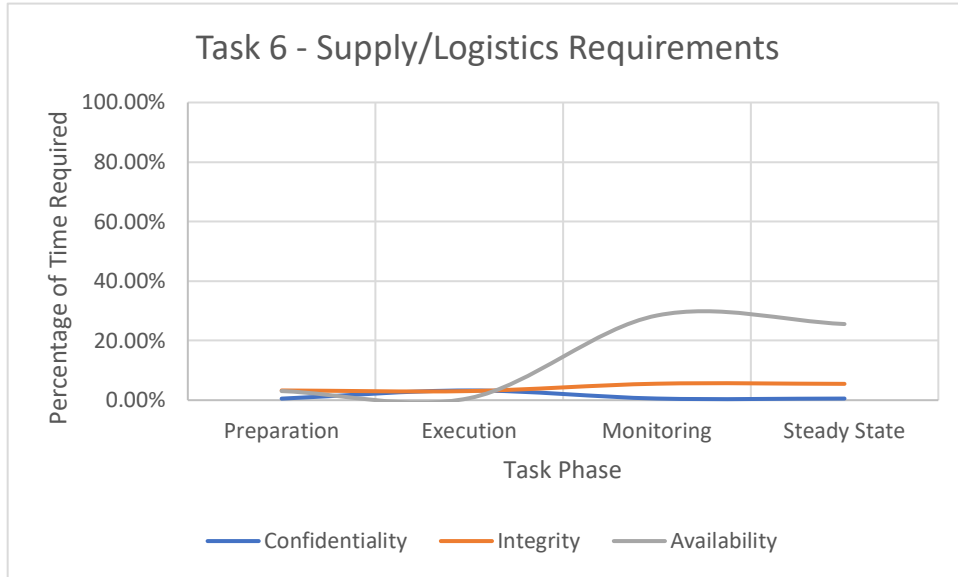


Figure 28. Task 6 supply/logistics requirements by percentage of time.

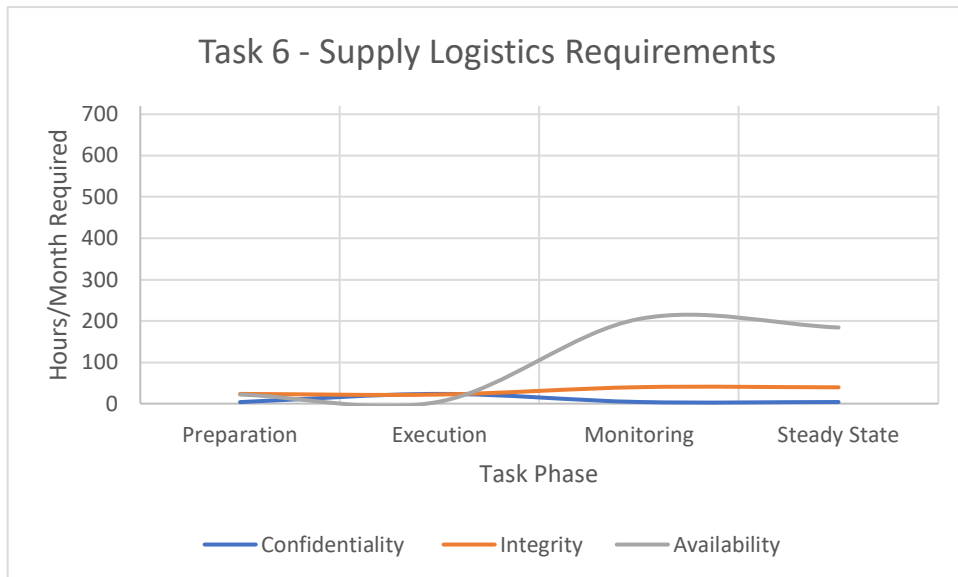


Figure 29. Task 6 supply/logistics requirements by hours/month.

3. Combined Analysis

While other tasks examined have been primarily peacetime or primarily wartime tasks, this is the first task to be equally executed in either case. The need for emergency repairs means that other mission essential tasks are unable to be completed and requires outside resources to correct. Operations department requirements are front-loaded while supply/logistics department requirements are back-loaded. In the case of this task, availability is the primary requirement for both operations and supply. This is due to the need to coordinate with outside entities. The cybersecurity needs vary dependent the department and phase of execution.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. RESEARCH CONTRIBUTIONS TO THEORY AND PRACTICE

This research has provided a framework that suggests that it may be possible to reduce cognitive loading on analysts by changing the priority of their tasking in response to changing operational context. This has the effect of creating slack resources as suggested by Galbraith (1973), improving analysts' performance, and enhancing cybersecurity. The focus on operational contexts allows for better understanding of the requirements of mission essential tasks. This increase in understanding allows for the creation of better, more relevant, standardized processes which would reduce Galbraith style exception and allow supervisory personnel to make better and more timely decisions.

This research has given a method for measuring cybersecurity requirements based on operational context. Through understanding minimum cybersecurity requirements for mission essential tasks, leaders may gain a better understanding of their information processing capacity as compared to their information processing load. That knowledge can be used to prioritize task execution and schedule tasks in a way that reduces information processing load, improves cybersecurity productivity, and improves efficiency. Additionally, this knowledge provides a quantitative measure of how cybersecurity personnel are employed with respect to mission requirements. This allows for quantitative discussion, and perhaps improved management of, information processing resource slack or shortfalls, unacceptable risk shortfalls, or perhaps a quantitative measure allowing for precise understanding of acceptable risk resource requirements.

The framework proposed in this model extends the work of Galbraith and organizational theory into the field of cybersecurity. Through the consideration of operational relevance at an instant in time, the framework also links cybersecurity back to operational art and the execution of cybersecurity within the context of the larger organization. Through mapping of cybersecurity through an operational lens, workload may be reduced, efficiency may be improved, and both cybersecurity and operational tasks may be more successfully completed.

THIS PAGE INTENTIONALLY LEFT BLANK

VIII. CONCLUSIONS AND FUTURE WORK

A. CONCLUSIONS

This research effort started with the assertions that cybersecurity personnel operate in a state of consistent information overload and that the implementation of automated filtering techniques is insufficient to address the condition. This effort set out to test the hypothesis that a new cybersecurity risk framework could be designed to significantly reduce information overload without negatively affecting cybersecurity posture. The outcome is a highly effective framework that allows for a better understanding of information needs, quantifiable cybersecurity risk, and more effective human capital implementation by considering a task in execution as a set of requirements over time instead considering that task as an atomic unit. The data collected in this research strongly supports that information gathered in support of completion of mission essential tasks can be reduced by significant quantities without endangering the completion of those tasks or increasing cybersecurity risk.

Reducing the quantity of information that must be analyzed by the cybersecurity workforce can be accomplished in numerous ways if the purpose of cybersecurity is to support the completion of mission essential tasks. One tactic that may be employed is to collect only that information which is required to mitigate unacceptable risk in the completion of tasks. A slightly different implementation would continue to collect as much information as possible, but only ask human operators to evaluate the information required to assure completion of mission essential tasks. An advantage to having other information available is that additional information might provide insight into the root cause of an attack endangering the completion of mission essential tasks. In fact, it could be argued, that once an attack is detected, information which may provide insight into the attack is relevant from both a cybersecurity and operational context.

While the data gathered supports a minimum reduction of fifty percent of the information that could be gathered, it is important to recognize that this data supports the minimum requirements. From an operational resiliency perspective, mission directors are highly encouraged to decide if mitigating unacceptable risk is sufficient to provide

acceptable mission risk. This framework can be used by mission and SOC directors to account for resources with respect to mission critical tasks. In the case where resources are sufficient to meet requirements for acceptable risk, a good accounting of surge capacity is possible. In the case where resources are insufficient to meet acceptable risk, more informed discussions may be had with quantitative data to support adjustment in either resources or determinations of acceptable risk.

B. GENERALIZABILITY

The applicability of this research extends to all military units and beyond. While military units have already conducted a mission-based analysis and have well-documented mission essential tasks and tolerances, any government or commercial entity can, and should, do the same. Once mission essential tasks have been documented, corporations and other entities could use this framework to reduce information overload within their own cybersecurity workforces. As in this study, having a greater understanding of mission-essential sub-tasks would allow for greater insight. Additionally, this study and implementation of this framework could help inform future law and regulations dealing with protection of sensitive material. Laws and regulations such as the Privacy Act of 1974, General Data Protection Regulation (GDPR), and Health Industry Portability and Accountability Act (HIPAA), could be adjusted for an optimum balance of protection given mission requirements and available cybersecurity resources. Finally, this framework can be used to help determine if organizations are adequately staffed to defend mission critical tasks. After applying this framework, simple mathematics will allow for a rapid determination of appropriate staffing.

C. RESEARCH LIMITATIONS

The principal limitation of this research is the construction of the measurement instrument. Since SME elicitation was limited to one visit per location, there was limited opportunity to validate the survey construction. The inability to validate the measurement instrument led an issue in that it did not account for the wide disparity of functions conducted by the supply/logistics department. This led to a higher variance in responses than was anticipated. An additional issue was the small population available to elicit for

expertise. While findings from nuclear powered aircraft carriers are undoubtedly generalizable to all U.S. Navy units, there are only eleven carriers. Finally, no documentation exists that links mission essential tasks to sub-tasks or supporting tasks. It's possible that further research will find areas that have sub-tasks or supporting tasks with higher requirements than those gathered in this research.

D. FUTURE WORK

Several areas of further research are recommended. The first is to conduct a similar study after conducting a full mission essential task deconstruction. Second, a mission systems analysis needs to be conducted from both the mission and network perspectives. Finally, research is required for network traffic characterization and network automation.

1. Task Deconstruction and Integration Analysis

Further research is needed to understand the sub-tasks required to accomplish a mission essential task. Those subtasks are accomplished by additional SMEs, may require the use of additional information systems, and may have differing cybersecurity requirements. It is possible that by further understanding subtasks and their dependencies, additional efficiencies may be gained. It is feasible that assuring the existence of cybersecurity principles in a subtask will allow for assurances in follow-on tasks via a transitive property.

2. Mission System Analysis

Further research is needed to better understand the link between mission essential tasks and the required information systems. Additionally, an understanding of information flow on the network is required to better understand the most efficient points of observation for required security principles. For example, it may be more efficient to collect security logs at network choke points (e.g., segment routers) than at hosts. On the other hand, if a router services many non-mission-essential devices, it may be more efficient to monitor specific end-point devices. Additionally, mapping all mission essential tasks to the network may allow for an emergence of characteristics, that would allow for further efficiencies in information overload reduction and/or the discovery of additional cybersecurity

requirements that are not obvious while conducting any one task, but instead apparent only when conducting a unique combination of tasks.

3. Graph Mapping and Reduction

Mapping tasks and dependencies, information flow, and network topology allows for the creation directed and undirected graphs. The examination of the graphs at each of these layers may allow for graph reduction leading to additional efficiencies. It is more likely, however, that by mapping graphs at these different levels to each other efficiencies may emerge that are not obvious when looking at only one of these levels. These efficiencies may result in either a further reduction in information processing load, or it may lead to reduced utilization of information processing capacity.

4. Framework Automation

Once subtasks and requirements are understood and a mission system analysis is complete, mission essential tasks can be modeled by heuristics. Further research would allow for some automated detection and identification of mission critical tasks. This automatic identification could be implemented into an AI model that allows for automatic context switching in dashboards used by cybersecurity personnel to highlight the most relevant information, and result in a more dynamic and context-sensitive monitoring tool. The existence of such a context-sensitive tool would provide various settings based upon operating environment and mission realities, more rapid identification of tasks actively executed, and expedite identification of cybersecurity shortfalls in the execution of those tasks. To be clear, it is not suggested that less information is collected on the network, but rather, that only the most operationally relevant information be presented SOC personnel. In a situation where additional disambiguation is required, analysts can choose to recall information collected in logs, but not necessarily displayed on the dashboard. While efficiencies may be gained, the limitations imposed by using Turing machines are ever present.

APPENDIX A. MEASUREMENT INSTRUMENT

Participant Demographic Information

What is your age?

How long have you been in the military?

What is your rank?

What is your current position?

How long have you held this position?

What is your highest civilian education completed?

How long have you served aboard a carrier, strike group staff, or carrier staff?

You are part of the operations (N3) or logistics (N4) department aboard a U.S. aircraft carrier. OPNAV [C3501.65F](#) denotes required operational capabilities for this platform.

For each task, four phases will be considered: preparation phase, execution phase, monitor phase, and steady-state phase. **Preparation phase** includes all preparations and subtasks that must be accomplished prior to execution of the actual tasks. **Execution phase** includes actual performance of the task. **Monitor phase** is the phase after which active tasks have been conducted when monitoring may be required to ensure the desired end-state. **Steady-state phase** is the period of time not covered by the prior three phases.

As an example, consider the task of feeding your children lunch. The preparation phase may include going to the store and purchasing bread, peanut butter, and jelly. The execution phase might include making the peanut butter and jelly sandwiches, getting your kids to the table, and serving them the sandwiches. The monitoring phase would include the time period between them being served the sandwiches and them actually eating the sandwich. The steady-state phase would be any other time not covered by the previous three phases.

For each task, denote how much time **your department** spends supporting its completion in each phase over a thirty-day period. Please note that this can be indirect support (e.g., ordering to support maintenance of aircraft supports a task of maintaining combat air patrol).

For each task consider how critical confidentiality, integrity, and availability are to the successful completion of each phase of each task **for your department**. **Confidentiality** is that principal the requires that only the initiator and authorized recipient be privy to the contents of a message. **Integrity** is that principal that only authorized personnel be able to alter the contents of a message that the message received is the message that was transmitted. **Availability** is that principal that governs that authorized users can access information.

When considering the requirement for each security principle, allot only for the time required to complete the necessary actions. Consider the aforementioned example of feeding your children lunch, it might only take you 30 minutes to buy the necessary components at the grocery store. In this case, the availability required of the store is 30 minutes a trip. Assuming that PB&J supply run last 15 days, you will need to make two trips a month for a total of 1 of availability a month.

Task: Transport and/or provide for casualty/patient evacuation.

How long is spent supporting the accomplishment of this task in each phase in a 30-day period during which this task is accomplished?

Preparation phase: _____ Days _____ Hours _____ Minutes

Execution phase: _____ Days _____ Hours _____ Minutes

Monitoring phase: _____ Days _____ Hours _____ Minutes

Steady-state phase: _____ Days _____ Hours _____ Minutes

For each phase of the assigned task, consider what percentage of time listed above requires each principle of confidentiality, integrity, or availability. It is possible that each principle will be required 100% at each phase.

Preparation Phase:

Percentage of time *Confidentiality* is required: _____

Percentage of time *Integrity* is required: _____

Percentage of time *Availability* is required: _____

Execution Phase:

Percentage of time *Confidentiality* is required: _____

Percentage of time *Integrity* is required: _____

Percentage of time *Availability* is required: _____

Monitor Phase:

Percentage of time *Confidentiality* is required: _____

Percentage of time *Integrity* is required: _____

Percentage of time *Availability* is required: _____

Steady-state Phase:

Percentage of time *Confidentiality* is required: _____

Percentage of time *Integrity* is required: _____

Percentage of time *Availability* is required: _____

Task: Conduct day helicopter operations.

How long is spent supporting the accomplishment of this task in each phase in a 30-day period during which this task is accomplished?

Preparation phase: _____ Days _____ Hours _____ Minutes

Execution phase: _____ Days _____ Hours _____ Minutes

Monitoring phase: _____ Days _____ Hours _____ Minutes

Steady-state phase: _____ Days _____ Hours _____ Minutes

For each phase of the assigned task, consider what percentage of time listed above requires each principle of confidentiality, integrity, or availability. It is possible that each principle will be required 100% at each phase.

Preparation Phase:

Percentage of time *Confidentiality* is required: _____

Percentage of time *Integrity* is required: _____

Percentage of time *Availability* is required: _____

Execution Phase:

Percentage of time *Confidentiality* is required: _____

Percentage of time *Integrity* is required: _____

Percentage of time *Availability* is required: _____

Monitor Phase:

Percentage of time *Confidentiality* is required: _____

Percentage of time *Integrity* is required: _____

Percentage of time *Availability* is required: _____

Steady-state Phase:

Percentage of time *Confidentiality* is required: _____

Percentage of time *Integrity* is required: _____

Percentage of time *Availability* is required: _____

Task: Maintain ready combat air patrol (CAP).

How long is spent supporting the accomplishment of this task in each phase in a 30-day period during which this task is accomplished?

Preparation phase: _____ Days _____ Hours _____ Minutes

Execution phase: _____ Days _____ Hours _____ Minutes

Monitoring phase: _____ Days _____ Hours _____ Minutes

Steady-state phase: _____ Days _____ Hours _____ Minutes

For each phase of the assigned task, consider what percentage of time listed above requires each principle of confidentiality, integrity, or availability. It is possible that each principle will be required 100% at each phase.

Preparation Phase:

Percentage of time *Confidentiality* is required: _____

Percentage of time *Integrity* is required: _____

Percentage of time *Availability* is required: _____

Execution Phase:

Percentage of time *Confidentiality* is required: _____

Percentage of time *Integrity* is required: _____

Percentage of time *Availability* is required: _____

Monitor Phase:

Percentage of time *Confidentiality* is required: _____

Percentage of time *Integrity* is required: _____

Percentage of time *Availability* is required: _____

Steady-state Phase:

Percentage of time *Confidentiality* is required: _____

Percentage of time *Integrity* is required: _____

Percentage of time *Availability* is required: _____

Task: Detect, localize, and track subsurface contacts w/ active/passive sonobuoys.

How long is spent supporting the accomplishment of this task in each phase in a 30-day period during which this task is accomplished?

Preparation phase: _____ Days _____ Hours _____ Minutes

Execution phase: _____ Days _____ Hours _____ Minutes

Monitoring phase: _____ Days _____ Hours _____ Minutes

Steady-state phase: _____ Days _____ Hours _____ Minutes

For each phase of the assigned task, consider what percentage of time listed above requires each principle of confidentiality, integrity, or availability. It is possible that each principle will be required 100% at each phase.

Preparation Phase:

Percentage of time *Confidentiality* is required: _____

Percentage of time *Integrity* is required: _____

Percentage of time *Availability* is required: _____

Execution Phase:

Percentage of time *Confidentiality* is required: _____

Percentage of time *Integrity* is required: _____

Percentage of time *Availability* is required: _____

Monitor Phase:

Percentage of time *Confidentiality* is required: _____

Percentage of time *Integrity* is required: _____

Percentage of time *Availability* is required: _____

Steady-state Phase:

Percentage of time *Confidentiality* is required: _____

Percentage of time *Integrity* is required: _____

Percentage of time *Availability* is required: _____

Task: Plan/direct attack of submarines.

How long is spent supporting the accomplishment of this task in each phase in a 30-day period during which this task is accomplished?

Preparation phase: _____ Days _____ Hours _____ Minutes

Execution phase: _____ Days _____ Hours _____ Minutes

Monitoring phase: _____ Days _____ Hours _____ Minutes

Steady-state phase: _____ Days _____ Hours _____ Minutes

For each phase of the assigned task, consider what percentage of time listed above requires each principle of confidentiality, integrity, or availability. It is possible that each principle will be required 100% at each phase.

Preparation Phase:

Percentage of time *Confidentiality* is required: _____

Percentage of time *Integrity* is required: _____

Percentage of time *Availability* is required: _____

Execution Phase:

Percentage of time *Confidentiality* is required: _____

Percentage of time *Integrity* is required: _____

Percentage of time *Availability* is required: _____

Monitor Phase:

Percentage of time *Confidentiality* is required: _____

Percentage of time *Integrity* is required: _____

Percentage of time *Availability* is required: _____

Steady-state Phase:

Percentage of time *Confidentiality* is required: _____

Percentage of time *Integrity* is required: _____

Percentage of time *Availability* is required: _____

Task: Emergency repairs to equipment critical to ship's mission.

How long is spent supporting the accomplishment of this task in each phase in a 30-day period during which this task is accomplished?

Preparation phase: _____ Days _____ Hours _____ Minutes

Execution phase: _____ Days _____ Hours _____ Minutes

Monitoring phase: _____ Days _____ Hours _____ Minutes

Steady-state phase: _____ Days _____ Hours _____ Minutes

For each phase of the assigned task, consider what percentage of time listed above requires each principle of confidentiality, integrity, or availability. It is possible that each principle will be required 100% at each phase.

Preparation Phase:

Percentage of time *Confidentiality* is required: _____

Percentage of time *Integrity* is required: _____

Percentage of time *Availability* is required: _____

Execution Phase:

Percentage of time *Confidentiality* is required: _____

Percentage of time *Integrity* is required: _____

Percentage of time *Availability* is required: _____

Monitor Phase:

Percentage of time *Confidentiality* is required: _____

Percentage of time *Integrity* is required: _____

Percentage of time *Availability* is required: _____

Steady-state Phase:

Percentage of time *Confidentiality* is required: _____

Percentage of time *Integrity* is required: _____

Percentage of time *Availability* is required: _____

APPENDIX B. EXPERIMENTAL DATA

A. TASK 1: TRANSPORT AND / OR PROVIDE FOR CASUALTY / PATIENT EVACUATION

1. Operations Department

Preparation									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
10	0	10	0	25.0000%	25.0000%	50.0000%	150	150	300
9	0	0	90	15.0000%	100.0000%	100.0000%	13.5	90	90
13	0	2	30	0.0694%	0.0694%	0.8333%	29.9808	29.9808	359.9856
12	0	1	0	0.1389%	0.1389%	0.1389%	60.0048	60.0048	60.0048
5	1	6	0	0.1300%	0.8300%	0.1700%	56.16	358.56	73.44
6	3	3	0	10.0000%	50.0000%	40.0000%	450	2250	1800
4	7	0	0	60.0000%	20.0000%	20.0000%	6048	2016	2016
35	0	4	0	100.0000%	100.0000%	100.0000%	240	240	240
36	0	4	0	100.0000%	100.0000%	10.0000%	240	240	24
44	2	0	0	25.0000%	100.0000%	25.0000%	720	2880	720
45	0	8	0	15.0000%	100.0000%	50.0000%	72	480	240
46	0	8	0	20.0000%	20.0000%	20.0000%	96	96	96
Execution									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
10	0	2	0	0.0000%	25.0000%	75.0000%	0	30	90
9	0	2	0	0.0000%	100.0000%	100.0000%	0	120	120
13	0	2	0	0.0694%	0.0694%	0.8333%	29.9808	29.9808	359.9856
12	0	2	0	1.6667%	1.6667%	1.6667%	720.0144	720.0144	720.0144
5	1	6	0	23.3000%	23.3000%	23.3000%	10065.6	10065.6	10065.6
6	0	5	0	10.0000%	30.0000%	60.0000%	30	90	180
4	0	1	0	10.0000%	10.0000%	80.0000%	6	6	48
35	0	4	0	100.0000%	100.0000%	100.0000%	240	240	240
36	0	2	0	100.0000%	100.0000%	100.0000%	120	120	120
44	0	2	0	10.0000%	100.0000%	100.0000%	12	120	120
45	0	5	0	10.0000%	50.0000%	100.0000%	30	150	300
46	1	2	0	10.0000%	25.0000%	60.0000%	156	390	936

Monitor									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
10	0	2	0	50.0000%	25.0000%	25.0000%	60	30	30
9	0	4	0	0.0000%	90.0000%	100.0000%	0	216	240
13	0	0	0	0.0347%	0.0347%	0.0347%	14.9904	14.9904	14.9904
12	0	2	0	1.6667%	1.6667%	1.6667%	720.0144	720.0144	720.0144
5	2	12	0	9.9900%	9.9900%	12.0000%	4315.68	4315.68	5184
6	0	0	30	0.0000%	0.0000%	100.0000%	0	0	30
4	0	2	0	75.0000%	15.0000%	10.0000%	90	18	12
35	0	4	0	100.0000%	100.0000%	100.0000%	240	240	240
36	0	4	0	100.0000%	100.0000%	100.0000%	240	240	240
44	0	4	0	15.0000%	100.0000%	50.0000%	36	240	120
45	0	2	0	10.0000%	100.0000%	40.0000%	12	120	48
46	0	2	0	10.0000%	100.0000%	25.0000%	12	120	30
Steady State									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
10	0	0	0	0.0000%	0.0000%	0.0000%	0	0	0
9	0	0	0	0.0000%	0.0000%	0.0000%	0	0	0
13	0	0	0	0.0347%	0.0347%	0.0347%	14.9904	14.9904	14.9904
12	0	0	0	0.0000%	0.0000%	0.0000%	0	0	0
5	4	0	0	23.3000%	23.3000%	20.0000%	10065.6	10065.6	8640
6	0	1	0	30.0000%	30.0000%	40.0000%	18	18	24
4	2	0	0	20.0000%	60.0000%	20.0000%	576	1728	576
35	0	1	0	50.0000%	100.0000%	100.0000%	30	60	60
36	0	1	0	50.0000%	50.0000%	100.0000%	30	30	60
44	0	1	0	0.0000%	50.0000%	50.0000%	0	30	30
45	0	0	0	0.0000%	0.0000%	0.0000%	0	0	0
46	0	1	0	25.0000%	50.0000%	50.0000%	15	30	30

2. Supply/ Logistics Department

Preparation									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
14	0	0	0	0.4	0.2	0.4	0	0	0
17	0	0	0	0	0	0	0	0	0
11	0	0	120	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0
2	0	4	0	0	0	1	0	0	240
8	0	8	0	0	1	1	0	480	480
7	0	10	0	0.0025	0.0083	0.0026	108	358.56	112.32
3	0	0	0	0	0	0	0	0	0
Execution									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
14	5	0	0	0.1	0.45	0.45	720	3240	3240
17	0	2	0	0.8	1	1	96	120	120
11	0	0	0	0	0	0	0	0	0
1	0	17	30	0	1	0	0	1050	0
2	0	2	0	0	0.5	0.5	0	60	60
8	0	2	0	1	1	1	120	120	120
7	0	10	0	0.0026	0.0083	0.0026	112.32	358.56	112.32
3	0	0	0	0	0	0	0	0	0

Monitor									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
14	5	0	0	0.1	0.45	0.45	720	3240	3240
17	0	2	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
1	0	30	0	0	1	0	0	1800	0
2	0	2	0	0	0	1	0	0	120
8	0	5	0	0	1	0.75	0	300	225
7	0	5	0	0.0013	0.0026	0.0026	56.16	112.32	112.32
3	0	0	0	0	0	0	0	0	0
Steady State									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
14	20	0	0	0.2	0.4	0.4	5760	11520	11520
17	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0
2	0	30	0	0	0	1	0	0	1800
8	0	2	0	0.25	1	0.75	30	120	90
7	0	5	0	0.0013	0.0026	0.0026	56.16	112.32	112.32
3	0	0	0	0	0	0	0	0	0

B. TASK 2: CONDUCT DAILY HELICOPTER OPERATIONS

1. Operations Department

Preparation									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
10	0	60	0	0.0000%	25.0000%	75.0000%	0	360	1080
9	0	0	90	18.0000%	100.0000%	100.0000%	16.2	90	90
13	1	0	0	3.3333%	3.3333%	3.3333%	1439.9856	1439.9856	1439.9856
12	0	8	0	0.0000%	1.6667%	1.6667%	0	720.0144	720.0144
5	5	0	0	23.3000%	23.3000%	23.3000%	10065.6	10065.6	10065.6
6	10	0	0	20.0000%	70.0000%	10.0000%	2880	10080	1440
4	2	0	0	20.0000%	20.0000%	60.0000%	576	576	1728
35	0	384	0	100.0000%	100.0000%	100.0000%	9216	9216	9216
36	0	384	0	100.0000%	10.0000%	100.0000%	9216	921.6	9216
44	10	0	0	10.0000%	75.0000%	10.0000%	1440	10800	1440
45	1	0	0	3.3330%	3.3330%	3.3330%	47.9952	47.9952	47.9952
46	0	20	0	10.0000%	50.0000%	10.0000%	48	240	48
Execution									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
10	0	90	0	0.0000%	10.0000%	90.0000%	0	540	4860
9	0	45	0	0.0000%	100.0000%	100.0000%	0	2700	2700
13	0	12	0	3.3333%	3.3333%	3.3333%	1439.9856	1439.9856	1439.9856
12	0	12	0	0.0000%	1.6667%	1.6667%	0	720.0144	720.0144
5	30	0	0	70.0000%	46.6000%	3.3000%	30240	20131.2	1425.6
6	0	12	0	10.0000%	45.0000%	45.0000%	72	324	324
4	0	12	0	25.0000%	50.0000%	25.0000%	180	360	180
35	0	384	0	100.0000%	100.0000%	100.0000%	23040	23040	23040
36	0	384	0	100.0000%	100.0000%	100.0000%	23040	23040	23040
44	0	12	0	3.3330%	100.0000%	40.0000%	23.9976	720	288
45	0	12	0	10.0000%	100.0000%	25.0000%	72	720	180
46	0	18	0	3.3330%	100.0000%	40.0000%	35.9964	1080	432

Monitor									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
10	0	150	0	10.0000%	10.0000%	80.0000%	900	900	7200
9	0	0	150	0.0000%	80.0000%	100.0000%	0	120	150
13	0	12	0	3.3333%	3.3333%	3.3333%	1439.9856	1439.9856	1439.9856
12	0	12	0	0.0000%	1.6667%	1.6667%	0	720.0144	720.0144
5	30	0	0	70.0000%	70.0000%	3.3000%	30240	30240	1425.6
6	0	6	0	30.0000%	30.0000%	40.0000%	108	108	144
4	0	4	0	15.0000%	65.0000%	20.0000%	36	156	48
35	0	384	0	100.0000%	100.0000%	100.0000%	23040	23040	23040
36	0	384	0	100.0000%	100.0000%	100.0000%	23040	23040	23040
44	0	6	0	15.0000%	65.0000%	20.0000%	54	234	72
45	0	5	0	10.0000%	40.0000%	40.0000%	30	120	120
46	0	20	0	10.0000%	40.0000%	10.0000%	120	480	120
Steady State									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
10	0	0	0	0	0	0	0	0	0
9	0	30	0	0	0.8	1	0	1440	1800
13	0	12	0	0.033333	0.033333	0.033333	1439.9856	1439.9856	1439.9856
12	0	2	0	0	0.003	0.003	0	129.6	129.6
5	30	0	0	0.7	0.7	0.033	30240	30240	1425.6
6	1	0	0	0.2	0.2	0.6	288	288	864
4	0	10	0	0.4	0.4	0.2	240	240	120
35	0	96	0	0.8	1	1	4608	5760	5760
36	0	48	0	0.5	0.5	1	1440	1440	2880
44	1	0	0	0	0.2	0.6	0	288	864
45	0	12	0	0.2	0.4	0.4	144	288	288
46	0	48	0	0	0.2	0.5	0	576	1440

2. Supply / Logistics Department

Preparation									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
14	0	120	0	0.4	0.3	0.3	1152	864	864
17	0	0	450	0.5	1	1	225	450	450
11	0	60	0	0	0	0	0	0	0
1	15	8	0	0	0	1	0	0	21792
2	0	15	0	0	0	1	0	0	360
8	0	15	0	0	1	1	0	360	360
7	0	20	0	0.016	0.0083	0.0026	691.2	358.56	112.32
3	6	2	0	0.1	0.5	0.4	868.8	4344	3475.2
Execution									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
14	16	0	0	0.2	0.4	0.4	4608	9216	9216
17	0	1	0	1	1	1	60	60	60
11	0	0	0	0	0	0	0	0	0
1	15	0	0	0	0	1	0	0	21600
2	0	360	0	0	0.5	0.5	0	10800	10800
8	0	2	0	0	1	1	0	120	120
7	0	20	0	0.016	0.0083	0.0026	691.2	358.56	112.32
3	6	6	0	0.1	0.5	0.4	900	4500	3600

Monitor									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
14	7	0	0	0.2	0.4	0.4	2016	4032	4032
17	0	1	0	0	0.8	0.5	0	48	30
11	0	30	0	0	0	0	0	0	0
1	30	0	0	0	0	1	0	0	43200
2	0	180	0	0	0	1	0	0	10800
8	30	0	0	0	1	1	0	43200	43200
7	0	20	0	0.0214	0.0013	0.0013	924.48	56.16	56.16
3	6	6	0	0.1	0.5	0.4	900	4500	3600
Steady State									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
14	3	0	0	0.2	0.4	0.4	864	1728	1728
17	0	0	0	0	0	0	0	0	0
11	0	90	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0
2	0	90	0	0	0	1	0	0	5400
8	0	0	0	0	0	0	0	0	0
7	0	20	0	0.0214	0.0013	0.0013	924.48	56.16	56.16
3	1	2	0	0.1	0.5	0.4	156	780	624

C. TASK 3: MAINTAIN READY COMBAT AIR PATROL (CAP)

1. Operations Department

Preparation									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
10	0	240	0	0.1	0.5	0.4	576	2880	2304
9	0	135	0	0.25	1	1	810	3240	3240
13	1	0	0	0.033333	0.033333	0.033333	1439.9856	1439.9856	1439.9856
12	0	4	0	0.006	0.006	0.006	259.2	259.2	259.2
5	25	0	0	1	0.7	0.46	43200	30240	19872
6	10	0	0	0.7	0.2	0.1	10080	2880	1440
4	5	0	0	0.4	0.4	0.2	2880	2880	1440
35	0	0	0	0	0	0	0	0	0
36	0	0	0	0	0	0	0	0	0
44	0	135	0	0.25	1	1	810	3240	3240
45	25	0	0	1	0.7	0.45	36000	25200	16200
46	5	0	0	0.25	0.4	0.2	1800	2880	1440
Execution									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
10	0	15	0	0.25	0.25	0.5	225	225	450
9	0	45	0	0.5	1	1	1350	2700	2700
13	0	12	0	0.033333	0.033333	0.033333	1439.9856	1439.9856	1439.9856
12	0	12	0	0.8333	0.016667	0.016667	35998.56	720.0144	720.0144
5	30	0	0	1	0.7	0.46	43200	30240	19872
6	1	0	0	0.1	0.3	0.6	144	432	864
4	0	0	30	0.45	0.45	0.1	13.5	13.5	3
35	0	0	0	0	0	0	0	0	0
36	0	0	0	0	0	0	0	0	0
44	25	0	0	1	0.6	0.45	36000	21600	16200
45	30	0	0	1	0.7	0.45	43200	30240	19440
46	0	0	30	0.45	0.45	0.1	13.5	13.5	3

Monitor									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
10	0	300	0	0.25	0.25	0.5	4500	4500	9000
9	0	0	450	0.5	1	0.25	225	450	112.5
13	0	12	0	0.016667	0.033333	0.033333	720.0144	1439.9856	1439.9856
12	0	12	0	0	0.016667	0.016667	0	720.0144	720.0144
5	30	0	0	1	0.7	0.23	43200	30240	9936
6	5	0	0	0.2	0.4	0.4	1440	2880	2880
4	0	8	0	0.1	0.6	0.2	48	288	96
35	0	0	0	0	0	0	0	0	0
36	0	0	0	0	0	0	0	0	0
44	0	45	0	0	0.5	1	0	1350	2700
45	30	0	0	1	0.7	0.25	43200	30240	10800
46	0	8	0	0.1	0.6	0.2	48	288	96
Steady State									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
10	0	0	0	0	0	0	0	0	0
9	0	360	0	1	1	1	21600	21600	21600
13	0	12	0	0.016667	0.033333	0.033333	720.0144	1439.9856	1439.9856
12	0	2	0	0	0.003	0.003	0	129.6	129.6
5	20	0	0	1	0.23	0.23	43200	9936	9936
6	1	0	0	0.3	0.35	0.35	432	504	504
4	0	12	0	0.15	0.4	0.45	108	288	324
35	0	0	0	0	0	0	0	0	0
36	0	0	0	0	0	0	0	0	0
44	0	360	0	0	1	0.75	0	21600	16200
45	20	0	0	1	0.25	0.25	28800	7200	7200
46	0	12	0	0.15	0.4	0.45	108	288	324

2. Supply / Logistics Department

Steady State									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
14	5	0	0	0	0.5	0.5	0	3600	3600
17	0	0	0	0	0	0	0	0	0
11	0	90	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0
2	0	90	0	0	0	1	0	0	5400
8	0	0	0	0	0	0	0	0	0
7	20	0	0	0.233	0.233	0.2	10065.6	10065.6	8640
3	7	8	2	0.1	0.5	0.4	1056.2	5281	4224.8
Monitor									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
14	5	0	0	0	0.5	0.5	0	3600	3600
17	0	90	0	0	0	1	0	0	5400
11	0	30	0	0	0	0	0	0	0
1	30	0	0	0	0	1	0	0	43200
2	0	180	0	0	0	1	0	0	10800
8	30	0	0	0	1	1	0	43200	43200
7	20	0	0	0.0999	0.0999	0.12	4315.68	4315.68	5184
3	7	8	0	0.1	0.5	0.4	1056	5280	4224

Execution									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
14	10	0	0	0	0.5	0.5	0	7200	7200
17	0	180	0	0.3	1	1	3240	10800	10800
11	0	0	0	0	0	0	0	0	0
1	15	0	0	0	0	1	0	0	21600
2	0	360	0	0	0.5	0	0	10800	0
8	0	2	0	0	1	1	0	120	120
7	10	0	0	0.233	0	0	10065.6	0	0
3	7	8	0	0.1	0.5	0.4	1056	5280	4224
Preparation									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
14	10	0	0	0.5	0	0.5	21600	0	21600
17	0	120	0	0.5	0.9	0.9	1440	2592	2592
11	0	60	0	0	0	0	0	0	0
1	15	0	0	0	0	1	0	0	21600
2	0	45	0	0	0	1	0	0	1080
8	0	15	0	0	1	1	0	360	360
7	7	0	0	0.233	0	0	10065.6	0	0
3	7	8	0	0.1	0.5	0.4	1027.2	5136	4108.8

D. TASK4: DETECT, LOCALIZE, AND TRACK SUBSURFACE CONTACTS WITH ACTIVE / PASSIVE SONOBUOYS

1. Operations Department

Preparation									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
10	0	60	0	0	0.25	0.75	0	360	1080
9	0	0	90	0.15	1	1	13.5	90	90
13	0	24	0	0.033333	0.033333	0.033333	1439.9856	1439.9856	1439.9856
12	0	24	0	0.033333	0.033333	0.033333	1439.9856	1439.9856	1439.9856
5	5	0	0	1	0.46	0.23	43200	19872	9936
6	15	0	0	0.8	0.1	0.1	17280	2160	2160
4	1	0	0	0.6	0.3	0.1	864	432	144
35	0	0	0	0	0	0	0	0	0
36	0	0	0	0	0	0	0	0	0
44	0	0	90	0.15	1	1	13.5	90	90
45	5	0	0	1	0.45	0.25	7200	3240	1800
46	1	0	0	0.6	0.5	0.1	864	720	144
Execution									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
10	0	30	0	0	0.1	0.9	0	180	1620
9	0	150	0	0	1	1	0	9000	9000
13	0	24	0	0.033333	0.033333	0.033333	1439.9856	1439.9856	1439.9856
12	0	36	0	0.05	0.05	0.05	2160	2160	2160
5	5	0	0	1	0.46	0.23	43200	19872	9936
6	1	0	0	0.1	0.4	0.5	144	576	720
4	0	4	0	0.6	0.3	0.1	144	72	24
35	0	0	0	0	0	0	0	0	0
36	0	0	0	0	0	0	0	0	0
44	0	150	0	0	1	1	0	9000	9000
45	5	0	0	1	0.45	0.25	7200	3240	1800
46	0	4	0	0.6	0.5	0.1	144	120	24

Monitor									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
10	0	80	0	0.1	0.1	0.8	480	480	3840
9	0	0	150	0	0.8	1	0	120	150
13	0	24	0	0.033333	0.033333	0.033333	1439.9856	1439.9856	1439.9856
12	0	36	0	0.003	0.003	0.003	129.6	129.6	129.6
5	5	0	0	1	0.033	0.46	43200	1425.6	19872
6	1	0	0	0.4	0.4	0.1	576	576	144
4	0	4	0	0.4	0.5	0.1	96	120	24
35	0	0	0	0	0	0	0	0	0
36	0	0	0	0	0	0	0	0	0
44	0	0	150	0	0.9	1	0	135	150
45	5	0	0	1	0.033	0.45	7200	237.6	3240
46	0	4	0	0.4	0.5	0.1	96	120	24
Steady State									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
10	0	0	0	0	0	0	0	0	0
9	0	1.3	0	0	0.8	1	0	62.4	78
13	0	24	0	0.033333	0.033333	0.033333	1439.9856	1439.9856	1439.9856
12	0	2	0	0.003	0.003	0.003	129.6	129.6	129.6
5	5	0	0	0.46	0.7	0.23	19872	30240	9936
6	1	0	0	0.3	0.35	0.35	432	504	504
4	0	2	0	0.4	0.5	0.1	48	60	12
35	0	0	0	0	0	0	0	0	0
36	0	0	0	0	0	0	0	0	0
44	0	1.3	0	0	0.8	1	0	62.4	78
45	5	0	0	0.45	0.7	0.25	3240	5040	1800
46	0	2	0	0.4	0.5	0.1	48	60	12

2. Supply / Logistics Department

Preparation									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
14	10	0	0	0.5	0	0.5	7200	0	7200
17	0	0	60	1	1	1	60	60	60
11	0	0	0	0	0	0	0	0	0
1	15	0	0	0	0	1	0	0	21600
2	0	30	0	0	0	1	0	0	720
8	0	10	0	1	1	1	240	240	240
7	10	0	0	0.233	0.0999	0	10065.6	4315.68	0
3	7	12	0	0.25	0.5	0.25	2592	5184	2592
Execution									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
14	10	0	0	0	0.5	0.5	0	7200	7200
17	0	0	180	1	1	1	180	180	180
11	0	0	0	0	0	0	0	0	0
1	15	0	0	0	0	1	0	0	21600
2	0	15	0	0	0.5	0.5	0	450	450
8	0	4	0	0	1	1	0	240	240
7	10	0	0	0.233	0.0999	0	10065.6	4315.68	0
3	7	12	0	0.25	0.5	0.25	2700	5400	2700

Monitor									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
14	5	0	0	0	0.5	0.5	0	3600	3600
17	0	0	30	0	0.5	0.8	0	15	24
11	0	0	0	0	0	0	0	0	0
1	30	0	0	0	0	1	0	0	43200
2	0	15	0	0	0	1	0	0	900
8	30	0	0	0.5	1	1	21600	43200	43200
7	5	0	0	0.016	0.12	0.016	691.2	5184	691.2
3	7	12	0	0.25	0.5	0.25	2700	5400	2700
Steady State									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
14	5	0	0	0	0.5	0.5	0	3600	3600
17	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0
2	0	15	0	0	0	1	0	0	900
8	0	0	0	0	0	0	0	0	0
7	1	0	0	0.0999	0.0999	0.0999	4315.68	4315.68	4315.68
3	7	12	0	0.25	0.5	0.25	2700	5400	2700

E. TASK 5: PLAN / DIRECT ATTACK OF SUBMARINES

1. Operations Department

Preparation									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
10	0	60	0	0.1	0.15	0.25	144	216	360
9	0	0	90	0.15	1	1	13.5	90	90
13	1	0	0	0.016667	0.033333	0.033333	720.0144	1439.9856	1439.9856
12	0	24	0	0.033333	0.033333	0.033333	1439.9856	1439.9856	1439.9856
5	0	0	0	0	0	0	0	0	0
6	7	0	0	0.6	0.3	0.1	6048	3024	1008
4	1	0	0	0.6	0.3	0.1	864	432	144
35	0	0	0	0	0	0	0	0	0
36	0	0	0	0	0	0	0	0	0
44	0	0	90	0.15	1	1	13.5	90	90
45	0	0	0	0	0	0	0	0	0
46	1	0	0	0.5	0.25	0.1	720	360	144
Execution									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
10	0	90	0	0.1	0.15	0.75	540	810	4050
9	0	150	0	0	1	1	0	9000	9000
13	0	3	0	0.000694	0.000694	0.000694	29.9808	29.9808	29.9808
12	0	36	0	0.05	0.05	0.05	2160	2160	2160
5	0	0	0	0	0	0	0	0	0
6	1	0	0	0.2	0.4	0.4	288	576	576
4	0	4	0	0.4	0.4	0.2	96	96	48
35	0	0	0	0	0	0	0	0	0
36	0	0	0	0	0	0	0	0	0
44	0	150	0	0	1	1	0	9000	9000
45	0	0	0	0	0	0	0	0	0
46	0	4	0	0.5	0.5	0.75	120	120	180

Monitor									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
10	0	240	0	0.1	0.15	0.75	1440	2160	10800
9	0	0	150	0	0.8	1	0	120	150
13	1	0	0	0.0083333	0.0083333	0.0083333	359.99856	359.99856	359.99856
12	0	36	0	0.05	0.05	0.05	2160	2160	2160
5	0	0	0	0	0	0	0	0	0
6	1	0	0	0.3	0.35	0.35	432	504	504
4	0	4	0	0.2	0.6	0.2	48	144	48
35	0	0	0	0	0	0	0	0	0
36	0	0	0	0	0	0	0	0	0
44	0	0	150	0	0.8	1	0	120	150
45	0	0	0	0	0	0	0	0	0
46	0	4	0	0.2	0.75	0.3	48	180	72
Steady State									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
10	0	0	0	0	0	0	0	0	0
9	0	30	0	0	0.8	1	0	1440	1800
13	1	0	0	0.0083333	0.0083333	0.0083333	359.9856	359.9856	359.9856
12	0	2	0	0.003	0.003	0.003	129.6	129.6	129.6
5	0	0	0	0	0	0	0	0	0
6	1	0	0	0.3	0.35	0.35	432	504	504
4	0	4	0	0.4	0.2	0.4	96	48	96
35	0	0	0	0	0	0	0	0	0
36	0	0	0	0	0	0	0	0	0
44	0	30	0	0	0.8	1	0	1440	1800
45	0	0	0	0	0	0	0	0	0
46	0	4	0	0.3	0.2	0.3	72	48	72

2. Supply / Logistics Department

Preparation									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
14	15	0	0	0.8	0.1	0.1	17280	2160	2160
17	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
1	15	0	0	0	0	1	0	0	21600
2	0	0	0	0	0	0	0	0	0
8	0	10	0	1	1	1	240	240	240
7	10	0	0	0.333	0	0	14385.6	0	0
3	7	12	0	0.25	0.5	0.25	2592	5184	2592
Execution									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
14	3	0	0	0.8	0.1	0.1	3456	432	432
17	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
1	15	0	0	0	0	1	0	0	21600
2	0	0	0	0	0	0	0	0	0
8	0	4	0	0	1	1	0	240	240
7	10	0	0	0.333	0	0	14385.6	0	0
3	7	12	0	0.25	0.5	0.25	2700	5400	2700

Monitor									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
14	2	0	0	0.8	0.1	0.1	2304	288	288
17	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
1	30	0	0	0	0	1	0	0	43200
2	0	0	0	0	0	0	0	0	0
8	30	0	0	0	0	0	0	0	0
7	5	0	0	0.016	0.14	0	691.2	6048	0
3	7	12	0	0.25	0.5	0.25	2700	5400	2700
Steady State									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
14	10	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
7	5	0	0	0.333	0	0	14385.6	0	0
3	7	12	0	0.25	0.5	0.25	2700	5400	2700

F. TASK 6: EMERGENCY REPAIRS TO EQUIPMENT CRITICAL TO SHIP'S MISSION

1. Operations Department

Preparation									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
10	0	30	0	0.15	0.25	0.6	108	180	432
9	2	0	0	1	1	0.05	2880	2880	144
13	1	0	0	0.000347	0.000347	0.000347	14.9904	14.9904	14.9904
12	4	0	0	0	0.14	0.14	0	6048	6048
5	10	2	0	0.46	0.23	0.033	19872	9936	1425.6
6	30	0	0	0.7	0.3	0	30240	12960	0
4	7	0	0	0.25	0.55	0.2	2520	5544	2016
35	0	45	0	1	1	1	1080	1080	1080
36	0	45	0	1	1	1	1080	1080	1080
44	0	0	450	0.5	1	1	225	450	450
45	7	0	0	0.25	0.25	0.033	2520	2520	332.64
46	7	0	0	0.25	0.25	0.2	2520	2520	2016
Execution									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
10	0	90	0	0.15	0.4	0.45	810	2160	2430
9	10	0	0	0.25	1	1	10800	43200	43200
13	0	12	0	0.000347	0.000347	0.000347	14.9904	14.9904	14.9904
12	5	0	0	0	0.175	0.175	0	7560	7560
5	5	10	0	0.46	0.7	0.23	19872	30240	9936
6	10	0	0	0.1	0.4	0.5	1440	5760	7200
4	2	0	0	0.1	0.6	0.3	288	1728	864
35	0	45	0	1	1	1	2700	2700	2700
36	0	45	0	1	1	1	2700	2700	2700
44	0	1	0	0.75	0.5	0.8	45	30	48
45	5	10	0	0.45	0.7	0.25	3510	5460	1950
46	2	0	0	0.1	0.6	0.3	288	1728	864

Monitor									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
10	0	120	0	0.15	0.4	0.45	1080	2880	3240
9	0	2	0	0.25	0.9	0.8	10800	38880	34560
13	0	3	0	0.000347	0.000347	0.000347	14.9904	14.9904	14.9904
12	2	0	0	0	0.003	0.003	0	129.6	129.6
5	5	10	0	0.46	0.46	0.7	19872	19872	30240
6	1	0	0	0.2	0.5	0.3	288	720	432
4	1	0	0	0.1	0.6	0.3	144	864	432
35	0	45	0	1	1	1	2700	2700	2700
36	0	0	0	0	0	0	0	0	0
44	0	0	450	0	0	0.9	0	0	405
45	5	10	0	0.45	0.45	0.7	3510	3510	5460
46	1	0	0	0.1	0.6	0.3	144	864	432
Steady State									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
10	0	0	0	0	0	0	0	0	0
9	180	0	0	0.25	0.8	0.8	10800	34560	34560
13	1	0	0	0.000347	0.000347	0.000347	14.9904	14.9904	14.9904
12	1	0	0	0.1389	0.1389	0.1389	6000.48	6000.48	6000.48
5	5	10	0	0.7	0.033	0.233	30240	1425.6	10065.6
6	1	0	0	0.3	0.35	0.35	432	504	504
4	3	0	0	0.2	0.4	0.2	864	1728	864
35	0	0	0	0	0	0	0	0	0
36	0	0	0	0	0	0	0	0	0
44	0	0	0	0	0	0	0	0	0
45	5	10	0	0.7	0.033	0.25	5460	257.4	1950
46	3	0	0	0.2	0.4	0.2	864	1728	864

2. Supply / Logistics Department

Preparation									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
14	0	0	0	0	0.5	0.5	0	0	0
17	0	0	450	0.5	1	1	225	450	450
11	0	30	0	0	0	0	0	0	0
1	0	30	0	0	0	1	0	0	720
2	0	30	0	0	0	1	0	0	720
8	1	12	0	0.5	1	1	864	1728	1728
7	0	2	0	0.0006	0.0019	0	25.92	82.08	0
3	7	2	0	0.1	0.5	0.4	1012.8	5064	4051.2
Execution									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
14	10	0	0	0	0.5	0.5	0	7200	7200
17	0	1	0	1	0.5	0.8	60	30	48
11	0	30	0	0	0	0	0	0	0
1	10	0	0	0	0	1	0	0	14400
2	0	60	0	0	0	1	0	0	3600
8	0	4	0	0.5	1	1	120	240	240
7	0	20	0	0.0083	0.0166	0.0026	358.56	717.12	112.32
3	7	2	0	0.1	0.5	0.4	1020	5100	4080

Monitor									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
14	10	0	0	0	0.5	0.5	0	7200	7200
17	0	0	450	0	0	1	0	0	450
11	0	90	0	0	0	0	0	0	0
1	30	0	0	0	0	1	0	0	43200
2	0	180	0	0	0	1	0	0	10800
8	0	8	0	0.1	0.5	1	48	240	480
7	0	5	0	0	0.007	0	0	302.4	0
3	7	2	0	0.1	0.5	0.4	1020	5100	4080
Steady State									
Respondent	Days	Hours	Minutes	Confidentiality (%)	Integrity (%)	Availability (%)	Confidentiality (mins)	Integrity (mins)	Availability (mins)
14	10	0	0	0	0.5	0.5	0	7200	7200
17	0	0	0	0	0	0	0	0	0
11	0	60	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0
2	30	0	0	0	0	1	0	0	43200
8	0	0	0	0	0	0	0	0	0
7	0	5	0	0	0.007	0	0	302.4	0
3	7	2	0	0.1	0.5	0.4	1020	5100	4080

LIST OF REFERENCES

- (ISC)², C. W. (2019). *Strategies for building and growing strong cybersecurity teams*. (Cybersecurity Workforce study 2019). International Systems Security Certification Consortium. <https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482>
- Anderson, S. P., & de Palma, A. (2012). Competition for attention in the Information (overload) age. *RAND Journal of Economics*, 43(1), 1–25. <https://doi.org/10.1111/j.1756-2171.2011.00155.x>
- Anley, C., Heasman, J., Linder, F., & Richarte, G. (2007). *The Shellcoder's Handbook. Book* (2nd ed.). Wiley Publishing, Ltd.
- Bergamaschi, S., Guerra, F., & Leiba, B. (2010). Information overload. *IEEE Internet Computing*, (November/December), 10–13. <https://ieeexplore.ieee.org/abstract/document/5617056/>
- BlackAngel. (2009). Malloc des-maleficarum. *Phrack Inc., 0x0d(0x42)* <http://phrack.org/issues/66/10.html>
- Buckshaw, D, Parnell, G, & Ukenholz et al. . (2005). Mission oriented risk and design analysis of critical information systems. *Military Operations Research*, 10(2), 19–38.
- Chant, Ian. (2017, 12 April). The institute: the cybersecurity talent shortage is here, and it's a big threat to companies. *IEEE Cyber Security*<https://cybersecurity.ieee.org/blog/2017/04/13/the-institute-the-cybersecurity-talent-shortage-is-here-and-its-a-big-threat-to-companies/>
- Schram, W., & Cherry, C. (1957). On human communication: a review, a survey, and a criticism. *Journal of the American Statistical Association*, 52(279), 410. <https://doi.org/10.2307/2280926>
- D. E. Denning (1987), An intrusion-detection model. *IEEE Transactions on Software Engineering*, vol SE-13(2), pp. 222–232. <https://ieeexplore.ieee.org/document/1702202>
- Department of Defense. (2011). Department of defense strategy for operating in cybersapce. Washington, D.C.
- Galbraith, J. (1973). *Designing complex organizations*. Addison-Wesley.
- Galbraith, J. R. (1995). *The Jossey-Bass management series. Designing organizations: an executive briefing on strategy, structure, and process*. Jossey-Bass.

- Godfrey-Smith, P. (2003). *Theory and reality*. The University of Chicago Press.
- Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G., & Williams, T. (2011). *Gray Hat Hacking*. McGraw Hill/Osbourne.
- Harris, S. (2008). *All-in-one CISSP certification exam guide* (2nd ed.). (G. Hancock & J. McKenzie, Eds.) (Second). New York: McGraw Hill Osborne.
- Heylighen, F. (2004). Complexity and information overload in society: why increasing efficiency leads to decreasing control. *Bulletin of the Medical Library Association*, 87.
- Himma, K. E. (2007). The concept of information overload: a preliminary step in understanding the nature of a harmful information-related condition. *Ethics and Information Technology*, 9(4), 259–272. <https://doi.org/10.1007/s10676-007-9140-8>
- Intel Corporation (2011). *Intel® 64 and IA-32 Architectures Software Developer's Manual* <https://doi.org/10.1109/MAHC.2010.22>
- Joint Chiefs of Staff. (2017). *Joint planning* (JP 5-0). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp5_0_20171606.pdf
- Joint Chiefs of Staff (2002). *Joint Mission Essential Task List (JMETL) Development Handbook*. <http://www.jcs.mil/Portals/36/Documents/Doctrine/training/JMETLbook.pdf?ver=2017-12-29-171303-350>
- Kastenmüller, A., Greitemeyer, T., Zehl, S., Tattersall, A. J., George, H., Frey, D., & Fischer, P. (2014). Leadership and information processing: The influence of transformational and transactional leadership on selective information search, evaluation, and conveying. *Social Psychology*, 45(5), 357–370. <https://doi.org/http://dx.doi.org/10.1027/1864-9335/a000177>
- Kelley, D. (1995). *Automata and Formal Languages: An Introduction*. Upper Saddle River.
- Kewley, D. L., & Bouchard, J. F. (2001). DARPA information assurance program dynamic defense experiment summary. *IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans*, 31(4), 331–336. <https://doi.org/10.1109/3468.935052>
- Klausegger, R., Sinkovics R., & Zou, H (2007). Information overload: a cross-national investigation of influence factors and effects. *Marketing Intelligence and Planning*, 25(7); 691–718. <https://doi.org/10.1108/02634500710834179>

- Kock, N. (2000). Information overload and worker performance: A process-centered view. *Knowledge and Process Management*, 7(4), 256–264.
[https://doi.org/10.1002/1099-1441\(200010/12\)7:4<256::AID-KPM79>3.0.CO;2-U](https://doi.org/10.1002/1099-1441(200010/12)7:4<256::AID-KPM79>3.0.CO;2-U)
- Levy, D. To grow in wisdom: Vannevar Bush, information overload, and the life of leisure. *Proceedings of the 5th ACM/IEEE-CS Joint Conference on Digital Libraries*, pp. 281–286.
- Ligh, M. H., Case, A., Levy, J., & Walters, A. (2014). *The art of memory forensics: detecting malware and threats in Windows, Linux, and Mac memory*. Wiley.
- National Institute of Standards and Technology. (2007). *FIPS 199. FISMA certification and accreditation handbook*. <https://doi.org/10.1016/b978-159749116-7/50032-9>
- National Institute of Standards and Technology. (2008). SP 800–60 volume II : appendices to guide for mapping types of information and information systems to security categories. <https://doi.org/10.6028/NIST.SP.800-60v1r1>
- National Institute of Standards and Technology. (2014). *NIST SP 800-37 - Guide for Applying the Risk Management Framework to Federal Information Systems*. <https://doi.org/10.6028/nist.sp.800-37r1>
- National Institute of Standards and Technology. (2011). *Managing information security risk*. <https://doi.org/10.1108/k.2011.06740caa.012>
- National Institute of Standards and Technology. (2013). *NIST SP 800-53: security and privacy controls for federal information systems and organizations*. <https://doi.org/10.6028/NIST.SP.800-53Ar4>
- National Institute of Standards and Technology. (2018). Risk management framework for information systems and organizations a system life cycle approach for security and privacy. <https://doi.org/10.6028/NIST.SP.800-37r2>
- Office of the DOD Chief Information Officer Department of Defense. (2014, March 12). *Risk management framework (RMF) for DOD information technology (IT)* (DODI 8510.01),. Department of Defense.
http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001_2014.pdf
- O’Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York, NY.
- O’Reilly, C. A. (1980). Individuals and information overload in organizations: is more necessarily better? *Academy of Management Journal*, 23(4), 684–696.
<https://doi.org/10.5465/255556>

- Office of the Chief of Naval Operations (2014, March 18). Required operational capability and projected operational environment for multi-purpose nuclear-powered aircraft carrier (OPNAV C3501.65F).
- PCI Security Standards Council LLC. (2019). *Mapping PCI DSS v3.2.1 to the NIST cybersecurity framework v1.1*.
<https://www.pcisecuritystandards.org/pdfs/Mapping-PCI-DSS-to-NIST-Framework.pdf>
- Qin, X., & Lee, W. (2004). Attack plan recognition and prediction using causal networks. *Proceedings - Annual Computer Security Applications Conference, ACSAC* (pp. 370–379). <https://doi.org/10.1109/CSAC.2004.7>
- Ramaki, A. A., Khosravi-Farmad, M., & Bafghi, A. G. (2015). Real time alert correlation and prediction using Bayesian networks. *12th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)* (Vol. 978, pp. 98–103). <https://doi.org/10.1109/ISCISC.2015.7387905>
- Shim, W. (2010). *Interdependent risk and cyber security: an analysis of security investment and cyber insurance* [Doctoral dissertation, Michigan State University]. Michigan State University Archive.
https://d.lib.msu.edu/.../Interdependent_risk_and_cyber_security__an_analysis_of_security_investment_and_cyber_insurance.pdf
- Silberschatz, A., Galvin, P. B., & Gagne, G. (1995). *Operating system concepts* (4th ed.). Addison-Wesley.
- Simperl, E., Thurlow, I., Warren, P., Dengler, F., Davies, J., Grobelnik, M., Mladenic, D., , Gomez-Perez, J., & Moreno, C. R. (2010). Overcoming information overload in the enterprise: the active approach. *IEEE Internet Computing*, 14(6), 39–46.
<https://doi.org/10.1109/MIC.2010.146>
- Sipser, M. (1996). Introduction to the theory of computation. *ACM SIGACT News* (Vol. 27). McGraw-Hill. <https://doi.org/10.1145/230514.571645>
- Torres, A. (2015). *Building a world-class security operations center: a roadmap*. SANS.
<https://www.sans.org/reading-room/whitepapers/analyst/building-world-class-security-operations-center-roadmap-35907>
- Veeramachaneni, K., Arnaldo, I., Korrapati, V., Bassias, C., & Li, K. (2016). AI2: training a big data machine to defend. *Proceedings - 2nd IEEE International Conference on Big Data Security on Cloud, IEEE BigDataSecurity 2016, 2nd IEEE International Conference on High Performance and Smart Computing, IEEE HPSC 2016 and IEEE International Conference on Intelligent Data and Security* (pp. 49–54). <https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2016.79>

Woods, David & Patterson, Emily & Roth, Emilie. (2002). Can we ever escape from data overload? *A Cognitive Systems Diagnosis. Cognition, Technology & Work*. 4(1). (pp. 22–36). 10.1007/s101110200002.

Zhong, C., Yen, J., Liu, P., & Erbacher, R. F. (2016). Automate cybersecurity data triage by leveraging human analysts' cognitive process. *Proceedings - 2nd IEEE International Conference on Big Data Security on Cloud, IEEE BigDataSecurity 2016, 2nd IEEE International Conference on High Performance and Smart Computing, IEEE HPSC 2016 and IEEE International Conference on Intelligent Data and Security* (pp. 357–363). <https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2016.41>

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