NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CYBERSECURITY RISK MANAGEMENT PROCESS FOR UNMANNED AERIAL SYSTEMS (UAS) AT THE STRATEGIC LEVEL

by

Gonzalo Santiago

June 2019

Thesis Advisor: Raymond R. Buettner Jr.
Co-Advisor: Aurelio Monarrez Jr.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE June 2019	3. REPORT TYPE AND DATES COVERED Master's thesis

4. TITLE AND SUBTITLE CYBERSECURITY RISK MANAGEMENT PROCESS FOR UNMANNED AERIAL SYSTEMS (UAS) AT THE STRATEGIC LEVEL	5. FUNDING NUMBERS R4M3G
6. AUTHOR(S) Gonzalo Santiago	
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) CRUSER, Monterey, CA 93943	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)

In the last decade, the integration of unmanned aerial systems (UAS) into military operations has grown substantially. UAS have significantly contributed to U.S. military tactical, operational and strategic operations. Recently, the U.S. military has made increasing use of commercial off-the-shelf (COTS) UAS, yet none of the U.S. military services have a defined cybersecurity risk management process for COTS UAS. These systems have been susceptible to cyber attacks, leading to the May 2018 ban on the use of these systems across the Department of Defense (DoD). This research effort has developed a multi-echelon cybersecurity risk assessment process for the DoD. The proposed process would enable strategic, operational and tactical commanders to assess and communicate cybersecurity risks associated with COTS UAS. The process combined four steps from the Joint Risk Analysis Methodology (JRAM) framework and seven steps from a strategic risk business management process. This process would allow commanders to have an enhanced awareness of cybersecurity risks associated with COTS UAS operations, improved current cyber threat assessments, and tailored action plans for their areas of responsibility. The proposed process would help units and agencies across the DoD to resume their use, test and purchase of COTS UASs without the need for the current centralized waiver process.

14. SUBJECT TERMS cybersecurity risk management	15. NUMBER OF PAGES 67
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

CYBERSECURITY RISK MANAGEMENT PROCESS FOR UNMANNED AERIAL SYSTEMS (UAS) AT THE STRATEGIC LEVEL

Gonzalo Santiago
Major, United States Army
BS, University of Puerto Rico – Mayaguez Campus, 2006

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
June 2019

Approved by: Raymond R. Buettner Jr.
Advisor

Aurelio Monarrez Jr.
Co-Advisor

Dan C. Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In the last decade, the integration of unmanned aerial systems (UAS) into military operations has grown substantially. UAS have significantly contributed to U.S. military tactical, operational and strategic operations. Recently, the U.S. military has made increasing use of commercial off-the-shelf (COTS) UAS, yet none of the U.S. military services have a defined cybersecurity risk management process for COTS UAS. These systems have been susceptible to cyber attacks, leading to the May 2018 ban on the use of these systems across the Department of Defense (DoD). This research effort has developed a multi-echelon cybersecurity risk assessment process for the DoD. The proposed process would enable strategic, operational and tactical commanders to assess and communicate cybersecurity risks associated with COTS UAS. The process combined four steps from the Joint Risk Analysis Methodology (JRAM) framework and seven steps from a strategic risk business management process. This process would allow commanders to have an enhanced awareness of cybersecurity risks associated with COTS UAS operations, improved current cyber threat assessments, and tailored action plans for their areas of responsibility. The proposed process would help units and agencies across the DoD to resume their use, test and purchase of COTS UASs without the need for the current centralized waiver process.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AO	Area of Operations
AOR	Area of Responsibility
CMF	Cyber Mission Force
CO	Cyberspace Operations
COTS	Commercial Off-the-Shelf
CRM	Cybersecurity Risk Management
DoD	Department of Defense
DoDI	Department of Defense Instruction
FOC	Full Operational Capability
FY	Fiscal Year
IA	Information Assurance
IS	Information Systems
IT	Information Technology
JP	Joint Publication
JRAM	Joint Risk Analysis Methodology
NIST	National Institute of Standards and Technology
OCO	Offensive Cyberspace Operations
PIT	Platform Information Technology
RMF	Risk Management Framework
SOP	Standard Operating Procedure
T&E	Test and Evaluation
UAS	Unmanned Aerial Systems
USCYBERCOM	Unites States Cyber Command

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First and foremost, I would like to acknowledge and thank my amazing and always supporting wife Sarah for all her support throughout this learning process through my military career. I would also like to thank my son Dante for showing me how to look at the world from a different perspective and my daughter Amelia for her contagious energy and perseverance. This accomplishment would not be possible without your inspiration and support. I would next like to thank to Dr. Raymond Buettner and Mr. Aurelio Monarrez for their guidance, knowledge patience and support with this thesis. I am taking all I learned from them to continue developing and growing professionally and personally.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

In 2011, U.S. special forces raided Osama bin Laden's compound in northern Pakistan. During this operation, the military seized a significant number of written documents [1]. In these documents, Osama bin Laden expressed how much he feared drone technology and its capabilities against his terrorist organization [1]. For the terrorist leader, the technological superiority of his adversary limited his options for movement and communication. This is one illustration of how unmanned aerial systems (UAS) technological advancements have changed military operations today. Moreover, advancement, development, and modernization of current and future UAS technology will play a significant role in future military operations.

As the U.S. military modernizes, the adoption of new technology remains an essential part of military operations. In 2018, the U.S. Army created the Army Futures Command as part of the Army's modernization strategy. This strategy is centered on technology, scientific developments and the enhancement of commercially available technology that could be applicable to military operations [2]. The military focuses on not just engineering and developing its own technology, but on the militarization of commercially available technology, where benefits such as lower cost and increased availability often offer an advantage over Department of Defense (DoD) developed systems. In April 2018, the Under Secretary of Defense for Research and Engineering told the Senate Armed Services subcommittee that "The department is not short of innovators. We are short of time, and we lack expertise in adapting commercial market advances to military needs" [3]. While commercially available technology offers many advantages to the military modernization strategy, national-level concerns can result from cybersecurity risks associated with this technology.

Cybersecurity risks associated with commercially available technology have reached national-level concerns. On December 2018, a news article from the *Consumer News and Business Channel* reported that the U.S. government is making changes to

national policy focused on two major Chinese companies [4]. This change in policy is a consequence of allegations that these companies (company 1 and company 2) are developing technology that may be used, on behalf of the Chinese government, to spy on the Americans [4]. Moreover, a similar news article reported that Poland has changed its national policy with respect to Chinese companies, based on allegations of Chinese espionage [5]. Due to these national-level concerns, policy is rapidly changing with respect to some commercially available technology, encouraging end users to consider strategic-level risk. This consideration seeks to ensure commanders are aware of the cybersecurity risks associated with information technology (IT) and unmanned system technology. Nonetheless the usage of these technologies continues to increase.

In the last decade, the rapid increase in the capability and availability associated with UAS technology has enabled commanders at the tactical operational and strategic levels to successfully deploy these systems in their area of operations (AO) to support their missions. Based on the UAS Task Force Airspace Integration Integrated Product Team report, the DoD increased by 81% the UAS flight hours in support of Operation Enduring Freedom and Operation Iraqi Freedom missions from 2005 to 2010 [6]. The effectiveness of this UAS technology in the battlefield increased the DoD's demand for these systems. A report from the Center for the Study of the Drone at Bard College shows DoD's exponentially increasing demand for UAS [7]. The DoD's UAS proposed budget for fiscal year (FY) 2019 is approximately $6.05 billion, a $1.05 billion increase from the requested $5 billion in FY2017 and FY2018 [7]. The proposed budget is intended to cover the costs for UAS combat operations and UAS mission readiness.

For military operations where the cost of UAS technology does not justify the necessity of developing new military systems, commercial off-the-shelf (COTS) UASs have become an option for many commanders. The affordability and availability of COTS UAS technology have allowed commanders to acquire these systems and to deploy them across various AOs. However, the continued growth of reliance on these systems for military operations may represent a risk at all command levels in the military.

As cyberspace enables the employment of these systems, which are themselves cyber physical systems, they are susceptible to cyber-attacks. The cybersecurity risks

associated with the COTS UAS technology can affect multiple command levels at once because the cyber domain has no easily delineated boundaries. While the applicability of rules, regulations and authorities can be limited to specific physical boundaries, a cyber-attack can cross multiple physical boundaries at once. For example, an attacker can cross civilian and government boundaries at once by using the same cyber-attack techniques against personal or government computers. Due to this unique characteristic of the cyber domain and national-level concerns related to cybersecurity, the deployment of COTS UAS technology in military operations requires the development of a multi-echelon cybersecurity risk assessment process. This process should enable strategic, operational and tactical level commanders to communicate elements of cybersecurity risks up and down the chain of command for systems that are being employed.

Currently, none of the U.S. military services have a defined cybersecurity risk management process for COTS UAS. In June 2018, the *Marine Times* reported that all use of COTS UAS across the DoD was banned due to cybersecurity risks associated with the use of COTS UAS [8]. Without a defined process, commanders do not have the ability to conduct an adequate cybersecurity risk assessment and make informed decisions for COTS UAS operations in their area of responsibility (AOR). As a result, the DoD immediately put in place a waiver process to allow limited use of COTS UAS across the DoD until the services developed a strategy to adequately assess and mitigate the risks associated with COTS UAS use.

B. RESEARCH QUESTION

The goal of this research is to identify a process that communicates relevant cybersecurity risks effectively across multiple echelons. The objective is to facilitate better informed decisions regarding cybersecurity risks associated with COTS UAS operations in any AOR.

To achieve this goal, two interrelated questions are addressed: First, how can the strategic-level commander be made aware of the cybersecurity risks they may be assuming as a result of tactical-level operations of COTS UAS? Second, how can the

tactical-level commander be assured that the strategic-level cybersecurity risks have been considered when using COTS UAS?

C. BENEFITS OF THE STUDY

This work provides the DoD with a proposed cybersecurity risk management (CRM) process which will allow the strategic, operational and tactical level commanders to communicate, assess and make better informed and effective decisions for UAS operations in their AOR. Because cybersecurity risks can extend beyond the tactical-level, it is important for strategic-level commanders to have a multi-echelon process that will allow them to efficiently and effectively communicate their strategic-level concerns to tactical-level commanders. This will enable commanders to assess and reduce the risk associated with operations of COTS UAS in their AOR. Additionally, the proposed process should help units and agencies across the DoD to resume their use, test and purchase of the COTS UAS.

D. APPROACH

This thesis begins with a review of the DoD's existing cybersecurity risk assessment processes, policies, definitions and instructions, as well as similar CRM processes used by other organizations. This research focuses on COTS UAS that are being deployed with tactical units in support of strategic-level commands. Also, this research defines and identifies gaps in the implementation of the current CRM process. Next, a proposed multi-echelon CRM process is derived from similar strategic-level risk management process and modified to specifically address the use of COTS UAS. The proposed CRM process is validated through a hypothetical scenario. By using the scenario, it is possible to demonstrate how the model could be used by organizations to communicate relevant cybersecurity risks across multiple command levels, to assess the risk and develop risk mitigation action plans.

E. THESIS OVERVIEW

This chapter (I) has described the motivation for this work and its potential benefits with regard to COTS UAS operations.

Chapter II examines cybersecurity risk management through current doctrinal definitions, existing cybersecurity risk assessment processes, policies and instructions, as well as similar processes used by other organizations outside the DoD. Chapter III introduces a cybersecurity risk management process for COTS UAS operations in any given AOR. Chapter IV uses a hypothetical scenario to demonstrate how the proposed cybersecurity risk management (CRM) process can be used by organizations to communicate and determine the risk. Chapter V presents the conclusions and future work.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

This chapter begins with an examination of the DoD's hierarchical structure, the current doctrinal definition of the cyberspace domain and cyberspace operations (CO), the existing cybersecurity risk assessment processes, policies and instructions, as well as similar processes used by other organizations outside the DoD. This information provides a comprehensive understanding of how the DoD organizes, conceptualizes and directs CO and CRM in support of national-level objectives. These concepts provide a better understanding of the DoD's approach to CRM and supports the identification of potential gaps in its risk analysis methodologies in relation to UAS operations. This produces a foundation for the development of the proposed UAS cyber risk communication process.

A. WARFARE AND THE CYBERSPACE DOMAIN

The actions, planning and execution of military objectives are organized to support national-level objectives. Doctrinal terms and definitions allow the military to conceptualize doctrine for military operations in cyberspace. Furthermore, it implements security requirements to manage risks associated with CO. These concepts are introduced to better understand how the DoD organizes strategies and policies for military operations in the cyberspace domain.

1. Levels of Warfare

As defined in Joint Publication (JP) 1, the military actions used to achieve a national objective are expressed at three levels of warfare: strategic, operational and tactical [9]. These levels are interrelated and linked to specific objectives as shown in Figure 1. The combinations of all objectives ultimately support the national policies as expressed by the executive branch of the government. While there are not rigidly defined boundaries between the levels, they establish the framework of military operations planning and synchronization that allow commanders at each level to achieve their objective, mission and task in support of the national objective [9].

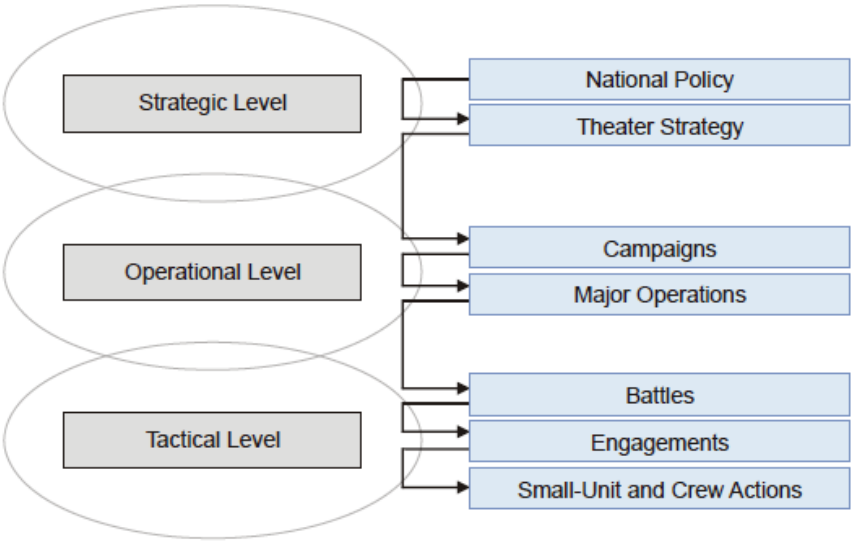

Figure 1. Levels of Warfare. Source: [9]

a. Strategic Level

At the strategic-level, the employment of national power is synchronized to achieve national and multinational objectives [9]. The President establishes the policy and national strategic objectives that the Secretary of Defense uses to define the DoD strategic military objectives, that are used by the combatant commanders for theater strategic planning [9].

b. Operational Level

The operational-level establishes the objectives used to achieve the military end-state within the strategic objectives [9]. Commanders at this level determine deployment of forces and major battle operation arrangements to support operational and strategic objectives [9].

c. Tactical Level

Activities at this level are organized to plan and execute individual battles and engagements to achieve the military objectives assigned to tactical units [9]. Also, at this level the tactical forces employ different tactics to achieve their assigned objectives [9]. Tactics are actions that describe how tactical forces are employed to fight.

2. The Cyberspace Domain

As defined in JP-3–12, cyberspace "is the domain within the information environment that consists of the interdependent network of IT infrastructures and resident data" [10]. This domain has no geographic or geopolitical boundaries. Dominance in cyberspace will enable U.S. military commanders to "achieve and maintain continuing advantages in the operational environment" [10]. The cyberspace domain is incorporated with "the physical domains of air, land, maritime, and space" to achieve strategic, operational or tactical objectives [10].

The cyberspace domain has become an important tool used by commanders at all levels to project force and presence beyond the national boundaries and achieve their strategic, operational and tactical objectives [10]. Also, commanders have seen how military operations executed in the cyber domain can be effective, less risky and more cost effective than operations executed in the physical domain [11]. The inclusion of cyberspace with other physical domains is now considered essential for many military operations to be successful [11].

a. Cyberspace Layers

To understand and facilitate the use of cyberspace as a military operational space the DoD has conceptualized cyberspace in layers. Each layer defines basic concepts of its elements as well as some of the important characteristics that are unique to each layer.

The DoD describes cyberspace in "three interrelated layers: physical network, logical network, and cyber-persona" [10]. This definition simplifies the planning and executions of CO [10].

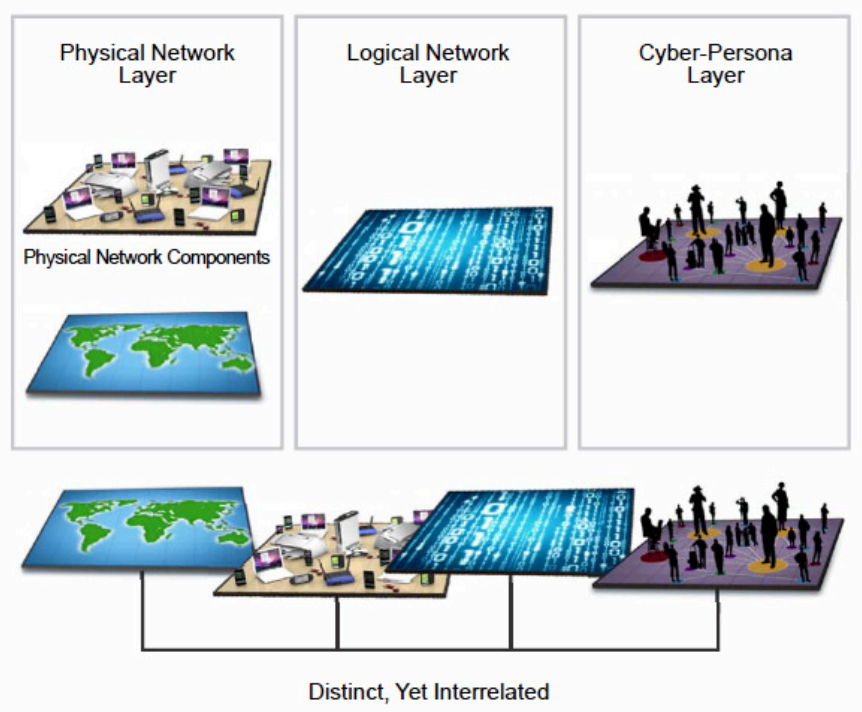

Figure 2. Cyberspace Layers. Source: [10]

The physical network layer is composed of the IT devices and infrastructure that provides an environment to save and process information [10]. Some of the unique characteristics of these layers are based on the private and public physical component ownership [10]. Because the owners of the physical devices control the access and security controls of the majority of the physical elements, the DoD must take into consideration these unique characteristics for mission planning and execution [10].

"The logical network layer consists of those elements of the network related to one another in a way that is abstracted for the physical network" [10]. This means that elements do not have to be necessarily connected by a specific physical element to address and process data [10]. For example, a cable connecting two network devices is considered a physical element of the network while a network protocol used to establish how the data travels from one physical element to another is considered the logical element of the network. A unique characteristic of this layer is that the logical elements can only be engaged with a device or program designed to create a cyberspace effect [10].

The cyber-persona layer is where cyberspace connects to the real world and represents an actor or entity that is defined with data abstracted from the logical network [10]. This consists of network or IT user accounts that are related to an actual person or entity [10]. For example, the email accounts that we create are part of the logical network to allow email to be received and sent; however, these accounts belong to an individual or organization that represent the cyber-persona layer. These are unique characteristics of this layer that the DoD have to take into consideration for mission planning [10].

b. Military Operations in Cyberspace

To execute military operations in cyberspace, the DoD organized a Cyber Mission Force (CMF) supporting three cyberspace missions: Department of Defense Information Networks operations, Offensive Cyberspace Operations (OCO) and Defensive Cyberspace Operations [10]. These operations are intended maintain the confidentiality, integrity and availability of the DoD information [10]. The execution of this mission is assigned to the United States Cyber Command (USCYBERCOM) and its subordinate forces.

To organize the CMF, the DoD organizes its forces in three main units: Cyber Protection Forces, Cyber National Mission Forces and the Cyber Combat Mission Force. The CMF units are directed by the USCYBERCOM subordinate command elements: Cyber National Mission Force-Headquarters, the Joint Force Headquarters-Department of Defense Information Network, the Joint Force Headquarters-Cyberspace, the Service Cyber Components Headquarters and the CMF [10]. Figure 3 shows the relationships of the CMF elements.

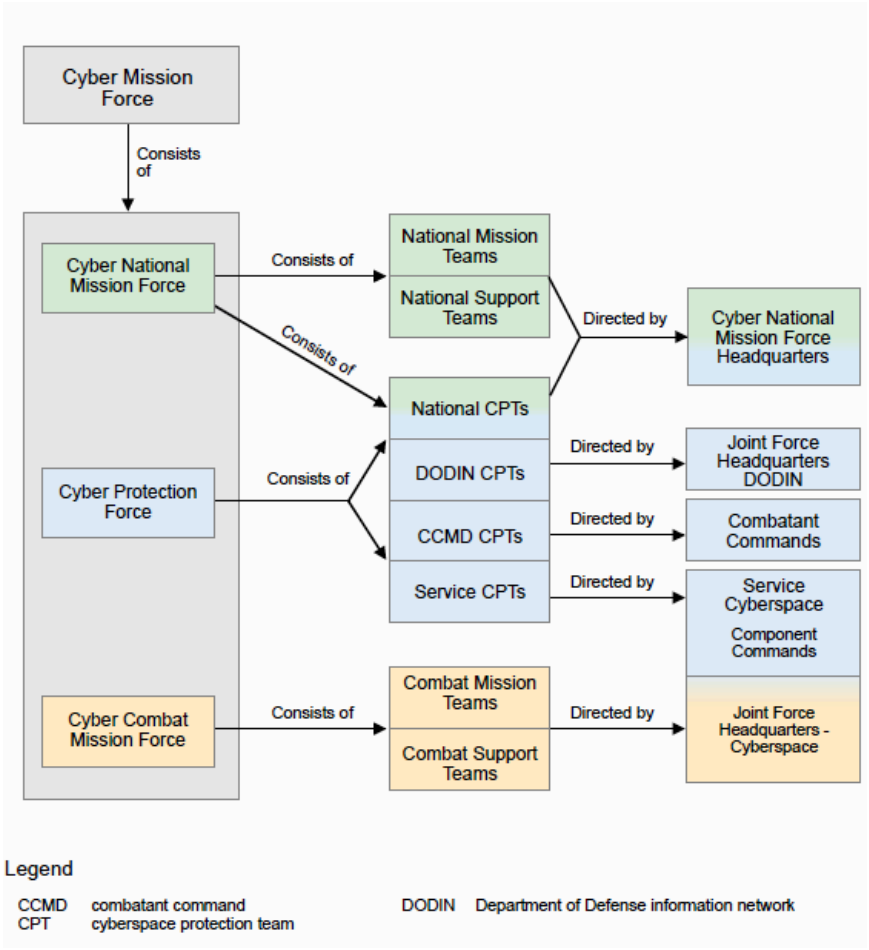

Figure 3. DoD Cyber Mission Forces Relationships. Source: [10].

The integration of the CMF to military operations allows commanders to extend their capabilities globally and in theater-level or joint operations [10]. Based on JP-3–12, commanders should effectively address the integration of the cyberspace capabilities that are provided by the CMF into the planning, coordination and execution of military operations. Additionally, the CMF structure provides commanders constant and detailed coordination between strategic, operational and tactical levels and can be adapted to the constant changes and emerging risks [10].

c. Cyberspace Security

From JP-3–12, "cyberspace security are actions taken in order to prevent unauthorized access to, exploitation of, or damage to computers, electronic

communications systems, and other IT, including PIT [platform information technology], as well as the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation" [10]. While "cyberspace security" is the term used in JP-3–12, the DoD adopts the term "cybersecurity" from the National Directive-54/Homeland Security Presidential Directive-23 [12], [13]. Cybersecurity is employed to reduce potential exploitation of military IT, hence the term can be associated with cyber risk when developing military plans and operations at all levels.

The criticality of IT for military operations, planning and execution across the DoD and across all levels of commands makes imperative the consideration of cybersecurity risks across all levels in the DoD [12]. The unique characteristics of the cyberspace domain are such that even tactical-level vulnerabilities can present a strategic risk. Adversaries seek to exploit cyberspace to obtain political, economic and military strategic advantage over the United States [14]. These advantages can be used by adversaries to compromise critical infrastructure, military networks, and to deteriorate international political relations [14]. Moreover, the constant exposure of inherent vulnerabilities from IT systems and the risk of compromising DoD military operational capabilities require a continual risk assessment process, that will enable commanders to manage the revolving risk.

Taking into consideration the potential impact of the cybersecurity risk to the DoD mission, the DoD has promulgated strategies, policies and directives that are intended to assist commanders to defend the U.S. and its interests in cyberspace [14].

B. STRATEGY

The DoD strategy for military operations in cyberspace defines and prioritizes a set of goals to support strategic-level objectives. These goals allow the DoD to assign specific objectives to each of the levels of war and develop policies to support CO in this domain.

The initial DoD Cyber Strategy was released on April 2015. Its intent was to provide a comprehensive strategy for DoD leaders. It focused on CO assessment and cyberspace capabilities development. As the DoD's CMF reached full operational

capability (FOC) on May 2018, the DoD aimed to set specific objectives to guide the CMF to strengthen their cyber defense and deterrence posture. While this strategy was built on the DoD Strategy for Operating in Cyberspace of May 2011, it introduced strategic objectives to build cyber capabilities beyond FOC to improve cybersecurity and enable effective CO [14].

The 2018 DoD Cyber Strategy superseded the 2015 DoD Cyber Strategy. The new strategy focuses on strengthening cyber capabilities and conducting CO against U.S. strategic threats, mainly China and Russia [15]. The strategy focuses on strategic competition in cyberspace and develops five objectives to defend national interests and promote a culture of cybersecurity across the department [15]. According to the strategy:

> These objectives ensure the Joint Force can achieve its missions in a contested cyberspace environment; strengthen the Joint Force by conducting cyberspace operations that enhance U.S. military advantages; defending U.S. critical infrastructure from malicious cyber activity that alone, or as part of a campaign, could cause a significant cyber incident; secure DoD information and systems against malicious cyber activity, including DoD information on non-DoD-owned networks; and expand DoD cyber cooperation with interagency, industry, and international partners. [15]

C. POLICIES

DoD cybersecurity policies define how the department manages and assess risks associated to operations in the cyberspace domain. The department uses a multi-tiered risk management structure and guidance to provide a risk management framework (RMF) to manage the risks associated to operations in cyberspace.

The DoD Chief Information Officer establishes the department's cybersecurity program using Department of Defense Instruction (DoDI) 8500.01. In accordance with this instruction, the DoD instituted its policy for the CRM process, standards and procedures associated with information security and defense and the integration of cybersecurity at all levels across the department [12].

The DoDI 8500.01 instructs the department to use a multi-layered risk management process based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800–39 and NIST SP 80-37 as shown in Figure 4 [16], [17].

Additionally, to ensure that cybersecurity is incorporated throughout the IT life cycle, the DoD coordinates with the Under Secretary of Defense for Acquisition, Technology and Logistics [12]. This coordination ensures that cybersecurity and risk assessment happen as early as possible during the acquisition process. Furthermore, that they are also integrated into the acquisition planning, testing and evaluation process.

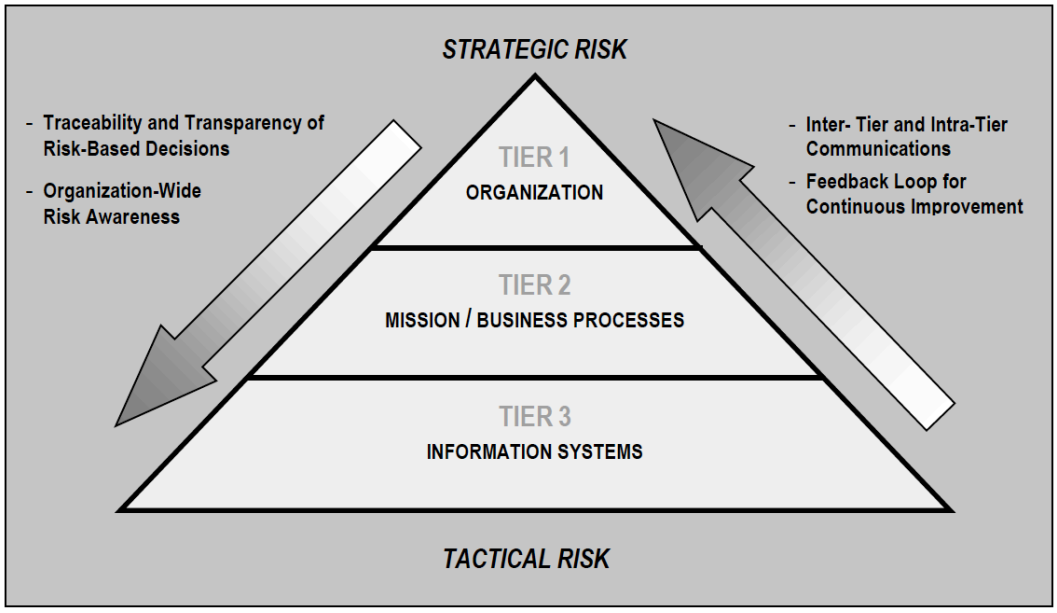

Figure 4. Multi-tiered Approach to Cybersecurity Risk Management. Source: [16].

Additionally, the DoDI 8500.01 establishes the foundational guidance and directions for an effective CRM across the DoD [12].

a. Management of Risk Based on Policy

The multi-tiered risk management approach described in the DoDI 8500.01 as the DoD RMF describes how the DoD will manage and assess cybersecurity risks concerns based on the organization levels [12]. In the RMF, the risks at each tier are communicated and managed by decisions made at the other tiers to ensure tactical, operational and strategic cybersecurity risks are communicated, assessed and managed

across all levels. This RMF should allow commanders at all levels to maintain a clear view of risk decisions and awareness of cybersecurity risks in their AO [12].

In March 2012, the DoD officially replaced the Defense Information Assurance (IA) Certification and Accreditation Process with the RMF as directed by DoDI 8510.01. This instruction describes the RMF as an "enterprise-wide decision structure for cybersecurity risk management that includes and integrates DoD mission areas" [18]. Also, the DoDI 8510.01 identifies the responsibilities and authorities assigned to DoD agencies as shown in Figure 5 [18]. This structure shows a hierarchical organization attempt to ensure that cybersecurity risks are considered and communicated at all levels with the participation of the responsible DoD agencies.

Each tier has specific roles and responsibilities in the RMF. Tier 1 provides coordination and deconflictions [18]. Tier 2 administrates the DoD Component RMF program, and Tier 3 is responsible for accountability of the RMF at the tactical-level [18].

Figure 5. Risk Management Framework Governance. Source: [18].

In addition, DoDI 8510.01 provides a six-step RMF process for IT that incorporates the DoD Acquisition Management Process into the RMF as shown in

Figure 6 [18]. These steps are designed to support and complement the DoD Acquisition Management Process to allow risk management activities to start as early as possible in systems life cycle [18].

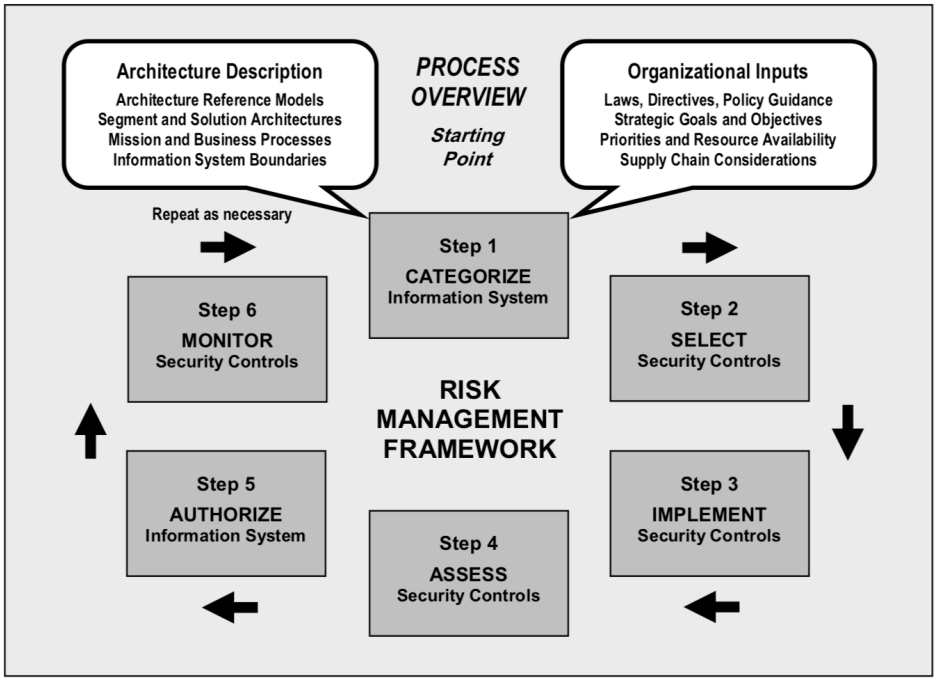

Figure 6. RMF Steps. Source: [17].

b. Risk assessment Based on Policy

To assess cybersecurity risks, the DoD references NIST Guide for Conducting Risk Assessment (NIST SP 300-30). As shown in Figure 7, this risk assessment process presents a framework to assess, respond to, and monitor cybersecurity risks. The assessment should allow the DoD's organizations to determine the cybersecurity risk based on the identification of threats and vulnerabilities [19].

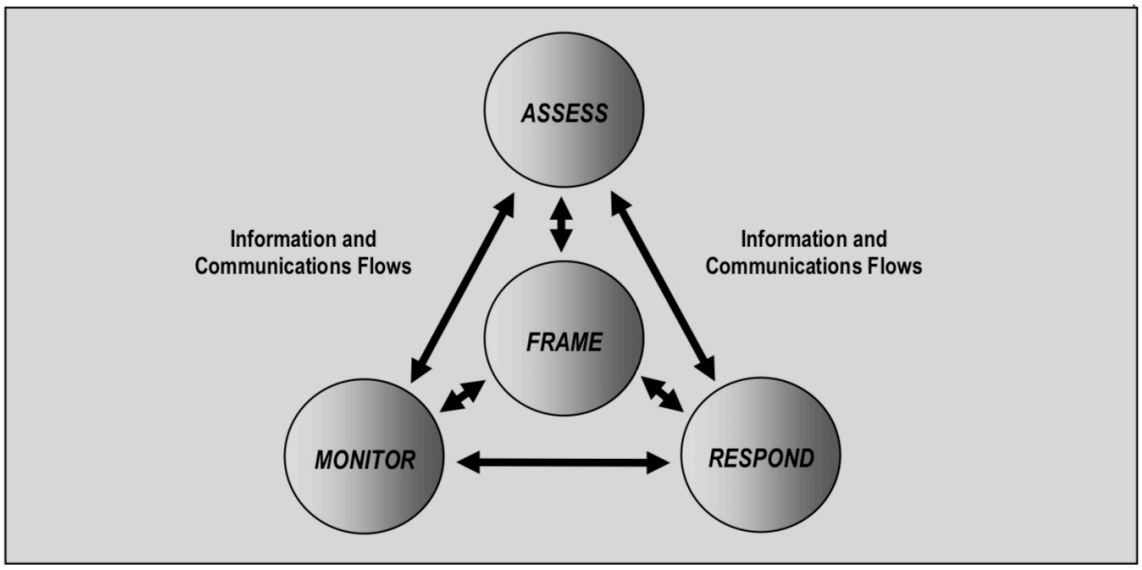

Figure 7. Risk Assessment within the Risk Management Process. Source: [19].

D. CONDUCT OF RISK ASSESSMENT

The NIST provides various publications describing how to manage and assess risk associated with information management. In addition, NIST provides a guide on how to apply the RMF to federal information systems (IS). This guide provides cybersecurity standards and technical best practice applications. Because these publications encompass a variety of best security practices that allow the U.S. to continually enhance cybersecurity capabilities against current and future cyber threats, the DoD has directed their use in its cybersecurity policy [12].

a. Managing Information Security Risk (NIST SP 800-39)

NIST SP 800-39 presents the fundamental concepts associated with information security risk management. It describes risk management as "a comprehensive process that requires organizations to: frame the risk, assess the risk and respond to the risk" [16]. Figure 7 shows the requirements of the risk management process as described by NIST SP 800-39 and also highlights that risk management is executed as an organization-wide activity that ensures every level of the organization—tactical, operational and strategic—are integrated into risk management [16].

The risk management processes presented in this publication provide ideas on how to conceptualize the environment where risk-based decisions are made in order to frame the risks. It provides strategies to identify appropriate risk assessment tools, techniques and methodologies and the means to monitor risk over time based on threat and vulnerability assessments [16]. Additionally, this publication emphasizes bidirectional communication among all levels of an organization as an effective way to maintain a flexible and dynamic risk management process [16].

To ensure that the risk management process is included throughout all levels in an organization, the NIST SP 800-39 proposes a three-tiered approach as shown in Figure 4. At every tier, components of fundamental risk management concepts are applied.

(1) Tier 1

Tier 1 provides the strategic-level objectives of the organization and provides the other tiers with the context of risks that are carried out through the organization [16]. In the context of strategic-level risk management, NIST suggests that organizations at this tier aggregate all the risks associated with IS at the operational and tactical-levels to provide a better understanding of the risks associated with IS at the strategic-level operations [16].

(2) Tier 2

Tier 2 translates the risk context provided by the Tier 1 to process and prioritizes missions associated to the strategic goals and objectives. Also, it identifies types of information and the criticality/sensitivity and establishes the security architecture to protect the information [16].

(3) Tier 3

Tier 3 addresses decisions and activities associated with risks from the other tiers [16]. It also provides feedback to the other two tiers. Furthermore, it ensures any additional vulnerabilities and risks to the organizations are included for risk consideration at the other two tiers [16]. Another consideration NIST suggests for this tier is that day-to-day operations of IS may translate to risk management at the operational-level. Based

on the NIST SP 800-39, “authorizing officials make follow-on risk-based decisions on whether or not the IS are initially authorized to operate within the designated environments of operation or continue to receive authorization to operate on an ongoing basis” [16].

Figure 8 shows how the risk management process is included at all levels of an organization.

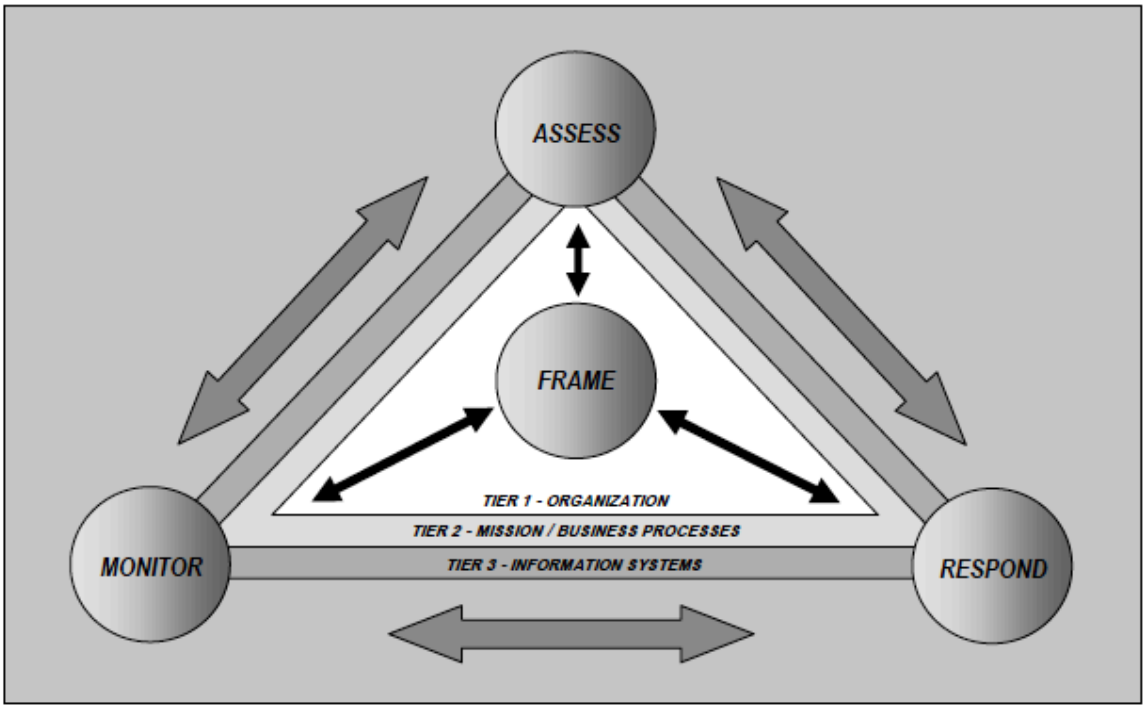

Figure 8. Risk Management Process Applied across the Three Tiers. Source: [16].

b. Guide for Applying the Risk Management Framework to Federal Information Systems (NIST SP 800-37)

The NIST SP 800-37 presents the same fundamental concepts presented in NIST 800–39. This publication combines the fundamental concepts of IS risk management and provides guidance on how to apply the RMF. The implementation of the RMF is described in six steps shown in Figure 6: “1) Categorize IS, 2) select security controls, 3) implement security controls, 4) assess security controls, 5) authorize security controls,

and 6) monitor security controls" [17]. NIST defines tasks under each of these six steps that are to be executed with well-defined organizational roles [17]. This ensures that organizations identify and task specific roles in support of the organization's RMF and that accountability is maintained across all levels in the organization.

c. Guide for Conducting Risk Assessments (NIST SP 800-30)

NIST SP 800-30 provides a four-step process for assessing information security risks as shown in Figure 9 [19]. The risk assessment process is correlated to the same risk management fundamentals presented in NIST SP 800-37 and NIST SP 800-39 that are referred in the DoD Cybersecurity Directive.

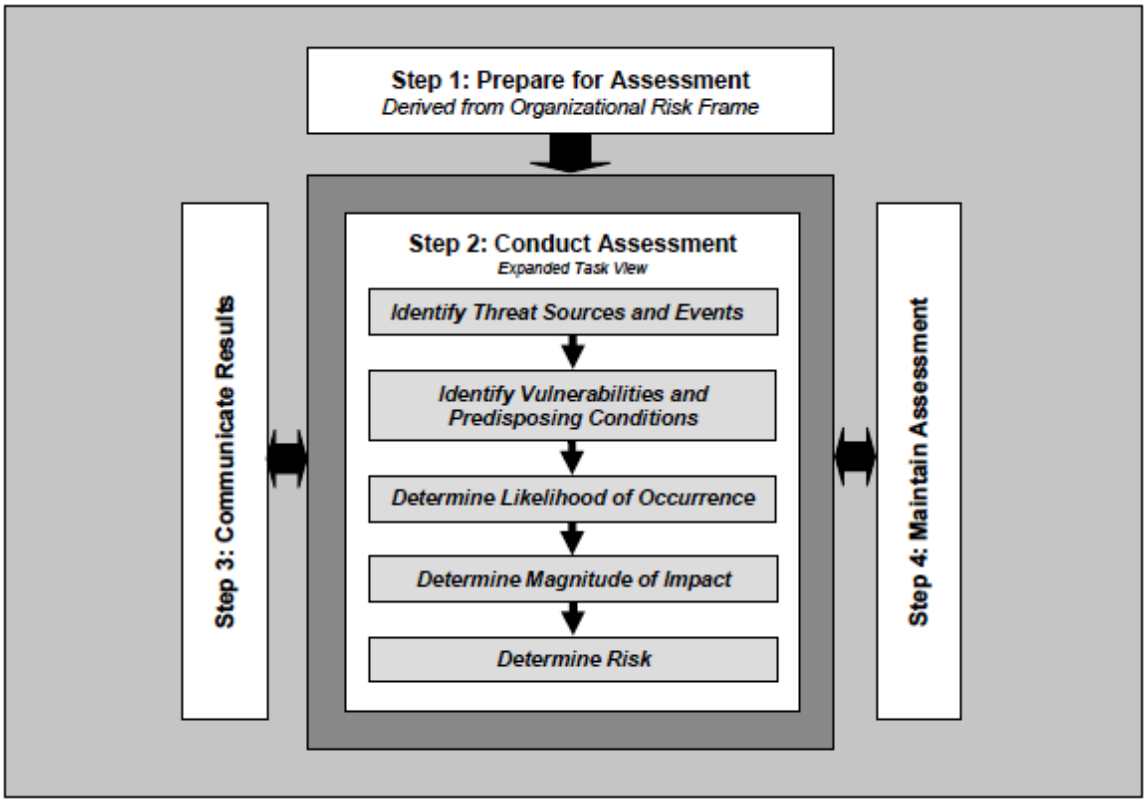

Figure 9. Risk Assessment Process. Source: [19].

Based on this publication, every step has specific tasks that can be summarized within the key activities: "Identify key risk factors that have been identified for ongoing monitoring, identify the frequency of risk factor monitoring activities and the circumstances under which the risk assessment needs to be updated, reconfirm the purpose, scope, and assumptions of the risk assessment, conduct the appropriate risk assessment tasks, as needed and communicate the subsequent risk assessment results to specified organizational personnel" [19]. Because differences exist in every organization, these steps are flexible and only provide an abstract process that may have implementation variations depending on the objectives of each organization.

E. SIMILAR PROCESSES

Cybersecurity requirements are extended to acquisition programs. The DoD has released two guidebooks to incorporate cybersecurity throughout the acquisition life cycle. However, the complexity of threats and risks in cyberspace domain makes it difficult to develop a specific cybersecurity framework that will work for all organizations inside or outside the DoD.

1. Cybersecurity for DoD Acquisition Programs

The DoD Program Manager's Guidebook for Integrating the Cybersecurity RMF into the System Acquisition Life cycle focuses on integrating cybersecurity into the DoD's acquisition programs [20]. By defining cybersecurity management roles, fundamental concepts and activities, this guidebook allows program managers to implement the RMF in the acquisition life cycle [20], including "acquisition, design, development, developmental testing, operational testing, integration, implementation, operation, upgrade, or replacement of all DoD IT supporting DoD tasks and missions" [12]. This guidebook includes the cybersecurity requirements for commercial products.

Based on this guidebook, all "Commercial-off-the-shelf (COTS) cybersecurity products and cybersecurity-enabled products should be certified compliant with Committee on National Security Systems Policy 11, National Policy Governing the Acquisition IA and IA-Enabled Information Technology Products" [20]. In addition to

this guidebook, in April 2018 the DoD released the DoD Cybersecurity Test and Evaluation (T&E) Guidebook. Figure 10 shows how the guide aligns the acquisition life cycle and the RMF to six cybersecurity T&E activities for DoD acquisitions programs [21]. The activities are progressive and ensure consideration of cyber-related risks are being considered, evaluated and mitigated throughout the acquisition life cycle [12].

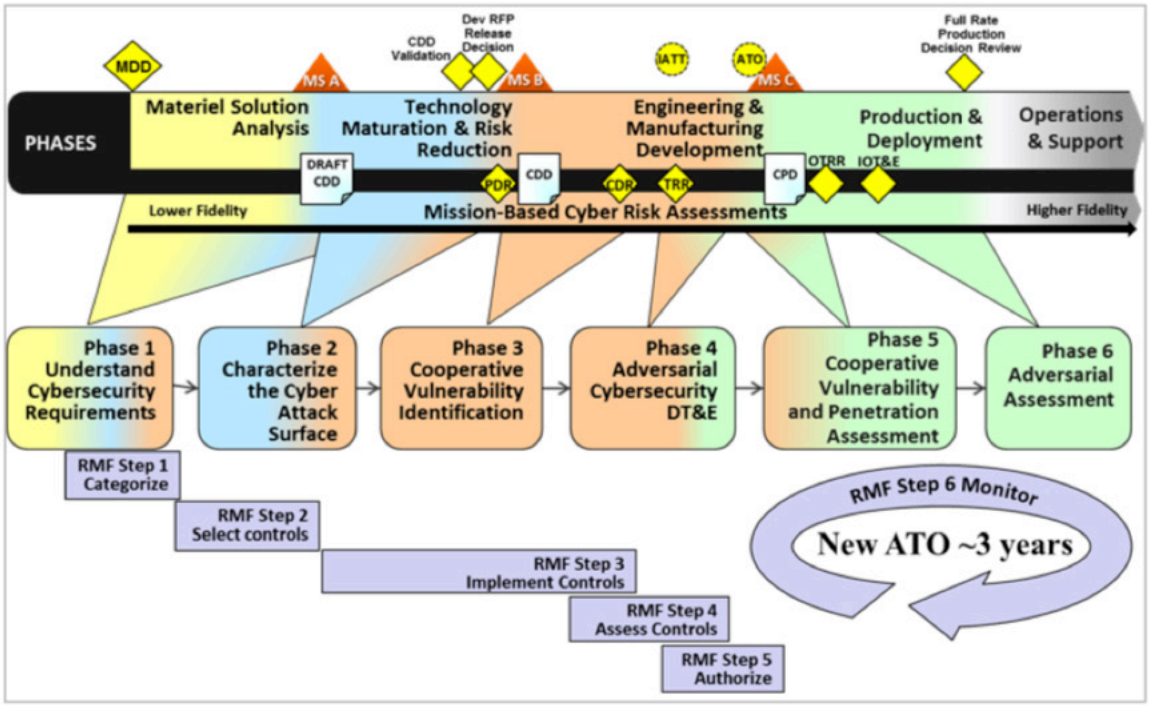

Figure 10. Cybersecurity T&E Phases and the Acquisitions Life Cycle. Source: [21].

2. Framework for Improving Critical Infrastructure Cybersecurity

Like the DoD, DHS refers to NIST publications to define their cybersecurity risk assessment frameworks. The DHS uses the Framework for Improving Critical Infrastructure Cybersecurity developed by NIST in 2014 [22] to assess and manage cybersecurity risk associated with critical infrastructure [23]. The framework is employed by the Critical Infrastructure Cyber Community Voluntary Program. This program, provides private and public sector best practices, maintains collaboration and improves

cyber risk management for some very different organizations such as healthcare and public health, emergency services, commercial businesses, critical manufacturing and transportation systems, etc. [23].

The fundamental guidelines for this framework consist of five functional areas: "Identify, Protect, Detect, Respond, and Recover" [22], [23]. These functional areas allow the DHS to incorporate the fundamental principles from the NIST publications. Also, they provide common frameworks for different organizations' cybersecurity needs based on the same fundamental cybersecurity principles.

F. GAPS

While the DoD's publications define and establish the strategy, policies and cybersecurity requirements for military operations in the cyberspace domain, none of these publications specifically address COTS UAS or cyber physical systems in general. Nor do they define specific requirements for COTS UAS operations. As indicated by the May 2018 ban, and subsequent waiver process, the Secretary of Defense determined that these COTS UAS posed a unique cybersecurity risk. Additionally, the requirement for waivers to originate at the tactical (operator) level and be approved by the third highest (strategic) member in the DoD demonstrates the need for an efficient mechanism to communicate cybersecurity risk across multiple echelons within the DoD Services.

III. PROPOSED CYBERSECURITY RISK MANAGEMENT (CRM) PROCESS FOR COTS UAS

This chapter introduces a process to apply CRM to COTS UAS. It also uses the RMF discussed in Chapter II to derive a CRM process for COTS UAS operations. The proposed framework includes a new process to communicate relevant cybersecurity risks effectively across multiple echelons for COTS UAS operations in any AOR. This process is intended to provide the commanders a better understanding of the cybersecurity risks associated with the COTS UAS technology.

A. MODEL APPROACH

This approach follows the Joint Risk Analysis Methodology (JRAM). The JRAM is a manual that provides guidance to manage risk for the Joint Forces. The approach considers a cyclical communication process paired with the current DoD multi-tiered risk management process—frame, assess, response, monitor—combining CRM with strategic risk and risk-to-mission assessments to enable risk assessment across multiple echelons [16], [24]. As shown in Figure 11, this approach centers on communicating elements of risks across multiple command levels to determine if cybersecurity risks associated with COTS UAS operations in a specific AOR are acceptable. The CRM approach considers three important components of the CRM process as they might apply COTS UAS operations in an AOR: strategic objectives, strategic risk and risk-to-mission. Considering risks in the context of strategic objectives and characteristics of the cyber threat gives commanders a better understanding of the cybersecurity risk associated with COTS UAS operations. Moreover, this approach facilitates continuous data gathering and comprehension of the risks, including future emerging cybersecurity risks, across multiple levels (Figure 12) [24].

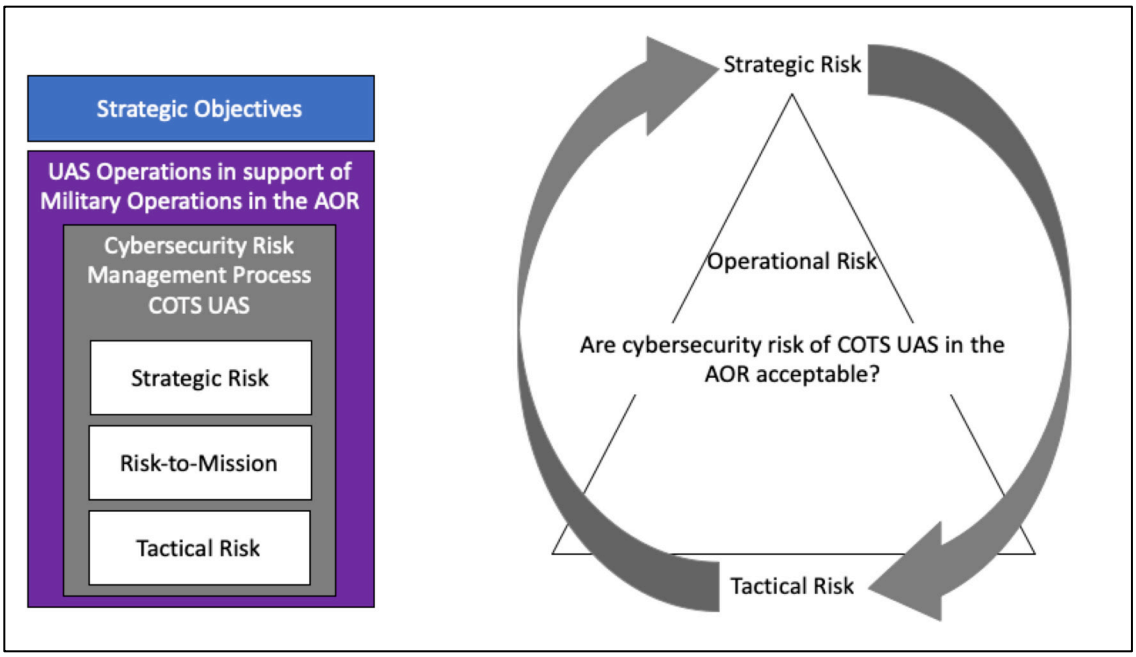

Figure 11. Proposed CRM process for COTS UAS Approach.

B. CRM PROCESS MODEL

The JRAM framework will be adapted to create a CRM for COTS UAS [24] The proposed CRM process for COTS UAS combines the four major steps from the JRAM framework [24], shown with gray stars in Figure 12, and seven steps from the strategic risk business management process developed by Frigo and Anderson [25]. The combination of these steps is intended to allow commanders to incorporate the proposed process as part of any military operations planning process where COTS UAS operations play a significant role for missions in the AOR [24]. It is expected that this will ensure that commanders consider elements of strategic risk as part of the overall military operations risk assessment [24].

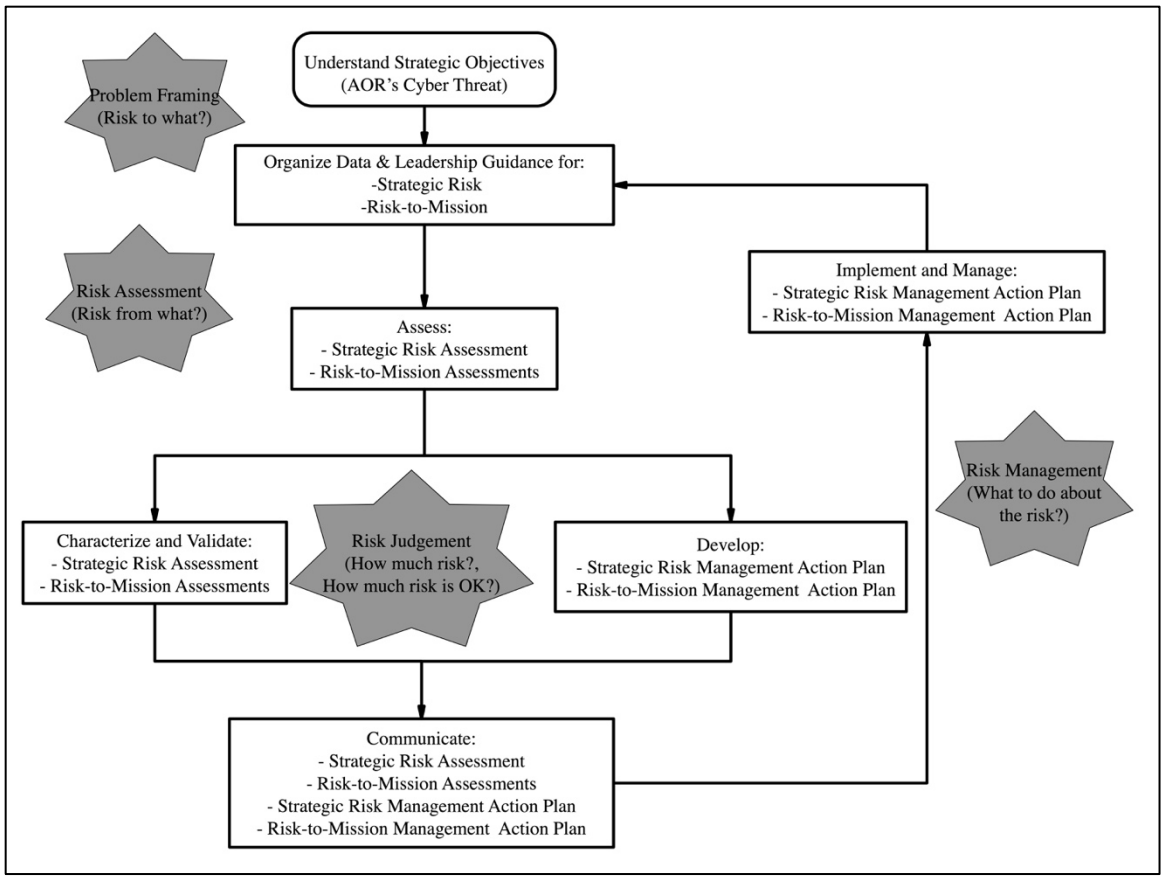

Figure 12. Proposed CRM process for COTS UAS. Adapted from [24], [25].

For the proposed CRM for UAS process, national priorities and the DoD's strategic objectives in the cyber domain provide the elements of risk that drive the AOR's strategic objectives. For example, the following notional risk equation shows an example of relevant elements of cybersecurity risk—threats, vulnerabilities, impact and security controls—that can be used with the CRM process to communicate across multiple echelons and to assess risk [26]:

$$Risk = Threats\ x\ Impact\ x\ \frac{Vulnerabilities}{Security\ Controls}$$

Problem framing considers the AOR's cyber threat and its potential impact to the military operations in the AOR. For example, if a strategic objective regarding the Chinese cyber threat in the AOR is considered, then the strategic risk assessment and the

risk-to-mission assessment will reflect elements of cybersecurity risk related to Chinese made technology in COTS UAS. In this case, the assessment also considers the Chinese adversarial characteristics which allow the commander to assess and determine the potential impact to the strategic, operational and tactical objectives. The information can then be used to identify the sources of risk, determine potential impact in the AOR, and is also used to conduct the strategic risk and the risk-to-mission assessments.

The strategic risk assessment focuses on the potential impact of the AOR's cyber threat to the strategic objectives. The risk-to-mission assessment is a subset of the operational risk. It focuses on identifying and assessing the elements of risk associated to UAS operations in support of tactical missions. This assessment reflects the ability of the tactical-level military operations to achieve their objectives without UAS support. The risk-to-mission assessment combines all the tactical units' mission risks to reflect the overall impact on operations at the operational-level. This allows the strategic, operational and tactical commanders to understand and communicate how the cybersecurity risks connected to UAS operations might affect operations in their AOR.

In addition, this proposed CRM process allows organizations to integrate additional comprehensive cybersecurity risk assessments as subsets of either of the two proposed risk assessments included in this model. For example, a cybersecurity risk assessment that focuses on assessing risks associated with IT system components, such as UAS avionics computer and radio components, can be included as a subset of the risk-to-mission risk assessment. This assessment will provide additional understanding of the cybersecurity risk in terms of vulnerabilities. Also, it provides the potential to establish security controls to minimize or eradicate the potential vulnerability and reduce the risk.

The purpose of this model is to allow leaders to make informed decisions regarding COTS UAS operations in any AOR. This model combines elements of risk from the strategic and tactical levels in a series of steps, that provides consistent comprehension of cybersecurity risks across all levels in the AOR. These steps are defined below by incorporating RMF and the strategic risk business management process steps with the major steps from the JRAM.

C. CYBER RISK MANAGEMENT PROCESS STEPS

The CRM process steps, illustrated as the four stars in Figure 12, are "activities used to assess risk comprehensively" [24]. These activities provide a consistent way to manage the CRMP and ensure the process is practical. They are discussed in this section.

1. Problem Framing

This step begins by understanding the strategic objectives and the cyber threat characteristics in the AOR. The strategic objectives provide the elements of cybersecurity of national and strategic concerns that incorporate the leadership's guidance in the AOR. The focus is for leaders to categorize and communicate the threat and the impact elements of the risk equation, that are associated with the two types of assessments—strategic risk and risk-to-mission—and to be able to communicate and provide leadership guidance in the AOR. Once the elements of cybersecurity risk are identified, the data is organized prior to conducting the risk assessments. The data gathering can be done by considering information already available or by other methods such as leadership interviews, surveys, working groups, or current operations assessments of a cyber adversary [25].

The characteristics of the cyber threat are defined based on the adversary's capabilities, intent and targeting (access) capability. The characteristics of the cyber threat capabilities defines the adversary's level of expertise, resources availability, and its chances to "support multiple successful, continuous, and coordinated attacks" in the AOR [19]. The cyber threat intent defines the level to which the adversary intends to impact the military mission objectives, IT systems and any military supporting infrastructure in the AOR [19]. The cyber threat's targeting characteristics define the methods used by the adversary to execute the attacks. For example, in an AOR a cyber threat can be describe as a sophisticated cyber expert, well-resourced, with a purpose to disrupt multiple organization's cyber resources by executing persistent attacks, and with access to possibly critical information [19].

2. Risk Assessment

The information gathered during the problem framing step helps to create the strategic and risk-to-mission risk profiles based on the cybersecurity risk elements from the risk equation [26]. While the details and complexity of the cybersecurity risk assessment may vary depending on the organization's needs and their standard operating procedures (SOPs). The basic framework is intended to help the organization focus on the strategic and risk-to-mission assessments needed to create and validate an action plan. The contributors of the risk assessments are encouraged to provide the elements of risks they believe will affect strategic-level objectives and the ability to achieve operational-level and tactical-level objectives [25]. Moreover, they should also assess the potential impact of the identified risk [25].

a. Strategic Risk

The CJCSM 3105.01 is the Joint Staff risk reference that provides a risk management methodology to the Joint Force commanders "to make consistent, timely risk assessments and provide best military advice in support of military operations" [24]. Based on CJCSM 3105.01, strategic risk "is the potential impact upon the United States-including the U.S. population, territory, civil society, critical infrastructure, and interests - of current and contingency events given their estimated consequences and probabilities" [24]. As shown in Figure 13, the probabilities and consequences will allow a decision maker to determine if the risk is acceptable and determine whether to accept, avoid, reduce or transfer elements of the risk. [24].

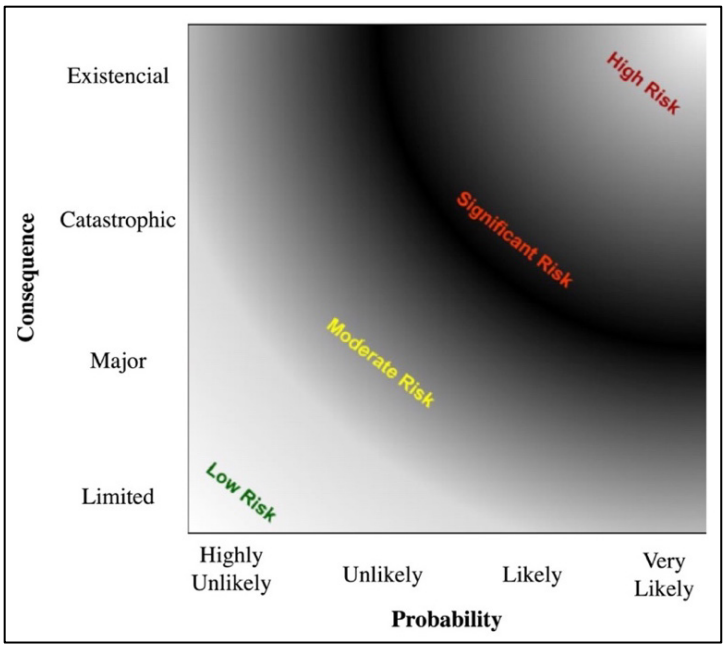

Figure 13. Strategic Risk Contour. Source: [24].

Table 1 provides the definition of the four consequences of the strategic risk assessment illustrated in Figure 13.

Table 1. Strategic Risk Table. Source: [24].

Consequence of Event (C)
Limited: Confined damage to strategic objectives
Major: Considerable damage to strategic objectives
Catastrophic: High order damage to strategic objectives
Existential: Permanent damage to strategic objectives

b. Risk-to-Mission

Risk-to-mission assessment has four probabilities—highly unlikely, unlikely, likely and very likely— and four consequences—can fully achieve all objectives, can achieve all critical objectives, can achieve only most critical objectives and potential failure/cannot achieve critical objectives— that reflect the ability of the tactical forces to achieve their mission objectives [24]. The risk-to-mission contour shown in Figure 14

allows a decision maker to determine if the risk is going to be accepted, avoided, reduced or transferred [16], [24].

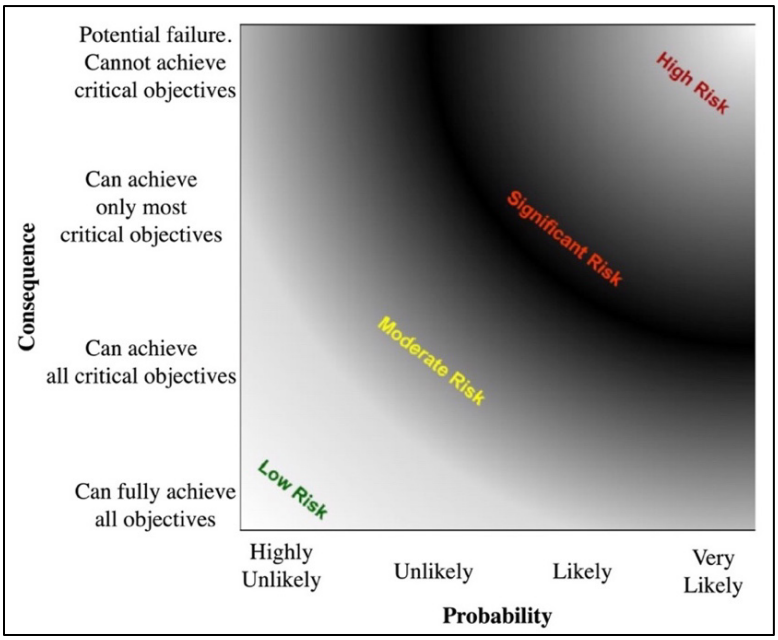

Figure 14. Risk-to-Mission Contour. Adapted from [24].

3. Risk Judgement

This step begins with the validation of the assessments and development of the management action plans for the strategic risk and risk-to-mission. In this step, a decision maker gathers the initial risk assessments and validates them by confirming they reflect the most critical risks to strategic direction and tactical mission. Also, in this step a decision maker verifies that management action plans are developed as a fundamental part of the risk assessments. The decision maker ensures completeness of the risk management action plans to ensure that security controls, activities and plans to reduce some of the risks are identified [25]. Additionally, the decision maker confirms that risk management action plans are monitored periodically to update the strategic risk and risk-to-mission assessments [25].

4. Risk Management

This step incorporates the resulting actions of the previous' steps with the elements of cybersecurity risk from the strategic and tactical levels. The actions focus on maintaining a continuous CRM process that allows leaders to make better-informed decisions regarding COTS UAS operations. It brings together elements of risk from the strategic and tactical levels to allow timely and consistent comprehension of cybersecurity risks related to COTS UAS. The cyclical communication process allows commanders across all levels to frame, assess, judge and manage the risk associated with COTS UAS operations and the cyber threat in their AOR. Moreover, the cyclical communication process allows leaders to continually assess new and emerging cybersecurity risks in their AOR and to update current assessments associated with COTS UAS.

The integrated risk matrix shown in Table 2 is a tool proposed by the JRAM to visualize the combined aspects risk [24]. This tool can be used with the proposed CRM process to communicate cybersecurity information such as cyber threat characteristics, risk assessments, and risk management action plan [24]. CRM process permits commanders at all echelons to develop a "big picture" of the overall risk assessment with their use of COTS UAS in their AOR [24]. This can be demonstrated in a hypothetical scenario that demonstrates how CRM provides increased awareness of the cybersecurity risks and the potential impact to military operations in the AOR.

Table 2. Integrated Risk Matrix. Adapted from [24].

Event Title:						
Purpose:						
Cyber Threat Characteristics:						
Assessments						
Risk	**Criteria**	**Low**	**Moderate**	**Significant**	**High**	**Overall Risk**
Strategic Risk	Probability of Event	Highly Unlikely (~0-20%)	Unlikely (~21-50%)	Likely (~51-80%)	Very Likely (~81-100%)	
	Consequence of Event	Limited: Confined damage to strategic objectives	Major: Considerable, damage to strategic objectives	Catastrophic: High order damage to strategic objectives	Existential: Permanent damage to strategic objectives	
Strategic Risk Notes:						
Risk-to-Mission	Probability of Event	Highly Unlikely (~0-20%)	Unlikely (~21-50%)	Likely (~51-80%)	Very Likely (~81-100%)	
	Consequence of Event	Can fully achieve all objectives	Can achieve all critical objectives	Can achieve only most critical objectives	Potential failure. Cannot achieve critical objectives	
Risk-to-Mission Notes:						
Overall Risk Assessment:						
Action Plan						
Risk Management Mitigation Plan:						

IV. APPLICATION OF THE CYBERSECURITY RISK MANAGEMENT (CRM) PROCESS

This chapter applies the proposed CRM process discussed in Chapter III to a hypothetical scenario to demonstrate how the CRM process can be used by organizations to communicate relevant cybersecurity risks across strategic, operational and tactical levels to determine the risk of COTS UAS operations. The scenario is focused on UAS operations where elements of the risk can be communicated to determine the overall risk imposed by a cyber threat. Additionally, it provides information regarding the potential impact to UAS operations without exposing low echelons to highly classified information.

The same cyber threat can introduce different cybersecurity risk in the AOR, this chapter (and thesis) focuses exclusively on the impact of the cyber threat to COTS UAS operations. Additionally, this scenario incorporates a UAS cybersecurity risk assessment methodology [27] to demonstrate how cybersecurity risk assessments that consider all elements of the risk equation, vulnerabilities and security controls, can be incorporated into the CRM process. Although many other factors such as weather, platform characteristics and sensor limitations can affect UAS operations, this scenario only addresses developing assessments to cyber threats.

A. SCENARIO

Imagine an AOR organized as shown in Figure 15. It is composed of a strategic-level command and two operational commands supported by five tactical-level commands. The strategic objectives in this AOR aim to defend the national interest by deterring and defeating any adversarial aggression, operating effectively in cyberspace, and reducing risks to the operating forces in the AOR.

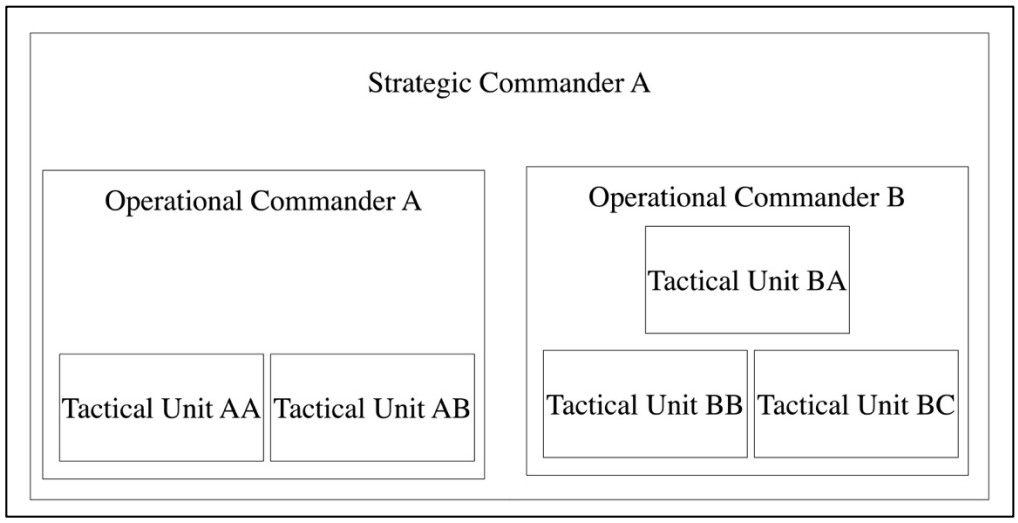

Figure 15. AOR Organization.

The threats in this AOR disrupt freedom of operations in cyberspace and increase violent extremists' activities have been identified. The extremist groups are organized in small cells operating from multiple areas across the AOR. The cyber threat is characterized as a mid-level nation state cyber actor with a sophisticated understanding of advanced penetration techniques. It is well-resourced, able to replicate and execute hacking examples found online, and intends to conduct cyber espionage and disrupt key resources across the AOR.

The organizations that supports Strategic Commander A's objectives are Operational Commander A and Operational Commander B. Each operational command fights in a different domain to support Strategic Commander A's fight against the AOR's threat in all domains. Operational Commander A is responsible for protecting freedom of maneuver throughout cyberspace from adversarial disruption. Operational Commander B is responsible for detecting and deterring violent extremists' activities. There are five tactical-level commands: Tactical Unit AA, Tactical Unit AB, Tactical Unit BA, Tactical Unit BB and Tactical Unit BC. Tactical Unit AA provides intelligence support capabilities and Tactical Unit AB provides cyber OCO capabilities in support of Operational Commander A. Tactical Unit BA and Tactical Unit BB provide intelligence, surveillance, and reconnaissance (ISR) support to multiple units in the AOR deploying

different UAS types. Tactical Unit BC provides combat and counter improvised explosive device capabilities to Operational Commander B.

While the operational commands (A and B) fight in different domains, the AOR's cyber threat poses a risk to both operational commands. Therefore, communication and synchronization from the Strategic Commander A allows the two operational commands to align objectives that support all the strategic objectives against the AOR's cyber threat.

B. APPLYING CRM PROCESS

1. Problem Framing

The initial step is to frame the problem. For this scenario, the AOR's strategic objectives and the leadership guidance frame the problem, with emphasis on the cyber threat and its impact to UAS operations in the AOR. The leadership guidance is focused on understanding how this cyber threat impacts military objectives that are mainly supported by UAS. The strategic-level command organizes the information along with the characteristics of the cyber threat. It then relays the information to the operational and tactical level, which is shown in Table 3.

Table 3. Scenario Problem Framing.

Event Title: Cyber Threat Impact to UAS Operations
Purpose: Determine the impact of the AOR's cyber threat to UAS operations.
Cyber Threat Characteristics: Mid-level nation state cyber actor that has sophisticated understanding of advanced penetration techniques, is well-resourced, is capable of replicating and executing hacking examples found, and intends to conduct cyber espionage and disrupt multiple organizations' key resources.

The CRM process focuses on assessing strategic risk and risk-to-mission based on impact to mission objectives. This information can also be used in conjunction with the risk equation to gather additional information. Furthermore, it can incorporate other elements of risk such as vulnerabilities to control systems. For example, in addition to the strategic risk and risk-to-mission, if the operation is incorporating cybersecurity risk assessments from equipment operators at the tactical-level, more specific variables will

be incorporated to better assess the overall cybersecurity risk, such as the UAS operators' cybersecurity risk assessment [27]. Likewise, additional components of risk can be added in when calculating risk, depending on the situation and capabilities being used to conduct military operations. Also, this information is being evaluated at different layers before the strategic risk and risk-to-mission assessments are completed. This increases each commander's confidence in the CRM process. In addition, it provides commanders a better understanding of how cybersecurity risk assessment translates to overall risk of military operations.

2. Risk Assessments

The next step is to conduct the risk assessments. The first assessment considered is the UAS operators' cybersecurity risk assessment [27]. These assessments consider all elements of the risk equation and determine the overall cybersecurity risks determined by the UAS operators as shown in Table 4 [27].

Table 4. UAS Operator's Cybersecurity Risk Assessment. Adapted from [27].

Assessment	Overall Risk	Notes
Tactical Unit BA (Drone-A)	Moderate	Requested platform despite higher threat assessment due to optical camera quality and increased endurance.
Tactical Unit BB (Drone-B)	Low	Requested as a secondary platform if Drone-A risk is not acceptable to the overall mission.

Using the information from these assessments, the operational commands assess the risk-to-mission given the impact to the military objectives supported by UAS operations. Considering the overall risk for Tactical Unit BA mission is moderate, the Operational Commander B determines that 50% of the critical objectives supported by UAS operations are at risk from the cyber threat, resulting in an overall risk-to-mission of moderate. Similarly, the Operational Commander A determines that this threat has no

impact to their critical objective in terms of UAS operations because they do not use UAS, resulting in an overall low risk-to-mission.

Using the risk-to-mission assessments from the operational-level, the strategic risk assessment determines that cybersecurity risk associated to UAS operations in the AOR have a highly unlikely probability of occurrence. As a result, it would inflict limited damage to the strategic objectives, resulting in an overall low strategic risk. The next step is to communicate the assessment information across the organizations.

3. Risk Judgement

In this step, the risk assessments in each level are given to the decision makers of each respective level so they can develop effective action plans.

Using the UAS operators' cybersecurity risk assessment, Operational Commander B confirms that 50% of the units supporting UAS operations are at risk from the cyber threat, imposing a moderate risk to their objectives. Operational Commander B's action plan is to deploy a different capability, with a lower overall cybersecurity risk for critical missions and accepts the risk for all other non-critical missions. This allows the commander to use cybersecurity risk factors and non-cyber related risk elements to decide what capability to deploy.

The Operational Commander A confirms that no units in their AOR operate UAS, assessing the overall risk as low. Operational Commander A's action plan is to report no impact to their critical objective in terms of UAS operations and continue with normal military operations.

The Strategic Commander A confirms that risk imposed to the strategic objectives is low; therefore, the commander endorses the operational command's action plans.

4. Risk Management

The overall risk of UAS operations in the AOR and the action plans are provided to all command-level risk management staff using the integrated risk assessment chart as shown in Table 5. This integrated risk assessment chart can include additional information and instructions that commanders want to communicate. For example, it can

communicate that cybersecurity risks will be monitored periodically. Also, any updates to the assessments will be conducted when new or emerging cyber threats or risks associated with COTS UAS are identified.

Table 5. AOR's Overall Risk Assessment. Adapted from [24], [27].

Event Title: Cyber Threat Impact to UAS Operations in AOR

Purpose: Determine the Impact of the AOR's Cyber Threat to UAS Operations.

Cyber Threat Characteristics: Mid-level nation state cyber actor with sophisticated understanding of advanced penetration techniques, well-resourced, capable of replicating and execute hacking examples found online and intends to conduct cyber espionage and disrupt multiple organization's key resources.

Strategic Assessment

Risk	Criteria	Low	Moderate	Significant	High	Overall Risk
Strategic Risk	Probability of Event	Highly Unlikely (~0-20%)	Unlikely (~21-50%)	Likely (~51-80%)	Very Likely (~81-100%)	Low
	Consequence of Event	Limited: Confined damage to strategic objectives	Major: Considerable, damage to strategic objectives	Catastrophic: High order damage to strategic objectives	Existential: Permanent damage to strategic objectives	

Strategic Risk Notes: AOR's cyber threat poses limited impact to strategic objectives. The operational commanders can accomplish all critical objectives.

Operational Assessment

Risk	Criteria	Low	Moderate	Significant	High	Overall Risk
Risk-to-Mission	Probability of Event	Highly Unlikely (~0-20%)	Unlikely (~21-50%)	Likely (~51-80%)	Very Likely (~81-100%)	Moderate
	Consequence of Event	Can fully achieve all objectives	Can achieve all critical objectives	Can achieve only most critical objectives	Potential failure. Cannot achieve critical objectives	

Risk-to-Mission Notes: AOR's cyber threat poses a Moderate risk to Operation Commander B's UAS operations. This affects 50% of the units supporting UAS operations; however, all other tactical units can achieve all critical objectives. Operational Commander B will ensure deployment of capabilities with less risk will be deployed in support to critical missions. All other non-critical mission risk is acceptable.

Tactical Assessment

UAS Operator's Assessment

Unit	Overall Risk	Commander's Notes
Tactical Unit BA	Moderate	Requested platform despite higher threat assessment due to optical camera quality and increased endurance.
Tactical Unit BB	Low	Requested as a secondary platform if Drone-A risk is not acceptable to the overall mission.

Overall Risk Assessment

Notes: AOR's cyber threat possess a Moderate risk to Tactical Unit BA's UAS operations. This affects 1 of 2 (50%) Units supporting UAS operations in the AOR. All other tactical units can achieve all critical objectives.

Action Plan

Risk Management Mitigation Plan: Deployment of UAS capabilities with less risk will be deployed in support to critical missions. For all other non-critical missions, risk is acceptable. The cybersecurity risks will be monitored periodically, and assessments will be conducted when new or emerging cyber threats or risks associated with COTS UAS are identified.

This scenario highlights how continuous cybersecurity risk assessment using the CRM process enhances awareness of cyber risks for COTS UAS operations in support of military operations. This model provides a method to share, deliver and communicate cybersecurity risk information across multiple command levels (Figure 16). While this application only shows one scenario, it can apply to any situation involving IT operations. The information contained in Table 5 functions as a guide to provide commanders a method for measuring the impact of cybersecurity risk elements against their military objectives.

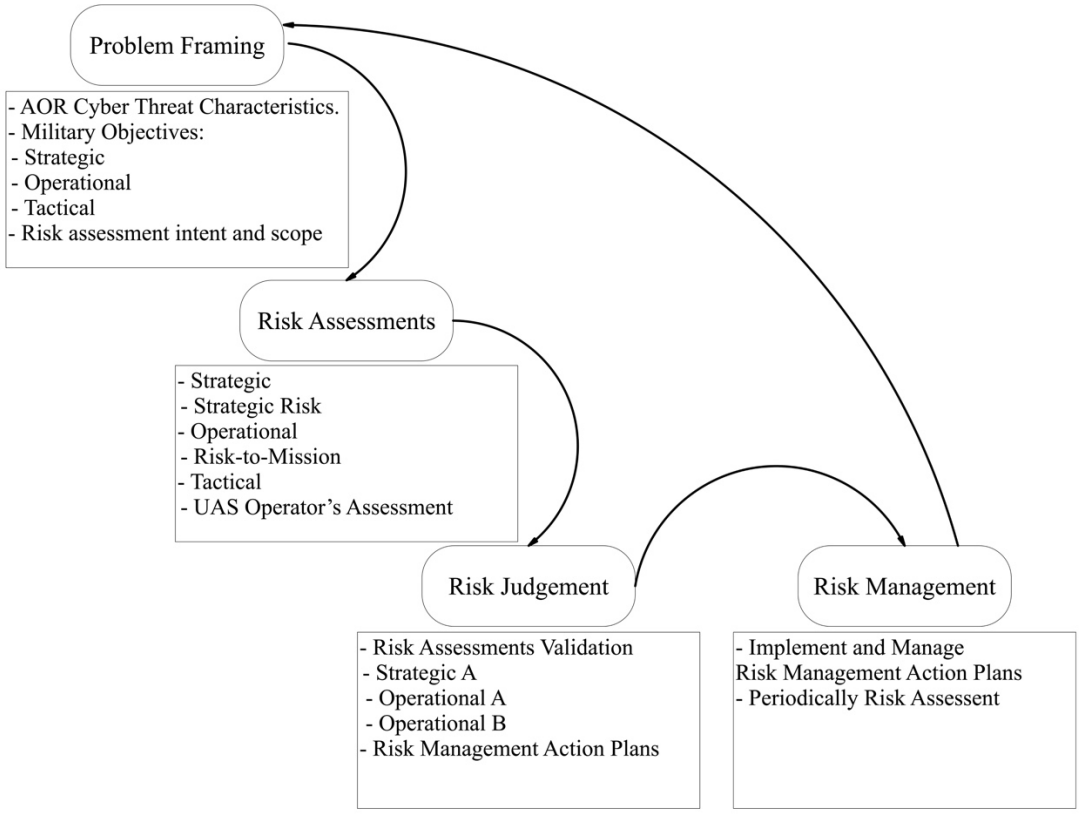

Figure 16. Applying CRM process.

V. CONCLUSION AND FUTURE WORK

A. CONCLUSIONS

There are no DoD policies or instructions addressing the cyber risk associated with COTS UAS (cyber physical systems) or definitions of specific requirements for COTS UAS operations in the cyber domain. Moreover, no guidance exists regarding how commanders should measure the impact of cybersecurity risk against their military objectives. Since no such process currently exists, neither the strategic, operational or tactical-level commanders are fully aware of the cybersecurity risks they may be assuming from COTS UAS operations in their AOR. Furthermore, the absence of cybersecurity risk information across multiple echelons can result in an inaccurate assessment of an AOR's cyber threat and its potential impact on military operations at the tactical, operational and strategic level.

With regards to COTS UAS, the addition of the CRM process to risk assessment and mission planning could give commanders a better awareness of risks, a way to accurately assess current cyber threats, and the ability to develop more effective action plans for their AORs. Potentially, commanders can also use the CRM process to assess the risk and potential impact of cyber threats against other IT systems in their AOR.

The flexibility of the CRM process may permit the incorporation of cybersecurity risk assessment to any type of risk assessment. For example, if a commander wants to conduct a risk assessment focused on manning, training and equipping, the CRM process allows the commander to also include cybersecurity risk elements related to the IT equipment.

The incorporation of the CRM process may enhance current efforts to promote the inclusion of cybersecurity into military culture. It does so by bringing cybersecurity elements into military operations and the risk assessment domain. The CRM process may enable the inclusion of cyber operations into the military culture where traditional planning processes may not have always included it. The ability to include cybersecurity risk elements into the overall military risk assessments could enable commanders to

incorporate the cyber domain risks with the other domains—land, sea, air and space. This can enable the future development and implementation of policies and instructions and may provide a better understanding of how cybersecurity elements can be used to determine risk to overall military operations.

B. FUTURE WORK

Adapting this process into military planning, operations and exercises may require organizations to develop new standard SOPs, policies, and directives to assign responsibilities and requirements. This can limit the ability of some organizations to adopt this process. Consequently, future work can focus on understanding how to incorporate the CRM process into current operations, training and exercises to determine the SOPs, policies, and directives necessary for the implementation of this proposed model across the DoD.

Time and additional resources may be required before benefits from adapting the CRM process emerge. Future work can explore the long term effect of these benefits and the impacts of incorporating cybersecurity elements into military operations and traditional risk assessment processes.

LIST OF REFERENCES

[1] J. Burke, "Bin Laden letters reveal al-Qaida's fears of drone strikes and infiltration," *The Guardian*, Mar. 1, 2016. [Online]. Available: https://www.theguardian.com/world/2016/mar/01/bin-laden-letters-reveal-al-qaidas-fears-of-drone-strikes-and-infiltration

[2] Office of the Chief of Public Affairs, "Modernizing for greater lethality," *Stand-To*, Oct. 9, 2017. [Online]. Available: https://www.army.mil/standto/2017-10-09?dmd

[3] "Accelerating new technologies to meet emerging threats," 116TH Congress, 2018. Available: https://www.armed-services.senate.gov/imo/media/doc/18-40_04-18-18.pdf

[4] Consumer News and Business Channel, "White House considering executive order to bar Huawei, ZTE purchases," *CNBC*, Dec. 27, 2018. [Online]. Available: https://www.cnbc.com/2018/12/27/white-house-considering-executive-order-to-bar-huawei-zte-purchases.html

[5] D. Michaels, "Poland urges NATO allies to coordinate against China cybersecurity challenges," *Wall Street Journal*, Jan. 13, 2019. [Online]. Available: https://www.wsj.com/articles/poland-urges-nato-allies-to-coordinate-against-china-security-challenges-11547408570

[6] UAS Task Force Airspace Integration Integrated Product Team, "Unmanned aircraft system airspace integration plan," Washington, DC, USA, 2011.

[7] D. Gettinger, "Summary of drone spending in the FY2019 defense budget request," Center for the Study of the Drone at Bard College, New York, NY, April 9, 2018. [Online]. Available: https://dronecenter.bard.edu/files/2018/04/CSD-Drone-Spending-FY19-Web-1.pdf

[8] S. Snow, "'Quads for squads' grounded over cyber concerns," *Marine Corps Times,* Jun. 15, 2018. [Online]. Available: https://www.marinecorpstimes.com/news/your-marine-corps/2018/06/15/quads-for-squads-grounded-over-cyber-concerns/

[9] *Doctrine for the Armed Forces of the United States*, JP-1, Joint Chiefs of Staff, Washington, DC, 2017. [Online]. Available: http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf

[10] *Cyberspace Operations*, JP-3–12, Joint Chiefs of Staff, Washington, DC, 2018. [Online]. Available: http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018 07–16

[11] S. Hall, "Cyberspace at the operational level: warfighting in all five domains," Naval War College, Newport, RI, USA, AD-1021506, 2016. [Online]. Available: https://apps.dtic.mil/docs/citations/AD1021506

[12] *Cybersecurity*, DoD Instruction 8500.01, Department of Defense, Washington, DC, USA, 2014.

[13] *National Security Presidential Directive-54/Homeland Security Presidential Directive-23, NSPD-54/HSPD-23*, The White House, Washington, DC, USA, 2008.

[14] *The Department of Defense Cyber Strategy,* Department of Defense, Washington, DC, 2015.

[15] *The Department of Defense Cyber Strategy,* Department of Defense, Washington, DC, 2018.

[16] *Managing Information Risk*, NIST Special Publication 800–39, 2011. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

[17] *Guide for Applying the Risk Management Framework to Federal Information Systems*, NIST Special Publication 800–37, 2010. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

[18] *Risk Management Framework (RMF) for DoD Information Technology (IT),* DoD Instruction 8510.01, Department of Defense, Washington, DC, USA, 2016.

[19] *Guide for Conducting Risk Assessments,* NIST Special Publication 800–30, 2012. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[20] *DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Life cycle*, DoD Guidebook, Department of Defense, Washington, DC, USA, 2015.

[21] *Cybersecurity Test and Evaluation Guidebook*, DoD Guidebook, Department of Defense, Washington, DC, USA, 2018.

[22] National Institute for Standards and Technology, "Cybersecurity framework," Accessed January 9, 2019. [Online]. Available: https://www.nist.gov/cyberframework

[23] Critical Infrastructure Sector Partnership, "Cybersecurity framework," Accessed January 9, 2019. [Online]. Available: https://www.us-cert.gov/ccubedvp/cybersecurity-framework#framework-guidance.

[24] *Joint Risk Analysis*, CJCSM 3105.01, Joint Chiefs of Staff, Washington, DC, USA, 2016. [Online]. Available: http://www.jcs.mil/Portals/36/Documents/Library/Manuals/CJCSM%203105.01%C2%A0.pdf?ver=2017-02-15-105309-907

[25] M. Frigo and R. Anderson, "Strategic Risk Assessment. A first step for improving risk management and governance," *Strategic Finance,* pp. 25–33, Dec. 2009.

[26] "Cyber incident handling program" class notes for Cyber Security Incident Response and Recovery, Dept. of Computer Science, Naval Postgraduate School, Monterey, CA, USA, Winter 2019.

[27] G. Lattimore, "Unmanned Aerial System Cybersecurity Risk Management Decision Matrix for Tactical Operators," M.S. thesis manuscript in preparation, Dept. of Information Science, NPS, Monterey, CA, USA, 2019.

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