NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

SYSTEMS ENGINEERING CAPSTONE REPORT

UNMANNED AERIAL SYSTEM RISK MANAGEMENT DECISION MATRIX

by

Aaron M. Daponte, Gregory A. Maguire, and Calvin J. Roldan

June 2020

Advisor: Douglas L. Van Bossuyt
Co-Advisor: Britta Hale

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

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 Systems Engineering Capstone Report

4. TITLE AND SUBTITLE UNMANNED AERIAL SYSTEM RISK MANAGEMENT DECISION MATRIX	5. FUNDING NUMBERS
6. AUTHOR(S) Aaron M. Daponte, Gregory A. Maguire, and Calvin J. Roldan	
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)

The Department of Defense (DOD) lacks a suitable method for identifying and managing the cybersecurity risks associated with commercial off-the-shelf (COTS) unmanned aerial system (UAS) use. With no method in place to mitigate the cybersecurity risk, the DOD suspended the purchasing and use of COTS UASs in a memorandum by the deputy secretary of defense on May 23, 2018, until a strategy was developed to mitigate the known cybersecurity risks and vulnerabilities. This research establishes a method to identify and mitigate the cybersecurity risk of COTS UASs at the tactical level. The chosen method was a cybersecurity risk-management decision matrix that would help produce a risk assessment to help tactical operators make informed operational decisions. More specifically, an architecture, method, and processes were developed for commands to be able to create their own risk matrices. Utilizing a systems engineering approach, the UAS was broken down into subsystems to help identify potential cybersecurity vulnerabilities. These vulnerabilities were then used to create inputs to the matrix that would assign an output risk that tactical operators could use to make real-time decisions. The matrix was then validated using the National Institute of Science and Technology (NIST) framework.

14. SUBJECT TERMS cybersecurity, decision matrix, unmanned aerial system	15. NUMBER OF PAGES 108
	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.

UNMANNED AERIAL SYSTEM RISK MANAGEMENT DECISION MATRIX

Aaron M. Daponte, Gregory A. Maguire, and Calvin J. Roldan

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
June 2020

Lead Editor: Calvin J. Roldan

Reviewed by:

Douglas L. Van Bossuyt	Britta Hale
Advisor	Co-Advisor

Accepted by:
Ronald E. Giachetti
Chair, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Department of Defense (DOD) lacks a suitable method for identifying and managing the cybersecurity risks associated with commercial off-the-shelf (COTS) unmanned aerial system (UAS) use. With no method in place to mitigate the cybersecurity risk, the DOD suspended the purchasing and use of COTS UASs in a memorandum by the deputy secretary of defense on May 23, 2018, until a strategy was developed to mitigate the known cybersecurity risks and vulnerabilities. This research establishes a method to identify and mitigate the cybersecurity risk of COTS UASs at the tactical level. The chosen method was a cybersecurity risk-management decision matrix that would help produce a risk assessment to help tactical operators make informed operational decisions. More specifically, an architecture, method, and processes were developed for commands to be able to create their own risk matrices. Utilizing a systems engineering approach, the UAS was broken down into subsystems to help identify potential cybersecurity vulnerabilities. These vulnerabilities were then used to create inputs to the matrix that would assign an output risk that tactical operators could use to make real-time decisions. The matrix was then validated using the National Institute of Science and Technology (NIST) framework.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1
- A. PROBLEM STATEMENT 1
- B. RESEARCH OBJECTIVES 2
- C. SYSTEMS ENGINEERING PROCESS 2

II. PROBLEM DEFINITION 11
- A. NEEDS ANALYSIS 11
- B. STAKEHOLDER ANALYSIS 12
- C. FUNCTIONAL ANALYSIS 17
- D. RECENT ATTACKS 22
- E. SUMMARY 31

III. MATRIX ARCHITECTURE 33
- A. MATRIX INPUTS AND CONSTANTS 34
- B. MATRIX ARCHITECTURE AND OUTPUTS 37

IV. EXAMPLE DECISION MATRIX 41
- A. MATRIX INPUTS 41
- B. EXAMPLE MATRIX WALKTHROUGH 64

V. NIST CYBERSECURITY FRAMEWORK 68
- A. IDENTIFY 68
- B. PROTECT 69
- C. DETECT 70
- D. RESPOND 70
- E. RECOVER 70

VI. CONCLUSION AND FUTURE WORKS 72
- A. CONCLUSION 72
- B. FUTURE WORKS 73

SUPPLEMENTAL 78

LIST OF REFERENCES 80

INITIAL DISTRIBUTION LIST 86

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. Engineering design process model.....4

Figure 2. Value curve for the compatibility, reusability, and the importance to stakeholder evaluation measures.....7

Figure 3. Value curve for schedule. 8

Figure 4. UAS basic components. Source: Hartmann and Steup (2013, 5). 18

Figure 5. UAS risk hierarchy diagram. 18

Figure 6. Matrix operation action diagram.....33

Figure 7. Matrix input/output diagram. 34

Figure 8. Matrix operator inputs hierarchy diagram. 36

Figure 9. Constant matrix inputs hierarchy diagram. 37

Figure 10. Matrix output hierarchy. 37

Figure 11. Matrix internal architecture input/output diagram. 38

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Raw scores. 6

Table 2. Value scores. 8

Table 3. Risk input swing weights/measure weights. 9

Table 4. Weighted scores. 10

Table 5. Stakeholders. 15

Table 6. Project objectives. 16

Table 7. UAS vulnerability types. Adapted from Mansfield et al. (2013, 6). 26

Table 8. GCS vulnerabilities. Adapted from Mansfield et al. (2013, 6). 27

Table 9. UAV vulnerabilities. Adapted from Mansfield et al. (2013, 6). 28

Table 10. Communication link vulnerabilities in availability. Adapted from Mansfield et al. (2013, 6). 30

Table 11. Risk rating comparison key. 41

Table 12. Communication link attack risk rating. 48

Table 13. Communication links of COTS UAS. 49

Table 14. Wi-Fi risk rating. 52

Table 15. Wi-Fi security risk rating. 57

Table 16. GPS mode risk values. 61

Table 17. GPS attack risk rating. 62

Table 18. Geography input risk. 63

Table 19. Adversary input risk. 64

Table 20. Demonstration operator inputs. 64

Table 21. Most likely GPS attacks. 65

Table 22. Matrix output. 67

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ARP	Address Resolution Protocol
C2	Command and Control
COTS	Commercial-off-the-shelf
DDoS	Distributed Denial of Service
DOD	Department of Defense
DoS	Denial of Service
FANET	Flying Ad-Hoc Networks
GCS	Ground Control Station
GHz	Gigahertz
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
IEEE	Institute of Electrical and Electronics Engineers
INS	Inertial Navigation System
IP	Internet Protocol
LAN	Local Area Network
LOS	Line of Sight
M&S	Modeling and Simulation
MAC	Media Access Control
MAJ	Major
MCCDC	Marine Corps Combat Development Command
MCWL	Marine Corps Warfighting Laboratory
MHz	Megahertz
MIMO	Multiple Input, Multiple Output
MiTM	Man in the middle
MU-MIMO	Multi-User Multiple Input, Multiple Output
NIST	National Institute of Standards and Technology
OSD	Office of the Secretary of Defense
PHY	Physical Layer

RAND	Research and Development
RF	Radio Frequency
RTT	Round Trip Time
SATCOM	Satellite Communication
TCP	Transmission Control Protocol
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
USECDEF	Undersecretary of Defense
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

EXECUTIVE SUMMARY

BACKGROUND

Over the years, the United States military has used commercial-off-the-shelf (COTS) unmanned aerial systems (UASs) to support its missions in an inexpensive and effective manner. However, the Department of Defense (DOD) lacks a suitable method for identifying and managing the cybersecurity risks associated with COTS UAS use at the tactical operator level. Due to the cybersecurity vulnerabilities in COTS UASs and no method in place to mitigate the cybersecurity risk, the DOD suspended the purchasing and use of COTS UASs until a strategy was developed to mitigate the known cybersecurity risks. This directive was issued in a memorandum by the Deputy Secretary of Defense on May 23, 2018. While exemptions to the directive are made on a case-by-case basis, this requires commands to submit a waiver before being able to utilize COTS UASs.

PURPOSE

This research is intended to provide a method for tactical operators to identify and mitigate cybersecurity risks of COTS UASs. The method of choice to achieve these results is through the creation of a cybersecurity risk management decision matrix. The objectives of this research are as follows:

- Identify and analyze potential RF, IP, and other operational COTS UAS risks.
- Develop a methodology, process, and architecture for a cybersecurity risk management decision matrix, which can be used to aid in the use of and approval to use COTS UAS in the military at the tactical level.
- Verify the cybersecurity risk management decision matrix using NIST cybersecurity framework and DOD guidance, and/or other methods.

The developed methodology and process are documented in this report with the intent that it help enable commands to create their own cybersecurity risk management

decision matrices using the operational environment and other factors as inputs to the matrix so that tactical operators can use to make real-time decisions.

METHODOLOGY

This thesis utilizes an iterative, systems engineering process model to meet stakeholder requirements. The systems engineering process being used in the creation of the cybersecurity risk management decision matrix consisted of multiple phases. These phases include identifying the need, researching the need, developing possible solutions, selecting the best solution, constructing a prototype, testing and evaluating, communicating the solution, and reevaluating. The identifying and researching the need phases include initial research and information gathering, problem scoping, developing a needs statement, and generating requirements. The next phases, which include developing possible solutions, selecting the best solution, and constructing a protype phases, focus on the conceptual development of the cybersecurity risk management decision matrix, determining the inputs and outputs to the matrix, and creating a functional architecture that satisfies how all elements related to matrix design function as a whole. In addition, an analysis of alternatives is performed to see what design method is most useful in satisfying stakeholder needs. Once these phases are near completion, the testing and evaluating phase is initiated, where the process for implementing the cybersecurity risk management decision matrix architecture is explored and a recommended alternative is selected. Additionally, the testing and evaluation phase is used to ensure the developed matrix meets the stakeholders needs. This is done by using the NIST cybersecurity framework. Any gaps between the NIST cybersecurity framework and the proposed matrix are used to identify faults in the system design. These faults are then corrected and re-evaluated using the NIST cybersecurity framework.

Using the aforementioned iterative systems engineering process, the project team identifies the relevant stakeholders and conducts a needs and requirements analysis. Discussions with the stakeholders provide valuable information to the formation of the needs analysis. The outcome of the needs analysis is presented as the objectives of this research identified in the purpose section of the executive summary. With the stakeholder needs identified, a functional analysis is conducted to better understand how the project

team can create the cybersecurity risk management decision matrix. This is accomplished by examining the common COTS UAS in smaller functional entities. During the functional analysis, four subsystems are identified. These include the ground control station, the unmanned aerial vehicle, the up/down control link, and other external factors such as the location of the operational area. With these four subsystems defined, the project team is able to identify potential cybersecurity vulnerabilities in each functional piece of the UAS. Researching the different protocols used by COTS UASs aids in identifying those potential cybersecurity vulnerabilities. This research focuses heavily on command and control (C2) links, Wi-Fi, and GPS links as those are commonly used in COTS UASs as well as the COTS UAS vulnerabilities. GPS, Wi-Fi, and C2 links each have a variety of different modes and protocols so each one is researched to allow a cybersecurity risk code to be assigned. These cybersecurity vulnerabilities are then used to create inputs to the cybersecurity risk management decision matrix that aid in assigning an output risk that tactical operators can use to make real-time decisions.

Once the basic functional analysis of the UAS is complete, the solidification of the cybersecurity risk management decision matrix architecture can begin. The matrix inputs, constants, architecture, and outputs are all finalized during this phase, barring the successful validation of the matrix. Since the inputs to the matrix are mostly identified during the functional analysis, the inputs to the matrix are broken down into three categories. These categories are as follows:

- Cyber-attacks (Constant Input)
- Cyber Vulnerabilities (Operator Input)
- Operational Environment (Operator Input)

Once these three inputs are created, the inputs are further decomposed. The cyber attacks' input is broken down into two sub-categories: attacks and symptoms. Using a list of known cyber-attacks provides a constant, automatic input into the matrix. Each of the cyber-attacks are given different effectiveness levels based upon the C2 link and GPS mode the tactical operator has chosen for the mission. Those different levels of effectiveness are

used to assign a risk rating. Additionally, the cyber vulnerabilities input is broken down into C2 and GPS attacks and the operational environment input is broken down into three subcategories: the current adversary, the RF range, and the geography of the operational location. All of these subcategories provide input to the matrix.

Using the three main inputs, cyber-attacks, cyber vulnerabilities, and operational environment, a set of three outputs to the matrix are derived, intended to direct the operators' decisions. These outputs are as follows:

- Most Likely Cyber Attacks
- Symptoms
- Risk Rating

The first output of the matrix is a list of most likely cyber-attacks and their corresponding symptoms. The list is derived from a combination of the constant input "cyber-attacks" and the operator input "adversary." Since different adversaries possess different capabilities, this is an important distinction in the calculation of risk. The final output is the risk rating which is a numerical value that is assigned to each of the most likely cyber-attacks and their corresponding symptoms and displayed to the operator.

Once the architecture of the matrix is created, a sample cybersecurity risk management decision matrix is created to demonstrate how commands would create their own matrices using the proposed architecture. This example shows all the different matrix inputs with various protocols for GPS and Wi-Fi that can be utilized. The example clarifies how the risk is calculated from each of the matrix inputs and what the output will be from those inputs. After the example matrix was established, the decision to implement the cybersecurity risk management decision matrix in Microsoft Excel VBA was made. This decision is made based on the widespread availability of Excel and a lower potential of human error by tactical operators using other methods.

RESULTS

By utilizing the proposed methodology for the construction of a cybersecurity risk management decision matrix, there is an effective way to produce a matrix that satisfies the stakeholders' needs. The proposed methodology satisfies the project objectives; developing a cybersecurity risk management decision matrix architecture and methodology, identifying COTS UAS risks to use as inputs to the matrix, and validating the proposed matrix architecture using the NIST cybersecurity framework. Using the table of vulnerabilities, created through the project team's research, proved to be a useful tool when creating a cybersecurity risk management decision matrix. It provides a list of vulnerabilities associated with the GCS, UAV, operators, and communications link. This list can be updated at any time with the emergence of new technologies or protocols and their associated vulnerabilities to be used as a reference for inputs to the cybersecurity risk management decision matrix. The cybersecurity risk management decision matrix architecture is considered a suitable solution as it is validated by the NIST cybersecurity framework while maintaining the ability to be modifiable.

CONCLUSION

This research develops a cybersecurity risk matrix framework that can be used by tactical operators of COTS UASs to produce matrices that help determine proper courses of action to mitigate cybersecurity risk. Since different vulnerabilities and the effectiveness of certain protocols and their level of security change over time, a framework for developing a matrix is far more valuable than developing a solution that may become dated within a few years. By defining the process behind the creation of the matrix and demonstrating how operators would define inputs, assigning risk ratings, and developing the risk outputs, commands will be better equipped to handle the changing problem space for years to come. The different commands and tactical operators are then able to customize the risk matrix to support their own needs, even down to a tailored approach to each individual mission. The example matrix in this report provides the demonstration of the thought process behind tailoring the matrix that can be used by many different commands.

FUTURE WORK

While conducting research and development of the cybersecurity risk management decision matrix architecture, there were several potential needs identified that were outside of the scope of this research. These needs could spur future research in other, more specific areas of study regarding the cybersecurity risk management decision matrix for COTS UAS. The first area of consideration is performing a real-world validation exercise with tactical operators to identify any shortcomings of the matrix architecture design. This would also allow the tactical operators to tailor the matrix to their own cybersecurity risk assessment needs, which would provide an opportunity to see how easily this can be implemented on a larger scale. Another consideration for future work is to study the best method for implementing the cybersecurity risk management decision matrix. Since the matrix architecture is developed using Excel, future work would need to be done to see what platforms could support this matrix. Given the matrix will be hosted on an electronic platform, another area of exploration could be putting the matrix on a web or phone-based application. The third consideration for future work is the development of an expansion library of other protocols and vulnerabilities. While this study focuses heavily on RF, GPS, and Wi-Fi vulnerabilities, there are many other protocols in existence and the list will continue to grow as new technology emerges. For instance, there are currently UAVs that utilize 5G cellular networks instead of Wi-Fi to connect the aerial vehicle to the operator, although it is not too common. The final consideration for future works related to the cybersecurity risk management decision matrix is applying a time-phased use of the matrix. The time-phased cycle would start during the acquisition phases, and continue through the pre-mission, during mission, and post mission phases. Since there are different operational risks at each phase, there are more inputs to the matrix that could be considered.

I. INTRODUCTION

A. PROBLEM STATEMENT

The Undersecretary of Defense (USD) issued a decision memo enacting a moratorium on the use of Commercial-off-the-Shelf (COTS) Unmanned Aerial Systems (UAS) across Department of Defense (DOD). The Office of the Secretary of Defense (OSD) stood up a board to assess COTS UAS on a case-by-case basis to exempt the COTS UAS from the policy and decision-making authority has further been devolved to the service branches. However, operators on the ground need the ability to assess if a COTS UAS can still complete its mission while posing an acceptable level of risk, even when potentially compromised by an adversary (e.g., a COTS UAS with an encrypted and secure control link but an unencrypted video feed can be vulnerable to video feed intercept). In addition, there is a risk of the adversary being alerted to the presence of opposing forces via video feed detection. It is expected that some scenarios will be identified where a tactical operator may choose to continue operating in spite of the COTS UAS being compromised because the risk is sufficiently low compared to the benefit of the mission.

The objective of this technical report is to develop a methodology and process for commands to create cybersecurity risk matrices using the operational environment and other factors as inputs that tactical operators can use to make real-time decisions. This objective is completed by applying a systems engineering process to the development of the aforementioned methodology. A sample cybersecurity risk matrix is also developed in this technical report using COTS information and sample operational parameters to demonstrate the process and validate the methodology. The sample matrix is targeted for use by tactical operators to aid in making decisions on whether or not a COTS UAS can be flown from a cybersecurity perspective. Situation specific issues are beyond the scope of this technical report. Future COTS UAV developments dictate that the most appropriate solution is to provide a method that commands can follow to periodically refresh or redevelop cybersecurity risk matrices as needed.

To understand the level of security provided, the project team performed a qualitative literature analysis of security algorithms and protocols used in COTS UAS, and the methodology that produces the cybersecurity risk matrix is verified using the NIST cybersecurity framework. The decision matrix uses operational parameters as inputs and provides a risk level to the operator as an output, which can then be used to determine the level of cybersecurity risk that the COTS UAS faces in the operational environment. The final product is the methodology and process for commands to create the cybersecurity risk matrices using the operational environment and other factors as inputs for end users.

B. RESEARCH OBJECTIVES

The specific objectives proposed in this version for consideration by the stakeholders are as follows:

1. Identify and analyze potential RF, IP, and other operational COTS UAS risk.

2. Develop a cybersecurity operational risk management decision matrix, which can be used to aid in the use of and approval to use COTS UAS in the military at the tactical operator level.

3. Verify matrix using NIST cybersecurity framework and DOD guidance, and/or other methods.

4. Provide guidance on how to rapidly assess if a UAS may have compromised cybersecurity at the tactical operator level, and how to continue to operate with degraded capability despite the compromise.

C. SYSTEMS ENGINEERING PROCESS

According to Sharp, Finkelstein, and Galal (1999), the systems engineering process is an "iterative and recursive problem-solving process. It transforms needs and requirements into a set of system product and process descriptions, generate information for decision makers, and provides input for the next level of development." In this section of this technical report, the process of developing the cybersecurity risk management

matrix is examined. It includes stakeholder involvement, the systems engineering approach to the problem, and the development of the needs analysis. This section also covers the value system design, the generation of different risk matrix alternatives, and an analysis of those alternatives.

Stakeholders

The following stakeholders benefited from the creation of the cybersecurity operational risk management decision matrix: The Marine Corps Combat Development Command (MCCDC); the topic sponsor for the project, the Marine Corps Warfighting Laboratory (MCWL); and NPS System Engineering department. The sponsors helped shape and refine requirements for the cybersecurity risk management decision matrix. The sponsors benefited from the use of the proposed methodology of the matrix by being able to easily determine if commercial-off-the-shelf unmanned aerial systems are able to complete missions while posing an acceptable level of risk, even in the event an adversary has compromised the system.

Engineering Design Process

The team authoring this technical report conducted a review of several systems engineering process models and chose the engineer design process model which best supported our research project. The project team adapted the engineering design process model for this project by utilizing an iterative process between each phase of product development. Next, each phase was developed to a near-final solution, while allowing for new information to be fed through earlier phases in the process model before we came to a final solution. This feedback was derived from design constraints and stakeholder input, and each time a change was made, the new input was added to the engineering design process before finalizing each stage. The engineering design process model used for this research project is shown in Figure 1.

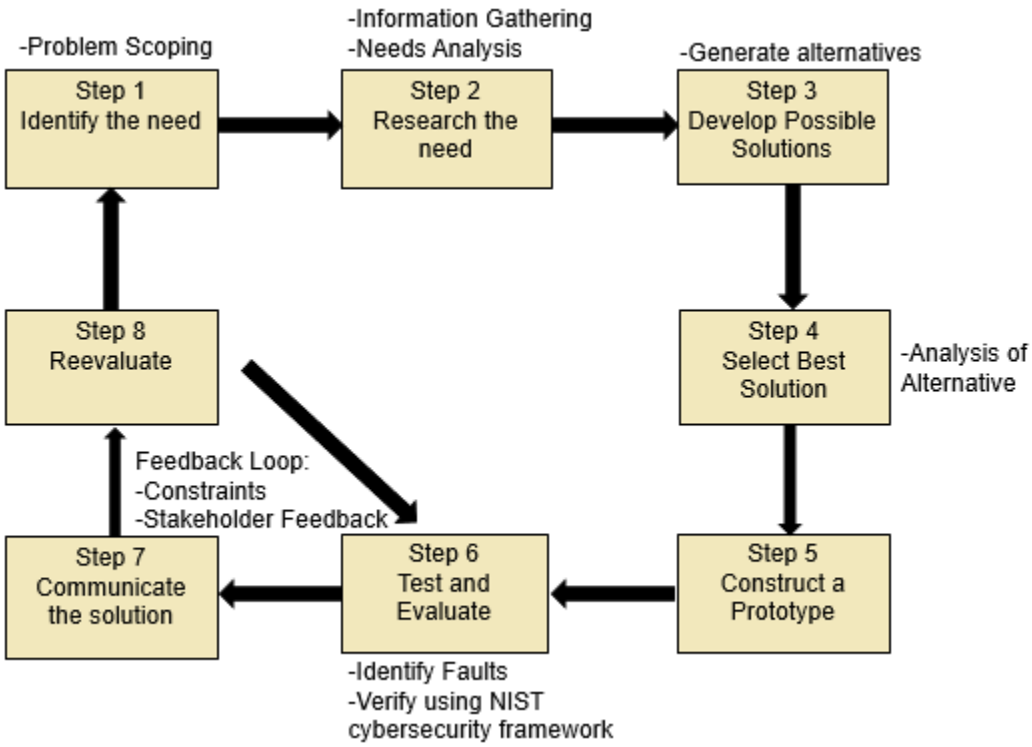

Figure 1. Engineering design process model.

Each step of the process was followed serially, starting with needs analysis, where the cybersecurity risk matrix needs were generated for construction of the matrix. From these needs, alternate solutions were generated. Then, an analysis of the alternatives was performed. After the design phase, the implementation considerations of the matrix were considered and then presented to the stakeholders. Once feedback was received, a loop of edits and reviews were made until stakeholders were satisfied.

Needs Analysis

The objective of the Needs Analysis was to support the risk matrix design by examining design tradeoffs and capabilities to scenarios and the threat environment, as well as other mission-level factors, to support the development of the operational concept and to determine the performance requirements of the risk matrix. The performance requirements of the risk matrix are reusability and compatibility. Reusability is a performance requirement because the matrix must be able to be used more than once.

Compatibility is also a performance requirement because the matrix must allow for adjustments and be compatible with numerous COTS UAS.

Risk Matrix Input Alternatives

Multiple alternatives were identified that address the problem statement. The risk matrix input alternatives identified were COTS UAS inputs or Open Source inputs. With COTS UAS inputs an operator chooses the specific brand and model of the UAS they want to use and use that brand's specifications as inputs. The COTS UAS alternative gives the operator a chance to use what is being sold commercially. This alternative limits the user to only use a COTS UAS researched by the capstone team. The user cannot modify or delete parts of the matrix. With Open Source inputs, an operator chooses specific component parameters of the UAS they want to use. The Open Source alternative gives the operator the option to choose their own input. This alternative allows the user to use any COTS UAS they choose. The user can modify or delete parts of the matrix under their own discretion. The project team compared both contrasting styles, the COTS UAS alternative being strictly based on what is sold commercially and the Open Source alternative which provides flexibility. An analysis of alternatives was performed to show which one is more valuable based on compatibility, reusability, time it takes to develop and importance to stakeholder.

Evaluation Measures

Multi-attribute value analysis was performed on each of the alternatives. According to Buede (2009) "Multi-attribute value analysis is a quantitative method for aggregating a stakeholder's preferences over conflicting objectives to find the alternative with the highest value when all objectives are considered." In order to perform a multi-attribute analysis, evaluation measures need to be identified to determine satisfactory performance of each alternative and differentiate between feasible and infeasible alternatives. The evaluation measures identified were the importance to the stakeholder, schedule, compatibility, and reusability. These evaluation measures will be discussed in greater detail in the swing weights/measure weights subsection of this chapter. Table 1 shows the raw scores for each evaluation measure for each alternative. The raw scores of each evaluation measure are

based on discussions the capstone team had with the stakeholder, where rankings and preferences were elicited. The scale is from 1 to 10 with 1 being the lowest and 10 being the highest for the importance to stakeholder, compatibility, and reusability evaluation measures. For the schedule evaluation measure the scale is 1 to 10 with 1 being the highest and 10 being the lowest. Both scales are patterned off the multi-attribute utility theory literature. The importance to stakeholder raw scores are based on the satisfactory level of each alternative to the stakeholder. Raw scores for schedule are based on time it would take the capstone team to develop the matrix. The compatibility and reusability raw scores are based on an estimate on how compatible and reusable each alternative is. The raw scores are converted to a value scores using value curves.

Table 1. Raw scores.

Evaluation Measure	objective	COTS UAS Inputs	Open Source Inputs
Importance to stakeholder	max	8	10
Schedule	min	3	7
Compatibility	max	3	8
Reusability	max	5	8

Value Curves

A Value Curve was used to compare the evaluation measures of each alternative in the value curve. It is an analysis tool that allows you to determine what the customer really wants. According to Buede (2009), "A value curve converts a raw score of each given evaluation measure, into a common value score, by showing how an evaluation measure value (raw score) gets translated into a value score." These value scores can then be combined and used to compare alternatives using the various evaluation measures. The value curves are used to create swing weights and a Multi-Attribute Decision Making matrix. Each value curve is then evaluated to help choose which is the best alternative.

raw score	Value
10	1
9	0.95
8	0.9
7	0.85
6	0.8
5	0.75
4	0.65
3	0.55
2	0.45
1	0.35

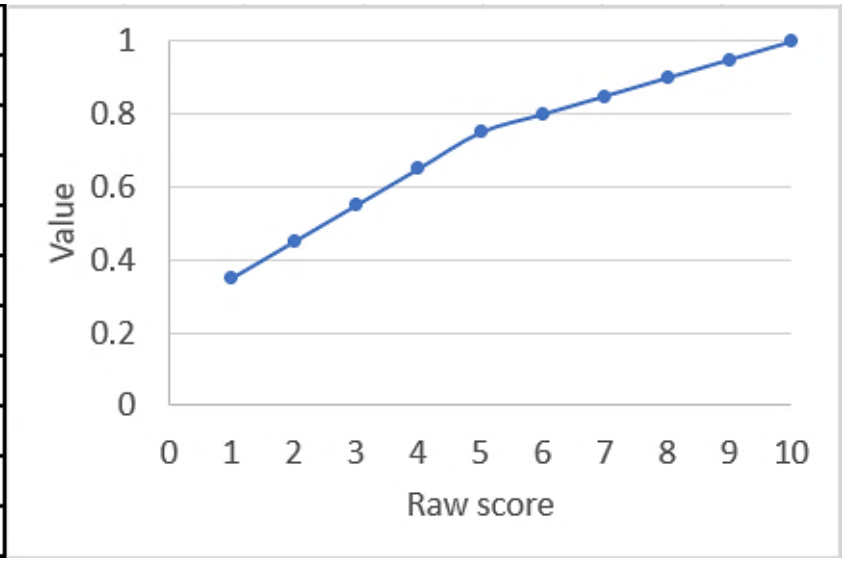

Figure 2. Value curve for the compatibility, reusability, and the importance to stakeholder evaluation measures.

The value curve for compatibility, reusability and the importance to stakeholder evaluation measures have a linear shape. The objective is for each alternative to meet the stakeholder's requirements be compatible and be reusable. The more the alternative has compatibility and reusability the closer the value goes to one. Also, the higher the level of importance, the closer the value goes to one. The open source alternative has a very high importance; therefore, it has a value of 1(raw score of 10). Also, this alternative is highly compatible, so it is assigned a value of 0.9 (raw score of 8). This alternative is also considered to be very reusable so a value of 0.9 (raw score of 8) is assigned. The COTS alternative has high importance but it is considered slightly less important than the open source alternative, therefore it has a value of 0.85 (raw score of 7).This alternative also has a low level of compatibility and reusability so these measures are assigned a value of 0.55 (raw score of 3), and 0.65 (raw score of 4) respectively.

Raw score	Value
1	1
2	0.98
3	0.95
4	0.9
5	0.85
6	0.75
7	0.6
8	0.4
9	0.2
10	0

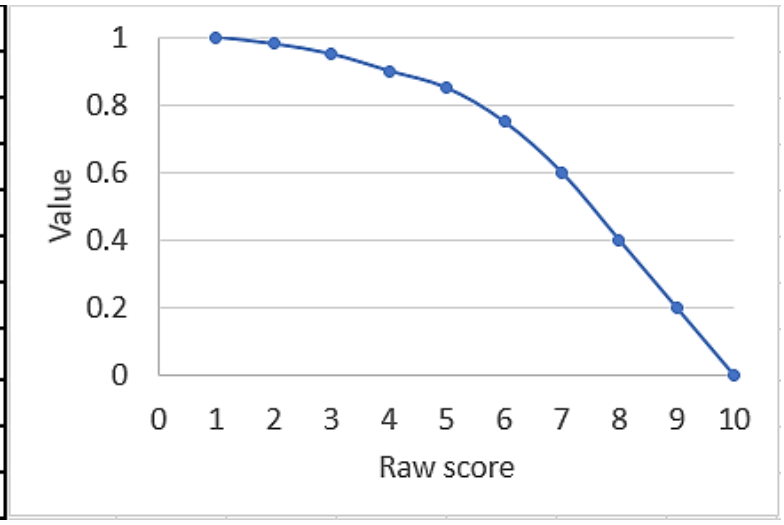

Figure 3. Value curve for schedule.

It is desirable to have an alternative that has the lowest impact on planned (and actual) schedule length since there is a limited amount of time for project completion. The longer it would take to research and build the alternative, the value goes closer to zero. The open source alternative has a value of 0.6 (Raw score of 7) for schedule because it has a high impact on the schedule. The COTS alternative has a value of 0.95 (Raw score of 3) because it will have a moderately high impact on the schedule. Table 2 shows the value score of each evaluation measure for each alternative. The value scores are used to develop a multiple attribute decision making matrix.

Table 2. Value scores.

Value Scores (from Value Curves)		Alternatives	
Evaluation Measure	objective	COTS UAS Inputs	Open Source inputs
Importance to stakeholder	max	0.85	1.00
Schedule	min	0.95	0.60
Compatibility	max	0.55	0.90
Reusability	max	0.65	0.90

Swing Weights/Measure Weights

Swing weights are assigned to evaluation measures based on importance and variation. According to Buede (2009) swing weights are "value weights that reflect the relative value in increasing from the bottom to the top of each value scale are called swing weights because they represent the value attached to the swing from bottom to top."

Table 3. Risk input swing weights/measure weights.

Evaluation Measure	Swing weight	Measure Weight
Importance to stakeholder	9	0.36
Schedule	5	0.20
Compatibility	5	0.20
Reusability	6	0.24
Total	25	1

The max evaluation measure number and the min evaluation measure number of the alternatives are added together and then divided by two and rounded down, and swing weights are assigned based on the importance and variation levels, as follows:

- Importance to stakeholder was assigned the most importance because customer satisfaction is the top priority.
- Reusability has the second most importance because the system be able to be used more than once
- Compatibility has the third most importance because having the ability to adapt to the user's needs is important.
- Schedule has the least importance.

The swing weight and measure weights will be used to create a multi-attribute decision making matrix to determine the highest value of each of the alternatives.

Multiple attribute decision making matrix

The multiple attribute decision making matrix is used to aggregate measure values into a single overall value for each alternative. As Buede (2008) states, "the purpose of MADM is to find the most desirable alternative or rank the feasible alternatives for supporting decision makings." Table 4 takes the value scores from Table 2 and multiplies them by the measure weights in Table 3 to get the weighted score (weighted score = measure weight * value score).

Table 4. Weighted scores.

Weighted Scores (from Value Curves)			Alternatives	
Evaluation Measure	objective	Measure Weight	COTS UAS Inputs	Open Source inputs
Importance to stakeholder	max	0.34	0.29	0.34
Schedule	min	0.14	0.10	0.06
Compatibility	max	0.31	0.17	0.28
Reusability	max	0.21	0.13	0.19
		Total	0.80	0.88

The Open source input method has the higher value with 0.88, while the COTS UAS input method has the lower value of 0.80. The open source method allows more flexibility and adaptability to the matrix, not only in potential options for the operator to choose, but also by allowing the operator to add in additional options in the future. Therefore, the project team chose the open source method.

II. PROBLEM DEFINITION

The purpose of this chapter is to scope and define the problem based upon the stakeholder's original need statement, and other input from stakeholders. Receiving stakeholder input, and consistently reframing the problem or perceived need, are important in delivering a product that is both useful and closely matches the stakeholders' objectives. In order to achieve an end product that meets the stakeholders' desires, a needs analysis and stakeholder analysis are performed. The outcome from this chapter is to discuss the functional analysis and show how the results of the functional analysis produce the initial design of the matrix.

A. NEEDS ANALYSIS

According to Blanchard and Fabrycky (2011), the objective of the needs analysis is to "translate broadly defined 'wants' into more specific system level requirements" (58). To ensure a successful needs analysis, a few basic questions must be answered including the following (Blanchard and Fabrycky 2011, 58):

- What is required of the system in "functional" terms?
- What functions must the system perform?
- What are the primary and secondary functions?
- What must be accomplished to alleviate the stated deficiency?
- When must this be accomplished?
- Where is it to be accomplished?
- How many times or at what frequency must this be accomplished?

One step used to answer some of these questions involves discussion with the stakeholders to help determine what their needs actually are, rather than their perceived needs. This will be discussed further in the following section.

B. STAKEHOLDER ANALYSIS

According to Katz-Haas (1998) another key piece of the needs analysis is to "define users, their tasks and goals, experience levels, functions they want and need from a system, and understanding how users think the system should work" (12–13). This is achieved by performing a stakeholder analysis, which consists of identifying a problem and all relevant stakeholders, developing a set of pointed questions for the stakeholders while conducting research on the problem, having an open dialogue with the stakeholders, filtering the needs of different stakeholders, and repeating the process as necessary (Katz-Haas 1998, 12–13).

Generally, from the project team's experience, the stakeholder analysis typically begins when the systems engineer receives a vague problem statement from the customer. At this stage in the process of developing the stakeholder analysis, the customer does not typically understand fully what they want or need, since they most likely did not perform a needs analysis or even discuss the problem with other potential external stakeholders. In addition, at this point, it is likely unclear to the customer as to which solutions exist. Therefore, it is up to the systems engineer to identify the actual problem given from the initial problem statement. Since the systems engineer will not fully understand the scope of the problem right away, it is important to make sure the stakeholder analysis follows an iterative process, wherein the problem can be updated and redefined as more knowledge is acquired from stakeholder involvement.

Since these problems are typically difficult to solve, the systems engineer will then try to identify all of the stakeholders that pertain to the perceived problem. These problems can range in a wide variety of subjects, and in many cases, the systems engineer is not an expert on the problem they are solving. This means the systems engineer will leverage experts in that field of study that will be able to identify many of the additional stakeholders and better understand stakeholders' needs from a technical perspective. According to Kotonya and Somerville (1998) and summarized by Sharp (1999), there may be different categories of stakeholders that include the "end-users, managers, and other involved in the organizational processes influenced by the system, engineers responsible for system development and maintenance, customers of the organization who will use the system to provide a service, external bodies such as regulators, domain experts, and so on" (2). As a

result, each of these stakeholders will have different objectives that will sometimes conflict with other relevant stakeholders (Sharp and Finklestein 1999, 2). Some of these stakeholders "will use the system directly or indirectly or will be involved in developing the system" (Sharp and Finklestein 1999, 1). The systems engineer is responsible for identifying and contacting these potential stakeholders to gain better insight into the actual needs that will need to be addressed later when proposing a solution to the problem.

For better understanding of the problem, the systems engineer will conduct additional research in the problem space and determine what areas of their research pertain to each set of stakeholders. With this additional knowledge, the systems engineer is better equipped to develop a set list of pointed questions directed at each relevant stakeholder in the problem space. Once these questions are developed, the systems engineer can have a discussion with each of the stakeholders to better understand each of their individual needs and wants in the current problem space. It is important to note that all stakeholders will not be in complete agreement, as each has their own separate needs, but including input from all relevant stakeholders helps create a more detailed map of the problem space, and can aid in identifying any gaps between the current and desired end state. This information also helps uncover the true needs of the customer, which then informs the systems engineer of the possible solution space (Davis 2005, 44–45).

Due to the complex nature of most problem spaces, it is unlikely that all of the necessary information will be acquired in the first round of stakeholder interviews. This means that questions on the subject will come up throughout the duration of the project that need to be addressed; therefore, stakeholder analysis is an iterative process. As new information becomes available through research, or through the sharing of new stakeholder information, the systems engineer may want to reiterate the previous steps in the stakeholder analysis.

Stakeholder Input

Based on the theoretical structure of incorporating feedback in the previous section, the capstone team starts soliciting stakeholder input. Since an important part of the systems engineering process is to produce requirements that can be measured and also achieved by

the proposed system, the key stakeholder's input becomes crucial. The key stakeholder's input is one of the most important pieces in producing these requirements. Before receiving any feedback from the stakeholder, it is useful for the systems engineering team to go through the stakeholder's initial needs statement and try to restate what the stakeholder wants before soliciting an opening discussion with the stakeholder.

Through discussing the research with the project sponsor, Major David Lemke of the Marine Corps Warfighting Laboratory, having a checklist to accompany the risk matrix is of interest. The checklist would be able to help tactical operators assess whether a cyber-attack is occurring and classifying what type of attack it is based upon what is happening within the UAS. This would broaden the scope of the work and drive additional inputs into the risk management decision matrix.

Another element the project sponsor is looking for within the risk matrix is a recommended course of action based upon the cyber risk assessment. This means there is additional research and design work that would need to be done for the output of the risk matrix. This piece of information conflicts with some of the other stakeholders on the project. Given the capstone team's work is being completed as a Naval Postgraduate School (NPS) capstone project, there is a limited amount of time for the capstone team to complete the additional work. This is being taken into consideration by both the capstone team and advisors as it would make the project much larger than originally intended. To maintain schedule, this is being considered as a recommended future work.

Another external stakeholder to the project is the Undersecretary of Defense, which issued a memorandum which banned the use of COTS UASs across the DOD. The Office of the Secretary of Defense stood up a board that assesses the COTS UASs on a case-by-case basis to exempt certain COTS UASs from the policy. However, a case could be made that, with an acceptable level of risk and using the proposed risk management decision matrix for tactical operators, the current process of exempting UASs on a case-by-case basis would not be necessary given a new process would be put in place to manage risk and aid in time sensitive tactical situations without prior approval from the board.

Other stakeholders include the tactical operators who will be using the cybersecurity risk management decision matrix, the launch and recovery team, and the team tasked with maintaining the risk matrix or UAS. While some of these stakeholders may not be directly involved with the matrix such as the launch and recovery teams, these stakeholders are worth mentioning since they affect the system being designed. The launch and recovery team may be affected by the use of the matrix because the matrix poses the possibility of increasing the frequency of their actions and how the tactical operators communicate with the recovery team. While potential adversaries are not listed as stakeholders, they are considered when conducting the stakeholder analysis. This is because these entities are the reason why this subject is being studied. The major difference between the stakeholders and adversaries is that the systems engineering design team does not want to represent adversaries' interests and instead actively oppose them through the construction of the cybersecurity risk management decision matrix.

Stakeholder Analysis Outcome

When conducting the stakeholder analysis, stakeholders are identified and each of their needs are revealed. Table 5 is a listing of the key project stakeholders for the development of the cybersecurity risk management decision matrix at the tactical level. While there may be other parties with interest in this project, three of the key project stakeholders are working with the project team to deliver the matrix.

Project Stakeholders

Table 5. Stakeholders.

Key Project Stakeholders	
1	Marine Corps Warfighting Laboratory (MAJ David Lemke)
2	Tactical Operators
3	Naval Postgraduate School, Department of Systems Engineering
4	The Marine Corps Combat Development Command

Maj. David Lemke of the MCWL has a vested interest in this work as the project sponsor. The project team is working with Maj. Lemke to produce a product that meets both the MCWL's and MCCDC's needs. The product being developed is for the use of a cybersecurity risk management decision matrix by tactical operators in the field. As the primary users, their input is critical in determining whether the proposed matrix meets the MCWL's and MCCDC's needs as well as being a feasible tool for tactical operators during a mission. Finally, the Naval Postgraduate School, systems engineering department and the project advisors are key stakeholders for this project as the research and development is being conducted under their guidance at the educational institution. The Department of Systems Engineering at the Naval Postgraduate School's key interest in this work is to have an end product meet the needs of the other stakeholders in a suitable timeframe set by the institution.

Project Objectives

Once the key stakeholders are identified, the project team uses the stakeholders' input to help create a defined set of stakeholder needs through verbal or written communication. These needs are used to create the guidelines for the duration of the project although these needs may be revisited at any time throughout the matrix development process. Through communication with the stakeholders, the objectives of the project are defined as shown in Table 6.

Table 6. Project objectives.

Project Objectives	
1	Identify potential RF, IP, other COTS UAS risk as inputs to the proposed matrix.
2	Develop cybersecurity operational risk management decision matrix.
3	Validate proposed matrix using NIST cybersecurity framework and other DOD guidance.

C. FUNCTIONAL ANALYSIS

According to Blanchard and Fabrycky (2011), the purpose of the functional analysis is to "break the system (and its elements) down into functional entities through functional packaging and the development of an open architecture configuration" (86). By breaking the system down into smaller parts, a systems engineer is able to describe what each part of the system will do.

UAS Overview

A UAS is a system that provides an operator with the ability to remotely pilot a semi-autonomous aircraft. "To analyze a UAS's vulnerabilities, it is important to understand what components a UAS is made of and how these components interact. In order to analyze UASs on a common basis, UASs are described in terms of component models" (Hartmann and Steup 2013, 21). A UAS consists of a variety of sub-systems, the core components of which include the UAV, GCS, and communications link. Hartmann and Steup (2013) summarize how the UAV consists of the UAV base, avionics and sensors or payloads. The GCS consists of the GCS and operator. The communications link provides the communication between the GCS and UAV. Commands are transmitted by the operator from the GCS to the UAV via the communications link. Data is transmitted from the UAV to the GCS in the same fashion. UAVs can also be outfitted with payloads and sensors to provide additional capability such as Intelligence, Surveillance, and Reconnaissance (ISR) payloads and weapons. "The UAV avionic system is responsible for the conversion of received control commands to commands of the engine, flaps, rudder, stabilizers, and spoilers" (4). The interface block diagram in Figure 4 shows a general breakdown of a standard UAS and how each entity interfaces (without an autonomous flight entity and weapons system).

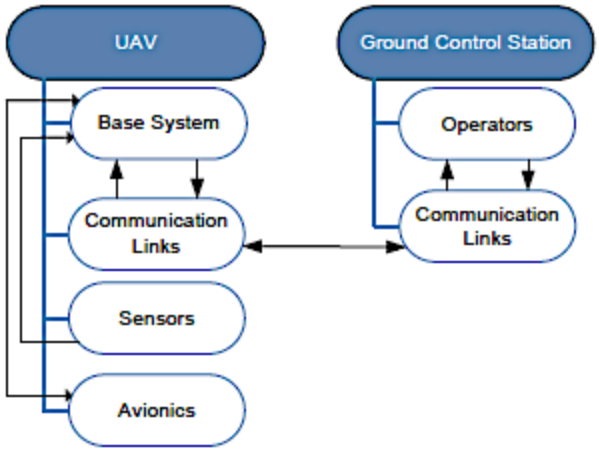

Figure 4. UAS basic components. Source: Hartmann and Steup (2013, 5).

For the risk management decision matrix, it is decided that the core focus is placed on the different components of the UAS itself in addition to other external factors such as environmental conditions which could expose additional risk to the UAS. The UAS's risk profile is broken down into four areas of focus including the ground control station, the unmanned aerial vehicle, external factors, and the up/down/control link. Figure 5 shows this decomposition in a hierarchy diagram of an unmanned aerial system. The highlighted green blocks in the UAS risk hierarchy diagram indicate the targeted areas of resesearch by the capstone team. The reasons for this selection are discussed in the following sections of this chapter.

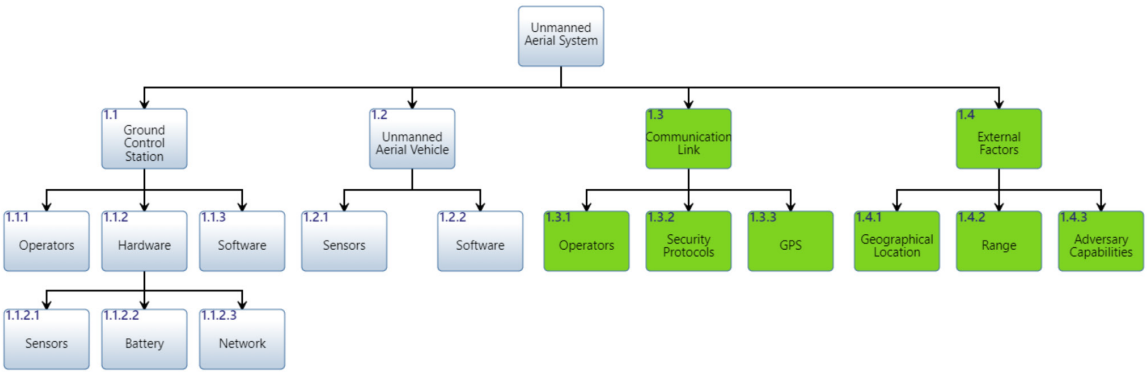

Figure 5. UAS risk hierarchy diagram.

Ground Control Station

The ground control station subsystem is the centerpiece of communication in the UAS. It needs to receive and transmit data in order to control the unmanned aerial vehicle as well as offload data collected from the UAV. It is the hub for RF communication and it typically hosts a display and a controller. COTS ground control stations are typically able to be run from a small phone or tablet making them extremely portable if that is what the mission entails. Other GCSs are stationary and tend to be larger than their portable counterpart.

The GCS may be subject to an availability attack, that can affect the operator's ability to view sensor data. In this type of attack, the adversary may compromise the GCS to modify the functionality of UAS's components. For instance, if an adversary gained control of the camera sensor, they would be able to turn it off thus rendering it useless for surveillance purposes. In addition, by exploiting the UAS through the GCS, an adversary can take control of the UAV and relocate it to another geographical location. This could be achieved by altering data collected by one of the UAV sensors, giving the operator an illusion of a safe operational environment. Since the GCS is the central point between the operator and the UAV, its RF communications are subject to adversary interference as illustrated in the jamming/spoofing scenario previously mentioned. This communication path is so essential and prone to adversary attacks, it is considered its own subsystem in regard to the cybersecurity risk management decision matrix. This subsystem may be found in the up/down/control link section of this chapter.

Unmanned Aerial Vehicle

The UAV subsystem is often the most discussed part of the UAS, because of its recent popularity in the commercial world. The airframes come in a different variety of sizes and materials as well as different payloads that will help meet mission needs. These payloads include video cameras, infrared sensors, thermal sensors, etc. Since the UAV has its own computer, it is able to receive, store, and transmit data, leaving it open to potential exploitation from adversaries (Pastor and Lopez 2007, 1).

The UAV base system is the main hub for connecting all of the UAV's components together. This base system allows the sensors, navigation system, avionics system, and communications system interact with each other as well as any additional auxiliary components. UAV sensor systems are commonly equipped with components such as cameras with inertial navigation systems (INS), GPS, and radar capabilities. The UAV's typical source of communication is through Radio Frequency (RF) communications; either Line of Sight (LOS) or Satellite Communication (SATCOM) (Hartmann and Steup 2013, 4).

The UAV is one of the largest attack surfaces of the entire UAS due to the fact it comes with its own computer and payloads such as video cameras and sensors (Pastor and Lopez 2007, 2). Like the GCS, adversaries can gain access to the system via the UAV itself through the download of malicious software or physical access to perform availability attacks that can turn off or manipulate UAV sensors to affect mission effectiveness. Integrity attacks may also be executed by adversaries. For instance, attacks may modify data from UAV sensors. In this type of attack the adversary could gain access to a camera used for surveillance and inject a pre-recorded video that would be viewed by the operators. This would allow the adversary to interfere with surveillance missions because the UAS operators will be unaware that the video was replayed rather than a live video feed, thus providing faulty intelligence (Vasconcelos et al. 2016, 2). Additional attacks via the communications link between the UAV and GCS may be found in the up/down/control link section in this chapter.

Up/Down/Control Link

While the communications link between the ground control station and unmanned aerial vehicle is technically a communications interface, in this instance it is considered a separate subsystem of the UAS system given that it has its own separate vulnerabilities from the ground control station and unmanned aerial vehicle (Pastor and Lopez 2007, 5). Since the communications link between the GCS and the UAV is the most prominent point of attack, it required a great deal of attention regarding assessing the cybersecurity risk. This up/down/control link between the GCS and UAV is subject to a host of availability,

integrity, and confidentiality attacks which will be discussed later in greater detail. Some of the most common availability attacks committed against this communications interface are jamming and GPS spoofing. When jamming occurs, the communications are disrupted through either interference or collision. The outcome of this type of attack can delay or eliminate signals being sent to the ground station. This type of attack is very common due to the ease of adversaries being able to launch an attack with little knowledge about their target. Jamming is considered a denial-of-service attack that is either flooding the network or buffer overflowing. A flooding attack occurs when the network is flooded with illegitimate requests preventing the legitimate packets from being sent between the UAV and GCS. GPS spoofing is another attack that could be considered either an availability or integrity attack depending on the circumstance. As an availability attack, spoofing has the ability to take control of the UAV and direct it to another geographical location or alter the sensors' collected data. As an integrity attack, spoofing provides the opportunity to destroy the communications integrity by replacing the actual data with false, inaccurate data if there is no authentication to provide a layer of security. This type of attack would be the same as the attack illustrated in the UAV section where a live video feed would be replaced by a pre-recorded one. Finally, a confidentiality attack occurs when an adversary is able to intercept sensor data. When intercepting data, the adversary has the ability to eavesdrop on the up/down/control link or actively transmit the data to another third-party if there is no confidentiality security layer. Using these methods, the adversary could spy, in real-time on U.S. reconnaissance mission and forward the feeds to a third-party through accessing the UAVs camera (Pastor and Lopez 2007, 5–15).

External Factors

When developing a cybersecurity risk management decision matrix, there are many factors other than the GCS, UAV, tactical operators, and control links that need to be considered. Such factors include the current environment such as the distance between the GCS and UAV and geographical location. The distance between the GCS and UAV, or range, is an important factor since it will affect the signal strength at the UAV. The lower the signal strength at the UAV, the more susceptible to a successful attack. Similarly, the geographical location has an effect on the signal strength at the UAV. Obstructions in the

environment such as structures, mountains, and trees in line-of-sight communications will have an impact on signal strength which affects the probability of a successful attack. Another factor is the assumed threat environment that the UAS will be operating in and which adversary capabilities will likely be employed during the current mission. Additionally, the current and perceived states of the GCS, UAV, and data links need to be considered when making a cybersecurity risk assessment. While many of these factors may not directly be considered as cybersecurity vulnerabilities, these are all important things to consider when developing the cybersecurity risk management decision matrix due to their ability to influence risk to the mission.

D. RECENT ATTACKS

By examining recent RF and cyber-attacks carried out against UASs, a great deal of insight can be acquired about UASs threats and vulnerabilities. This section will cover two different attacks and the outcomes of those attacks. When creating a cybersecurity risk management decision matrix, the information gained from these operational scenarios help produce a set list of potential outcomes, provided by the cyber-attack input. This method of using the input to capture the output aids in creating a mapping to assign a risk to each type of attack. Since this research is explicitly focused on creating a method, architecture, and process, this same concept can be utilized when creating or updating a cybersecurity risk management decision matrix.

Iran Captures U.S. RQ-170 Drone

In 2011, a RQ-170 Sentinel UAV was captured by Iranian forces while conducting routine surveillance. According to Hartmann and Steup (2013), "it is theorized that a vulnerability in the UAV sensor system which effects the navigation system was used to attack the GPS system. The attack used details about the GPS functionality to attack the GPS system of the UAV by a "GPS-spoofing"-attack" (7). In GPS spoofing attacks, a spoofed GPS signal is transmitted from a local transmitter at a higher signal strength than the GPS satellite signal. The spoofed GPS signal contains incorrect, or altered, parameters that cause the GPS receiver to calculate an incorrect position. It is theorized that Iranian

militants used this GPS spoofing technique to cause the drone to land within Iranian territory where it could be collected.

In this scenario, the vulnerability in the UAV sensor system that controlled the navigation system was exploited to attack the GPS system. Understanding the vulnerabilities comprising of each subsystems' lower level components helps in identifying potential sources of exploitation and how it may affect other components and subsystems if exploited. This identification of threat can help build a more holistic view in assigning risk as it includes the entire system implications (outcome) rather than the single component. In this case, the GPS system was exploited through the sensor system which ultimately provided the operator faulty information about the UAV's current position. This would affect the way the operator carries out the mission, potentially leading to unintended outcomes such as crashes. In addition to the GPS system being attacked, the jamming of the satellite communication was highlighted as a secondary attack in the same scenario. This potential jamming affected the ground control station's ability to communicate with and control the UAV via the up/down/control link. This left the tactical operators at the ground control station unable to control the UAV since the interface between the GCS and UAV was severed. The outcome of these two attacks being realized allowed the UAV to be captured by the adversary which poses a significant risk if information is extracted from the UAV. To summarize, the GPS spoofing attack and jamming of satellite communications, the inputs, led to the capture of the UAV, the outcome. Commands may use information from this scenario to help assign risk to the input by associating it with the impact of the outcome (the UAV being captured).

Hacking of U.S. Drone Video Feeds

There is evidence that U.S. UAV video feeds have been hacked by Iranian backed Shiite militants in Iran, Iraq, and other areas in the Middle East. According to Benson and Sefanov, Iranian militants used a software program, created by a Russian company called Skygrabber, which "allows users to take advantage of unprotected communications links such as those used in UAV's" (Benson and Sefanov 2009, 1). The United States has normally operated with drones using unencrypted video links without issue, especially in

third world countries where the adversaries did not have the technology to hack into these feeds. According to Hartmann and Steup, the UAV communications used operationally by the United States were normally not encrypted because encryption slowed down the link and reduced the real time situational awareness (Hartmann and Steup 2013).

This evidence of multiple militant groups being able to hack UAV video feeds using a software program designed to exploit unprotected communications links shows another example of how critical the up/down/control link between the GCS and UAV is. While the hacking of U.S. UAV video feeds and the capturing of the U.S. RQ-170 drone attacks are both executed through the same up/down/control link interface, the method of implementing the attack and end results are different. While the hacked video feeds provide the adversary with information on what the U.S. is surveilling, the adversary lacks the ability to control the UAV and capture it. The end result is not desired, but the tactical operators would still have control of the UAV via the GCS. In this scenario, the outcome of having the hacked video feeds would likely have an assigned risk to mission classified as lower than having the UAV captured by the adversary. The outcome in this case is the U.S. providing the adversary insight into their surveillance activities. Understanding the risk in a situation like this also provides the tactical operators the ability to make an informed tradeoff on whether the mission requires more of a real time situational awareness or the ability to keep its surveillance activities hidden through encryption with a slowed down link. This tradeoff could be quantified through the use of the cybersecurity risk management decision matrix.

Interpretation of Attacks

The Iranian capture of the U.S. RQ-170 drone and the hacking of U.S. drone video feeds both illustrate the need for a quick response to such actions at the tactical level. It shows that adversaries of the U.S. are capable of mounting cyber-attacks for the gain of intel or to disrupt operations. Unless the tactical operators have clear guidance on what to do in the event similar attacks like these occur, it leaves them more exposed to the worst-case scenario for each attack. With a method to determine what to do during such an event, measures can be taken to either reduce the severity of the attack or make a decision to keep

operating despite an attack occurring if the level of risk is deemed acceptable. The cybersecurity risk management decision assessment matrix is a tool intended to fulfill the need of the tactical operator deciding whether the risk is too great to continue a mission or what other possible actions can be taken to address the risk in a time critical manner.

Inputs to Cybersecurity Risk Management Decision Matrix

Utilizing the decomposition of the UAS, determining its vulnerabilities, and analyzing recent attacks allows the project team to develop a comprehensive list of input categories for the cybersecurity risk management decision matrix. These categories are separated by the protocol's type of attack, the protocol's vulnerability, and information about the operational environment. For demonstration purposes, the cybersecurity risk management decision matrix architecture includes inputs such as cyber-attacks, cyber attack symptoms, and operational environment to the matrix. These inputs will be discussed in further detail in Chapter III, where the cybersecurity risk management decision matrix architecture is discussed.

UAS Vulnerabilities

When performing the functional analysis, many UAS vulnerabilities are used to help develop the inputs to the cybersecurity risk management decision matrix. The vulnerabilities are focused on each of the subsystems of the UAS, the GCS, UAV, operators, and the communications link. These vulnerabilities are displayed in Table 7.

Table 7. UAS vulnerability types. Adapted from Mansfield et al. (2013, 6).

UAS Vulnerability Types	
GCS	Hardware
	Software
	Backend Network
	Removable Media
Communications Link	
UAV	Hardware
	Software

The three vulnerabilities of the GCS are the hardware components, software, and the GCS's backend network, and the base station. Additionally, the tactical operators using the GCS add other vulnerabilities to the GCS such as removable media and social engineering. The UAV's vulnerabilities also consist of hardware and software. In addition to the GCS and UAV, the communication link between them possesses a host of vulnerabilities. Each one of the vulnerabilities presented in the table will be discussed further in the subsequent subsections for each UAS subsystem.

Ground Control System

The ground control station is subject to hardware, software, and communication network attacks. If the GCS is a mobile smart device in a hardware attack, different sensors in the smart device such as the camera, GPS, and microphone give the attacker the ability to locate or monitor the UAS operator. The attacker can achieve these results through malware, software, or other vulnerabilities in the software application or operating system. Hardware attacks may include draining the smart device's battery and surveilling operator actions (Mansfield et al. 2013, 5). The GCS is also vulnerable to software attacks. These attacks include malware and data leakage. Through these attacks, the adversary can gain

access to vital information such as "real-time avionics, flight display, navigation systems, system health monitoring and prognostics display, graphical images and position mapping, and inward data processing to control and operate the UAV" (Mansfield et al. 2013, 6). The adversary may also be able to manipulate sensors, monitor the smart device, tap conversations, and view sensitive information through these software attacks. "Finally, communication network vulnerabilities include eavesdropping, spoofing, denial of service, and jamming" (Mansfield et al. 2013, 6). Since many operational scenarios will be in remote locations, a base station may be required. In the event the network connection between the base station and the ground control station is severed, the connection between the GCS and UAV will be disrupted. This vulnerability in the communication network is similar to the communication link between the GCS and UAV which will be discussed further in the UAV subsection. Table 8 shows a quick reference for the GCS's vulnerabilities with its associated threats.

Table 8. GCS vulnerabilities. Adapted from Mansfield et al. (2013, 6).

GCS Vulnerabilities and Associated Threats	
Vulnerability	Threat
Hardware	Battery Exhaustion
	Social Engineering
	Surveillance
Software	Malware
	Social Engineering
	Data Leakage

UAV

The UAV is host to hardware, software, and communications link vulnerabilities. The vulnerability points in the hardware include video cameras, infrared sensors, thermal sensors, and more (Pastor and Lopez 2007, 21). These pieces of hardware make it possible for attackers to perform availability or integrity attacks that can turn off sensors, spy through video feeds, and even modify data from the sensors (Vasconcelos et al. 2016, 2). Since many UAVs utilize software for pre-programming flight paths introduced by a computer or other smart device, UAVs may be injected with malware by an adversary. With the malware installed on the flight computer, the adversary has the ability to reprogram the flight computer and control the UAV (Sanchez et al. 2019, 1). Table 9 shows a breakdown of the UAV's vulnerabilities and its associated threats.

Table 9. UAV vulnerabilities. Adapted from Mansfield et al. (2013, 6).

UAV Vulnerabilities and Associated Threats	
Vulnerability	Threat
Hardware	Surveillance
Software	Malware
	Data Leakage

Communication Link

The biggest cybersecurity vulnerability to UAS is the communications link, which is also referred to as the command and control (C2) link. In this instance, we are referring to the communications interface between the GCS and UAV. The most common threats posed to the C2 link are jamming, when communications are interrupted through interference, and GPS spoofing, which allows an adversary to take control of the UAV and either move it or alter the UAV's sensors data (Vasconcelos et al. 2016, 2). Other

vulnerabilities in availability of the communication link and their associated threats are shown in Table 10.

Since consistent threats posed to the UAS come in the form of jamming and spoofing, C2 and GPS links are key inputs to the matrix. While GPS is not the only global navigation satellite system, it is the preferred method in the United States. Given this research focuses on COTS UASs used by the U.S. military, other subsystems of the global navigation satellite system are not covered. On the other hand, while software vulnerabilities are present on both the GCS and UAV, it is decided that these will not be included in the cybersecurity risk management decision matrix. This is because software threats may be preemptively minimized through the operator's adherence to procedure; in many cases, operators follow strict protocols to reduce cybersecurity risk on their computers and smart devices. Moreover, the focus on this work is on a tactical decision risk matrix related to real-time attacks during normal operation, while software exploits are likely to rely on attack stages prior to the UAV flight operation. Similarly, while there are hardware vulnerabilities on both the GCS and UAV, and these are also not included in the cybersecurity risk management decision matrix. This is due to the fact that most of the hardware vulnerabilities exploited in attacks are either a) through the communications link which is already determined to be a part of the matrix architecture, or b) through supply chain and other initial attack stages which are prior to the tactical operation. As with software mitigation, the threats in b) may be preemptively minimized prior to operation through following procedure.

Table 10. Communication link vulnerabilities in availability. Adapted from Mansfield et al. (2013, 6).

Communication Link Vulnerabilities in Availability and Associated Threats	
Communications Link	Eavesdropping
	Spoofing
	Denial of Service
	Jamming

Operators

While tactical operators may pose a cybersecurity risk to the UAS, they will not be factored into the cybersecurity risk management decision matrix because it is assumed that the tactical operators will be acting in good faith. Additionally, the tactical operators will be the ones using the cybersecurity risk management decision matrix, which means they are a variable to cybersecurity risk that already understand their role in safely maintaining and securing the UAS. The tactical operators also have little to do with the calculation of the cybersecurity risk management decision matrix since the cybersecurity risk they pose is through the GCS by using removable media or downloading software updates with malware or viruses.

Utilizing the decomposition of the UAS, determining its vulnerabilities, and analyzing recent attacks allows the development of a comprehensive list of input categories for the cybersecurity risk management decision matrix. Since the communication link between the GCS and UAV is a major component of the research, the cybersecurity risk management decision matrix focuses on the communication link and its different protocols. These categories are separated into potential attacks against the chosen protocol, the protocol's vulnerabilities, and information about the operational environment. These inputs will be discussed in further detail in Chapter III, where the cybersecurity risk management decision matrix architecture is discussed.

E. SUMMARY

This chapter provides an overview on the chosen approach for the development of the cybersecurity risk management decision matrix. Utilizing the needs and functional analysis, different factors that could affect the risk level of the UAS are identified by scoping the initial needs statement of the stakeholder. These identified factors and the scoping of the problem enable the systems engineering team to bound the problem. All of the information gathered during this process is used in the development of the cybersecurity risk management decision matrix. Since the chosen systems engineering approach is an iterative process, these analyses are revisited during different phases during product development to ensure stakeholders needs are being met.

THIS PAGE INTENTIONALLY LEFT BLANK

III. MATRIX ARCHITECTURE

The decision matrix will act as a tool for the operator to assess the cybersecurity risk of the COTS UAS being used for the operation. The purpose of this chapter is to provide a high-level overview of the inputs, constants, architecture, and outputs of the cybersecurity decision matrix. This chapter will first provide a high-level overview of the inputs and constants to the matrix. The internal architecture and thought process behind the matrix will then be described. This will be followed by a description of the outputs of the matrix.

Figure 6 is the action diagram for the matrix, which displays the steps and high-level interactions that occur when the matrix is used. As shown in the diagram, the operator will enter the inputs. The operator-entered inputs as well as constant inputs (not entered by the operator) will act as inputs to the matrix. The matrix will receive the inputs and develop and display the corresponding outputs. The matrix outputs will serve as an input to the operator receiving the matrix outputs.

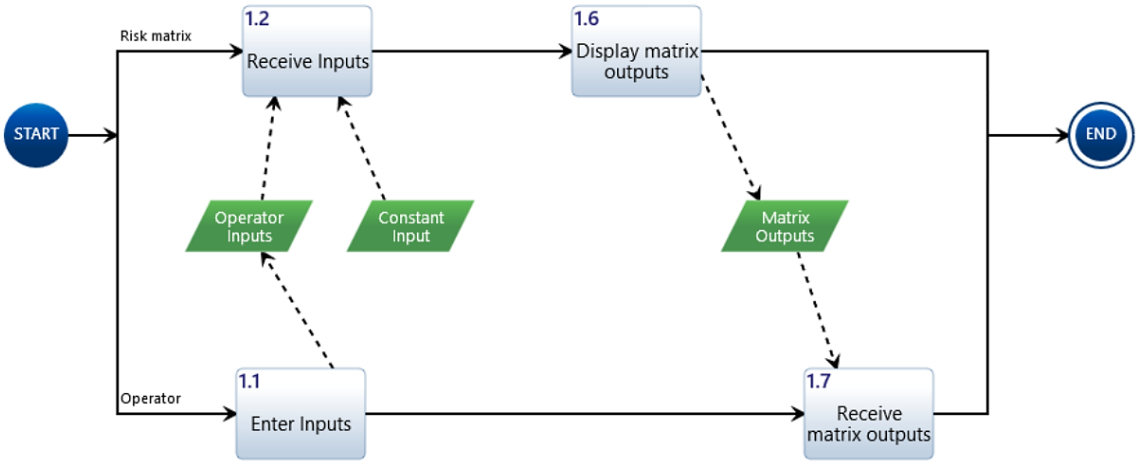

Figure 6. Matrix operation action diagram.

A. MATRIX INPUTS AND CONSTANTS

Figure 7 is a diagram of the inputs, constants, and outputs of the decision matrix that will be discussed in this section. The elements of the matrix shown in the diagram represent the vulnerabilities, threats, and operator information which are derived from the decomposition and analysis conducted in Chapter II. Each element is described in detail in the following sections of this chapter.

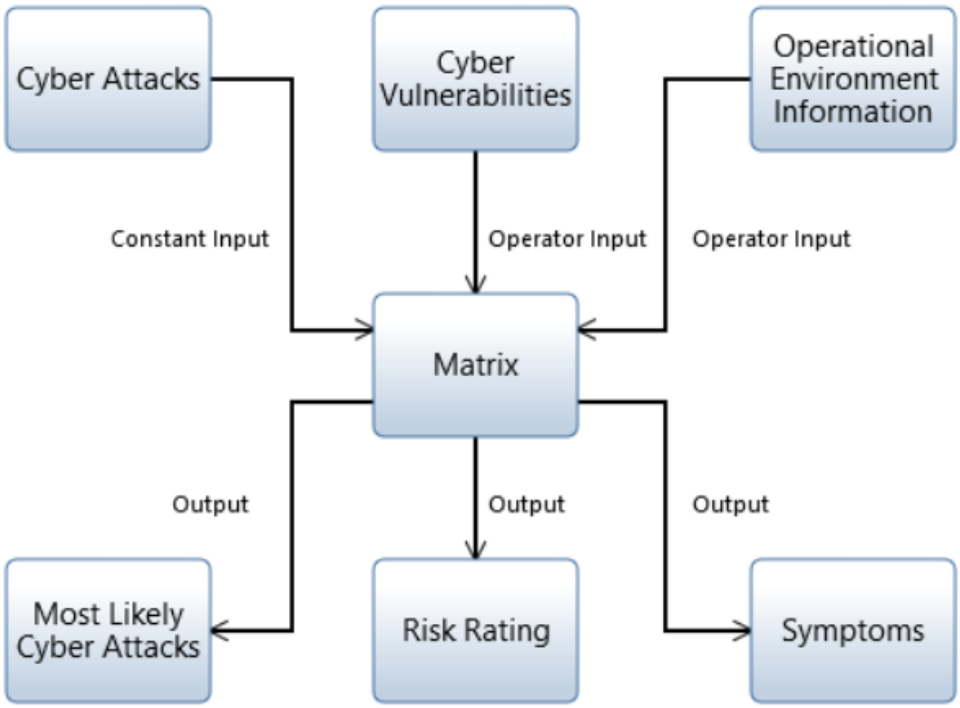

Figure 7. Matrix input/output diagram.

Matrix Operator Inputs

The operator inputs the cybersecurity relevant parameters of the mission into the matrix, split into two major categories: cyber vulnerabilities and operational environment information. These inputs are chosen based on the architecture of a UAS and past cyber-attacks which were discussed in the previous chapter. The most common method of cyber-attack is against the RF communication links of the UAS and focuses predominantly on the associated vulnerabilities, namely the vulnerabilities associated with the C2 and GPS

link, which are the most accessible vulnerabilities when separated from the UAS. There are additional cyber vulnerabilities that may be relevant from a cybersecurity perspective; however the vulnerabilities associated with C2 and GPS are the most prevalent, based both on past attacks and the typical loadout of COTS UAS's, and therefore are the main focus for this effort. Operational environment information is the second operator input to the decision matrix and includes a variety of additional inputs that impact the ability of an adversary to successfully conduct a cybersecurity attack. The inputs include the adversary, expected UAS range from the operator, and geography.

For both C2 and GPS there are a variety of different modes and protocols that can be used in a particular UAS. Each mode or protocol has different a different type of security and therefore different types of vulnerabilities. Each C2 link and GPS mode that is available for the operator to use will be assigned a numerical value based on its assessed level of vulnerability that will be used within the matrix to identify the level of risk associated with it. The operator will input both the GPS mode and C2 link method that they are using in the mission. In the same way, the operational environmental information also affects the vulnerability of the UAS and will also be input by the operator into the matrix. The additional inputs will vary the numerical risk assigned to the C2 and GPS vulnerabilities based on their effect on the overall risk. Figure 8 displays the matrix input hierarchy. It shows the decomposition of the top-level operator input which consists of both the cyber vulnerabilities and the operation environment information. The cyber vulnerabilities are separated into the two vulnerability areas which are the vulnerabilities associated with the C2 Link and GPS mode.

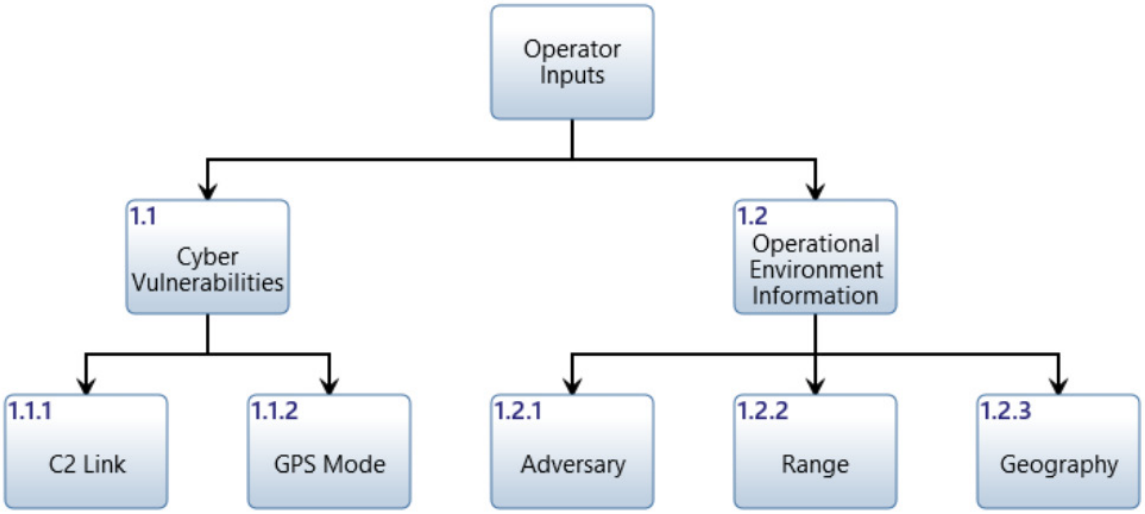

Figure 8. Matrix operator inputs hierarchy diagram.

Matrix Constants – Cyber Attacks

The decision matrix will contain a constant list containing all of the cyber-attacks that have been identified through research. The list of cyber-attacks will serve as a constant input to the matrix in the sense that they are used to develop the outputs but are not manually input by the operator. The list will include two groups: C2 attacks and GPS attacks. The attacks will vary in ease to employ, based on the required technical capability of the adversary. Those included in the list will differ in effectiveness based on the C2 link and GPS mode that the operator has chosen for the mission. Each will also be assigned a risk rating based on their overall effectiveness which will be used in the calculation of risk. Figure 9 displays the Constant Input Hierarchy which shows the decomposition of the Constant Inputs.

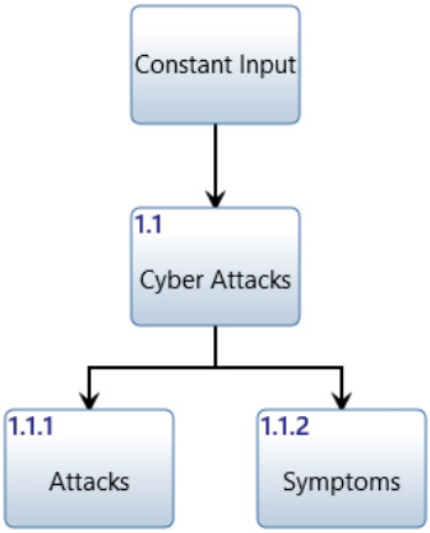

Figure 9. Constant matrix inputs hierarchy diagram.

B. MATRIX ARCHITECTURE AND OUTPUTS

The purpose of this section is to describe the relationship between the inputs and constants of the matrix and identify the thought process behind how the outputs of the matrix are determined from those inputs. Figure 10 provides a hierarchy diagram of the matrix outputs. It displays the subsets of the top-level matrix output which consists of the risk rating, most likely cyber-attacks, and the symptoms of the cyber-attacks. Figure 11 displays how each input feeds into each output; each output will be stepped through with an explanation of how the output is derived later in this section.

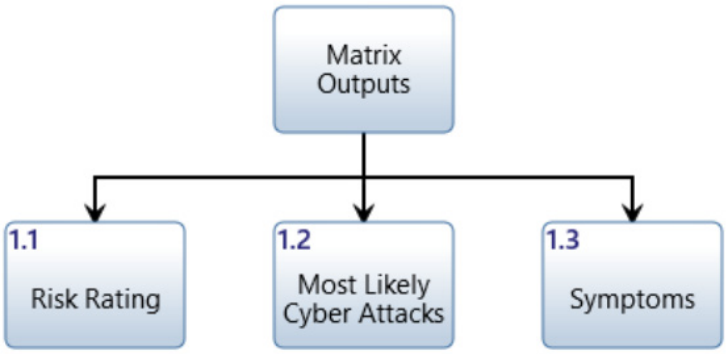

Figure 10. Matrix output hierarchy.

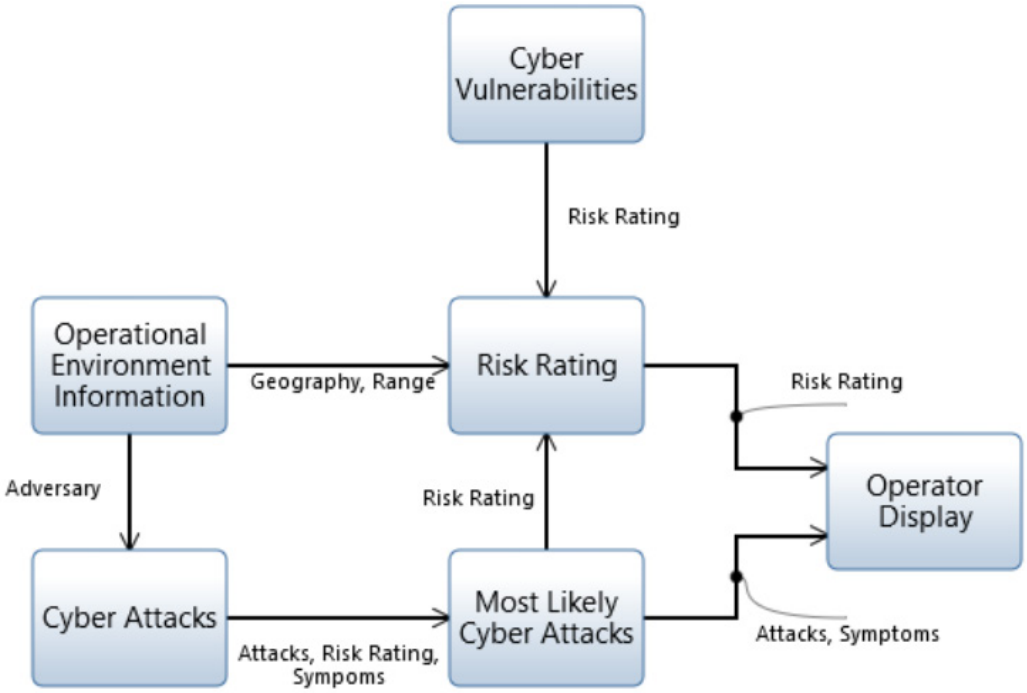

Figure 11. Matrix internal architecture input/output diagram.

Most Likely Cyber Attacks and Symptoms

The first output of the matrix will be the list of the most likely cyber-attacks and their corresponding symptoms. The list of most likely cyber-attacks is derived from a combination of the constant input "cyber-attacks" and the operator input "adversary." As described in the previous section, each attack varies in the technical requirements and equipment needed to conduct the attacks. This means that some adversaries will be able to conduct all of the attacks while some adversaries will only be able to conduct the lower level attacks. For instance, an insurgent group with limited resources will only be able to conduct the simple attacks in the list while a near-peer adversary will be able to conduct all of the attacks, both simple and sophisticated. In this sense, the adversary input by the operator will act as a gating mechanism to the constant input list of cyber-attacks. The most likely cyber-attacks, based on the adversary's capability, will be provided as an output to the operator. In addition to the list of most likely cyber-attacks, the symptoms of each attack will also be provided, acting as a queuing mechanism for the operator to identify if and when one of the potential attacks has been initiated on the UAS.

Risk Rating

The last output is risk, which is a numerical value that will be associated with each of the most likely cyber-attacks and displayed to the operator in one of three categories: high, medium, or low. As stated in the previous section, each of the operator inputs which include C2 link and GPS mode will have an assigned risk rating identifying the level of vulnerability associated with it. The additional operator inputs such as range, geography, etc., will augment the risk rating assigned to the operator input GPS mode and C2 link. In the same method, each cyber-attack in the constant input list will also have a risk rating assigned to it based on its effectiveness. The final risk rating for each attack will be based on the combination of the numerical risk values for the C2 link and GPS modes augmented by the operational environment inputs and compared to the risk rating for each of the most likely cyber-attacks derived from the comparison of the operator input adversary and the constant input cyber-attacks.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. EXAMPLE DECISION MATRIX

The purpose of this project is to provide the architecture, methodology, and process for the end user to create their own cybersecurity risk matrix using real world information and operational expertise. The following chapter will provide a detailed example of the creation of a risk matrix. The example matrix defined in this chapter is not meant to be operationally valid, nor should it ever be used in an operational scenario. The operator will have more accurate and relevant operational information on the matrix inputs that is not available to the public due to the sensitivity of the information. For instance, the operator will have specific information such as the potential adversaries and their technical capabilities, the C2 and GPS modes available for use, and the potential cyber-attacks that may be conducted. The purpose of this chapter is to define the thought process behind the creation of the matrix and to serve as an example of how the end user would go about defining inputs, assigning risk ratings, and developing the risk outputs.

A. MATRIX INPUTS

Risk Rating Combinations

Each step in the matrix will require a comparison of risk ratings to determine the overall cybersecurity risk of each of the most likely cyber-attacks. According to Lowrance (1976), risk is the measure of the probability and consequence of a particular event. The derivation of risk will require the calculation of both variables as well as the final risk determination. Table 11 identifies the solution key for each comparison of rating and will be used as the rubric as for each step in the matrix.

Table 11. Risk rating comparison key.

Risk Variable Combinations	**Low**	**Medium**	**High**
Low	Low	Medium	Medium
Medium	Medium	Medium	High
High	Medium	High	High

1. Operator Input – Cyber Vulnerabilities

As stated in Chapter III, the operator input consists of the communication link and GPS mode. The scope of the example matrix, in terms of communication link, was limited specifically to Wi-Fi. The project team will proceed to introduce Wi-Fi vulnerabilities in the context of general communication vulnerabilities, specific Wi-Fi protocol details, and specific Wi-Fi security and attacks. A set of options for each was generated and each was assigned a risk rating. The rationale behind each risk rating is defined in this section through the comparison and discussion of each of the options. Note that the descriptions and comparisons made in this section may be valid, however the exact risk rating that each is assigned may or may not be valid. As stated in the introduction to the chapter, the purpose of this example matrix is simply to provide an example to the end user on the approach to putting together their own matrix. Therefore, we allow that the specifics of this example matrix may or may not be valid.

Communication links

1) Types of communication link attacks

UAV communication links are susceptible to many different threats. Since there are many cyber-attacks and potential for new ones to be developed, attacks are categorized by types of attacks availability, integrity confidentiality and access control attacks. This section will describe each category of attack.

a) Attacks on Availability

Availability guarantees that systems, applications, and data are available to users when they need them. Availability attacks on the communication links are the interruption of access to information, system, devices or other network resources, and are more generally known as Denial of Service (DoS) attacks: jamming, flooding and de-authentication are examples of DoS attacks. A common attack vector for DoS is to ensure that the device or network is too busy processing fake requests that it fails to process the legitimate requests. Eavesdropping can be used to disrupt routing or degrade application performance.

Buffer overflow is a form of DoS attack. In a Buffer overflow attack the buffer memory of network cards on the devices being used in the system is flooded. Vasconcelos et al. (2016) show that a buffer overflow attack can be used to take down an UAV. The buffer overflow attacks performed compromised the video streaming application and computer vision application.

Jamming in wireless networks is overpowering wireless signals with a stronger signal. The attacker jams the wireless network frequency by emitting a strong radio signal which causes the target device to become useless. After a jamming attack is performed WLAN is inaccessible. Parlin, Alam and Moullec (2018) demonstrate that sweep jamming can completely disable WLAN communication. After the successful jamming attack, the UAV did not respond to the operator's commands.

Flooding basically floods the network with packets by continuously sending multiple packets. Beacon flooding is an example of flooding where an attacker "overloads the network by flooding it with thousands of illegitimate beacons so that the wireless AP is busy serving all the flooding packets and cannot serve any legitimate packets" (Waliullah and Gan, 2014, 181). Vasconcelos et al. (2016) show that a flood attack on an UAV can lead to loss of control. The operator may see the UAV crash, fly away or stall in place.

A de-authentication attack sends disassociate packets to a client. In this attack, the attacker acts as a client or access point and floods the target thousands of de-authentication frames which forces them to exit the authentication state. This attack can be used to generate ARP request or capture handshakes by forcing clients to reauthenticate. Fournier et al. (2017) demonstrate that the implementation of a de-authentication attack on an UAV can lead to compromised data as well as loss of control. Legitimate users of the UAV are disconnected and prevented reconnection. Some symptoms the operator may see the UAV crash or stall in place.

b) Attacks on Integrity

Integrity ensures that transmitted data is accurate and is not modified by unauthorized personnel. Integrity attacks either modify data being sent or fabricate

malicious data to replace legitimate data. Example types of integrity attacks include replay attacks, injection attacks, and packet modification.

A replay attack is when an attacker intercepts data transmission resends it. The network's security protocols handle the attack as an authorized data transmission. Sanchez et al. (2019) demonstrate that "replay attacks can be performed by replacing the real data coming from the sensors with previously recorded data causing performance degradation, loss of control, and allow an attacker to perform undetectable physical attacks." The Operator may see a latency in UAV control or video, video replay, the UAV stall, continue to fly in one direction, or crash.

Injection Attacks are a range of attacks where a device is inputted with data, which alters the system, falsifies device data, or fabricates operator commands. In a frame injection attack, intruders capture or send forged 802.11 frames into the middle of the transmission. Abbaspour et al. (2016) show how an injection attack can be leveraged to take the control of the UAV or interrupt it. This attack is leveraged by injecting faults into the UAV. Some symptoms the operator may see include the UAV flying in a different direction from what was directed, the camera disabled, UAV crash or shut down.

In packet modification, an attacker alters the packet information in order to find entry points, test network device's behaviors, check firewall rules and test a network. An attacker uses a MitM to observe packets, then modifies the packets and sends them to the target device. Destination address, source address, protocol type, data, version, and length are contained in a network data packet and are modifiable under a successful attack. Attackers can use packet modification to launch a DoS attack. For example, a standard ICMP ping packet can be modified to more than 65,535 bytes, which is the maximum allowed in a packet. The destination system responds with an echo reply, which in return consumes a larger packet frame and ultimately results in a DoS.

c) Attacks on Confidentiality

Confidentiality ensures that data exchanged is not accessible to unauthorized users. In these attacks, the attacker compromises the confidentiality by intercepting confidential or sensitive data. An example of a confidentiality attack is eavesdropping.

In an eavesdropping attack, the attacker has access to network traffic and tries to read the contents of messages that are being transmitted across the network. The attacker passively monitors network communications to gain access to sensitive information, either by observing unprotected information or by breaking the confidentiality protection mechanism (e.g., encryption). Samland et al. (2012) show that a UAV video stream can be susceptible to eavesdropping which could lead to confidential data being revealed. The operator may not see any change in UAV behavior when an eavesdropping attack is occurring.

d) Attacks on Access Control

Access control is used to control access to the information users can see and use by using authentication and authorization. Authentication is used to verify the identity of a user or device and to differentiate an authorized user from an unauthorized user. Authorization refers to the level of access granted to each user. If there is poor network access control on the network, it can leave the network vulnerable to attacks. Common types of attacks on access control are rogue access points, unauthorized access, and MitM attacks.

A MitM attack is when an attacker intercepts communication while sitting between two devices in order to eavesdrop or modify traffic. MitM attacks are a general classification for a wide range of methods and potential outcomes. One example is an attacker using DNS spoofing by altering a website's address within a DNS server. Then the attacker waits for a user to unwittingly visit the fake site in order to steal the user's information.

A rogue access point acts as an unauthorized access point that has been added to the network. With a rogue access point an attacker may compromise data, destroy data, disable network services, or upload viruses. In this attack, an attacker introduces an unauthorized access point and acts as a legitimate access point to intercept traffic from valid wireless clients. For example, the attacker could use the same Wi-Fi network name as the legitimate Wi-Fi network. Then the user may unknowingly connect to the rogue access point, thus an unwanted backdoor into a network is created. Karimibiuki et al.

(2019) show that an attacker can eavesdrop on the communication between the UAV and controller. They established a connection by scanning for access points used by the UAV with a rogue access point. After imitating the UAV's access point, the GCS will connect to the attacker's rogue access point. After the connection is made the attacker can monitor activity while the operator is unaware. MAC address spoofing is another example of a rogue access point attack. In this attack, the attacker gains access to confidential information and resources by using the identity of a valid user in the network by reconfiguring their MAC address to match the MAC address of the target device. After the MAC address is matched, the attacker sends traffic through the network causing the MAC address to overwrite the existing table entry with the attacker's entry. After the table is updated the target device will not receive any traffic until it sends traffic. Kamkar (2013) demonstrates how a drone can be hijacked using this attack. First, he locates the hardware MAC address for an AR Drone 2.0 quadcopter he is operating. Then he searches for local Wi-Fi signals that are connecting to that MAC address. After discovering UAVs nearby, he de-authorizes the Wi-Fi signal controlling the target UAV and establishes his UAVs Wi-Fi as the Wi-Fi access point controlling the target UAV. Once the target UAV connects to the attacker's UAV, the attacker can take control of the target UAV. The operator may see the UAV fly away or crash.

Unauthorized Access is when the attacker illegally gains unauthorized access to the services. Password theft is a common method used by attackers to gain unauthorized access to a system. Once an attacker gains access to the internal network, they can retrieve information, interfere with communications, or change the system. Vanunu, Barda and Zaikin (2018) discovered that the drone company DJI used the same cookie to identify and offer access to several of its platforms. They showed how an attacker can steal this cookie and use it to access DJI's camera and sensitive information such as flight videos, flight altitude/speed, home location and flight logs.

Evil Twin attacks behave similarly to a rogue access point, using an access point configured identical to the legitimate wireless network to entice users to connect to the spoofed network. The Evil Twin attack poses a significant risk to cybersecurity. Legitimate users may connect and log into an Evil Twin Wi-Fi hotspot thinking it is a legitimate access

point. The hacker behind the Evil Twin attack can obtain login credentials, steal data, or plant malware. Vemi and Panchev (2016) show how an UAVs wireless connection can be hijacked using an Evil Twin attack. They see what networks the UAV have accessed in the past and pretend to be one of those old network connections. Connecting to the UAV without authentication or interaction, the attacker has access to login credentials and other sensitive data. The operator may not detect that this attack is happening if the attacker is just eavesdropping. If the attacker gives the UAV commands the operator might see the device taken over.

e) Other

Traffic Analysis is a technique where an attacker intercepts, records and analyzes the network activity. During a traffic analysis attack, the attacker can discover packet information such as the size of the packets, the source and destination of the packets being transmitted and received and the number of packets being transmitted and received by monitoring the network communication. Deng, Han and Shiyakant (2005) show that attackers can determine the location of the base station by generating events and monitoring where sensor nodes forward the packets. Sciancalepore et al. (2019) show that status (the battery level of an UAV, current video, return to home location, etc.) can be revealed by performing a traffic analysis on the communication traffic exchanged between the drone and GCS.

A downgrade attack is when an attacker forces a device to switch to an unprotected or less secure data transmission standard. A downgrade attack leads to a weakened security, which can be leveraged to break confidentiality or integrity. If used to break confidentiality, the communication link can be susceptible to eavesdropping which could lead to confidential data being revealed and the operator may not see any change in UAV. If used to break integrity, the operator may see a latency in UAV control or video, video replay, the UAV stall, continue to fly in one direction, or crash.

f) Communication link attack risk rating

Based on the rationale and comparisons of the different types of communication link attacks defined in this section, risk ratings based on outcome consequence can be

assigned. The risk ratings are assigned as high, medium, or low. Access control attacks was assigned a risk rating of high because they have the highest impact. The Confidentiality and Integrity attacks were assigned a risk rating of medium. Availability has a risk rating of low because the impact of these attacks are relatively low. Table 12 shows the rankings and risk values of each of the Wi-Fi protocols discussed in this section.

Table 12. Communication link attack risk rating.

Type of C2 Attack	**Consequence of Outcome**	**Required Technical Capability**	**Symptoms**
Availability	Low	Low	- Loss of connection - Loss of control - Loss of network resources
Integrity	Medium	Medium	- Loss of connection - Altered C2 communications - Loss of control - Altered data
Confidentiality	Medium	Medium	- Loss of data
Access control	High	High	- Loss of connection - Altered C2 communications - Loss of control - Altered data - Loss of data

2) Wi-Fi protocols

In order to control a UAV remotely, wireless communication is necessary. There are a wide range of communication systems that allow the communication between the UAV and GCS. Common communication links include Wi-Fi, cellular protocols, Bluetooth, and satellite connections. The majority of the UAVs that was researched for this paper use Wi-Fi. Table 13 shows 15 out of the 25 randomly sampled UAVs use Wi-Fi as a wireless communication. Therefore, the emphasis is on the Wi-Fi standards used for the communication link between UAV the GCS. Cellular protocols and Bluetooth are commonly used in UAVs, but the project team decided to scope it out of our research due

to project time constraints and in the interest of supporting a greater in-depth analysis Wi-Fi risk. Proprietary protocols are not covered because information on these protocols are not public knowledge.

Table 13. Communication links of COTS UAS.

	UAV	**Wireless communication used**	**Wi-Fi protocol supported**	**Wi-Fi Security supported**
1	DJI Mavic 2	DJI OcuSync 2.0 (Proprietary)	n/a	n/a
2	DJI Mavic Mini	Wi-Fi	802.11ac	WPA2
3	SIMREX X300C 8816	Wi-Fi	802.11g/n/ac	WPA, WPA2
4	Potensic T18	Wi-Fi	802.11a/b/g/ n/ac	WPA, WPA2
5	GAOAG GPS RC	Wi-Fi	802.11a/b/g/ n/ac	WPA, WPA2
6	Teeggi Visuo xs809hw	Wi-Fi	802.11a/b/g/ n/ac	WPA, WPA2
7	Holy Stone HS200	Wi-Fi	802.11a/b/g/ n/ac	WPA, WPA2
8	DROCON U818PLUS	Wi-Fi	802.11a/b/g/ n/ac	WPA, WPA2
9	Potensic D80	Wi-Fi	802.11a/b/g/ n/ac	WPA, WPA2
10	LOHOME MJX Bugs B2SE	Wi-Fi	802.11a/b/g/ n/ac	WPA, WPA2
11	DJI Mavic Air	Wi-Fi	802.11a/b/g/ n/ac	WPA, WPA2
12	DJI Mavic Pro	Wi-Fi	802.11a/b/g/ n/ac	WPA, WPA2
13	DJI Phantom 4	DJI Lightbridge (Proprietary)	n/a	n/a
14	Parrot Bebop 2	Wi-Fi	802.11a/b/g/ n/ac	WPA2
15	Parrot Anafi	Wi-Fi	802.11a/b/g/ n/ac	WPA2
16	DJI Inspire 2	DJI Lightbridge (Proprietary)	n/a	n/a
17	DJI Inspire 1	DJI Lightbridge (Proprietary)	n/a	n/a

	UAV	Wireless communication used	Wi-Fi protocol supported	Wi-Fi Security supported
18	Freefly Alta 8	Wi-Fi	802.11b/g/n	WPA, WPA2
19	Flyability Elios 2	OFDM	n/a	n/a
20	DJI Agras MG-1	DJI Lightbridge (Proprietary)	n/a	n/a
21	senseFly eBee Classic	None	n/a	n/a
22	DJI Matrice 200 V2	DJI OcuSync 2.0 (Proprietary)	n/a	n/a
23	DJI Phantom Multispectral	DJI OcuSync (Proprietary)	n/a	n/a
24	DJI Phantom 4 Pro V2.0	DJI OcuSync 2.0 (Proprietary)	n/a	n/a
25	Skydio 2	Wi-Fi	802.11a/b/g/ n/ac	WPA, WPA2

In order to have constant usage of a UAV, it is necessary to have a simple, reliable and widely available data link, such as the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards. The IEEE 802.11 is set of standards used when implementing wireless local area network (WLAN). Wi-Fi works in two radio bands, the 2.4 GHz frequency (802.11b/802.11g/802.11n) as well as the 5 GHz frequency (802.11a/802.11ac). The 802.11a, 802.11g, 802.11n, and 802.11ac standards will be discussed individually.

a) 802.11a

One of the first Wi-Fi standards developed in the IEEE 802.11 is the 802.11a standard. The 802.11a uses an Orthogonal Frequency Division Multiplex based air interface along with the same data link layer protocol and frame format as the initial standard. Due to the high operating frequency of 5GHz the 802.11a is less susceptible to interference compared to the 802.11b which is more susceptible to interference.

b) 802.11b

The IEEE 802.11b standard was released along with the 802.11a standard but uses the 2.4 GHz frequency band. The Carrier Sense Multiple Access/Collision Avoidance

technique that was defined in the original 802.11 is used in 802.11b. This 802.11b experiences interference from other products operating in the 2.4 GHz frequency.

c) 802.11g

The 802.11g standard is an IEEE standard Wi-Fi wireless networking technology that uses the same Orthogonal Frequency Division Multiplex scheme as the 802.11a standard but operates in the 2.4GHZ frequency. Hardware Interference vulnerabilities can be mitigated by the OFDM encoding digital data on multiple carrier frequencies. Although the Orthogonal Frequency Division Multiplex mitigates some interference, devices still experience interference from other products operating in the 2.4 GHz frequency.

d) 802.11n

The 802.11n standard was developed in 2009. The 802.11n standard was developed to enhance network security and reliability, increase the speed of wireless networks as well as extend the range of wireless transmissions. The 802.11n standard uses the antenna technology MIMO (multiple input, multiple output) to transmit and receive data. MIMO is the ability to coordinate multiple simultaneous radio signals. As a result, both the wireless transmission range and throughput of a wireless network are increased. The 802.11n standard can operate on both 2.4GHZ and 5GHZ frequencies which mitigates interference. A negative to the extended range is that it can increase the possibility for an attack to occur because an increased range opens up the Wi-Fi to be attacked from a greater distance.

e) 802.11ac

The 802.11ac standard is an amendment to IEEE 802.11 that builds on 802.11n. The amendments made to the 802.11n standard are broader channels in the 5 GHz band, more spatial streams, higher-order modulation, and the addition of Multi-User MIMO. The Multi-User MIMO increases network speed and decreases interference. As Han (2014) indicates "The 802.11ac supports the multiuser MIMO (MU-MIMO) mode, in which multiple clients can be served concurrently without interfering with each other, achieving multiplexing gain even for those clients with a single antenna" (1). Although increased network speed creates faster data transfer for users, it also can be susceptible to faster

malicious traffic. An adversary can get into the network and have the opportunity to extract data more quickly. Interference still occurs on the 802.11ac standard.

f) Wi-Fi standard risk rating

Based on the rationale and comparisons of the different Wi-Fi standards defined in this section, risk ratings can be assigned. According to Abdelrahman, Mustafa and Osman (2015), the outdoor transmission range of 802.11a is 120m, the range of 802.11g and 802.11b is 140m and the range of 802.11n is 250m. According to Ganotra (2015) and the range of 802.11ac is 300m. The risk rating depends on how far out the UAV is. Under 125m, all standards are equally susceptible to interference. The risk of interference increases for lower levels as the range increases. Table 14 shows risk values of each of the Wi-Fi standards discussed in this section. The project team uses a generic interval bound of 15m. An operator may adjust the interval bound to be more accurate.

Table 14. Wi-Fi risk rating.

Transmission range	**802.11a**	**802.11b**	**802.11g**	**802.11n**	**802.11ac**
< 95m	Low	Low	Low	Low	Low
95m <110m	Medium	Low	Low	Low	Low
110m < 125m	High	Medium	Medium	Low	Low
125m < 140m	High	High	High	Low	Low
140m < 205m	High	High	High	Low	Low
205m < 220m	High	High	High	Low	Low
220m < 235m	High	High	High	Medium	Low
235m < 240m	High	High	High	High	low
255m < 270m	High	High	High	High	Medium
>270m	High	High	High	High	High

3) Wi-Fi security

Wireless networking is highly vulnerable to hacking; therefore, various security protocols are used to secure wireless networks via authentication and encryption to prevent eavesdropping, data modification, and wireless control by an adversary. Encryption protects information by altering the data to make it unreadable to users outside the network. A variety of wireless security protocols were established to protect wireless networks. Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2 and WPA3 are wireless security protocols that prevent unwelcome guests from connecting to your wireless network as well as encrypt your private data as it is being transmitted.

a) WEP

Wired Equivalent Privacy (WEP) was introduced alongside the 802.11 standard. It was developed to provide confidentiality similar to a wired network by encrypting data over radio waves. WEP is encrypted by using the Rivest Cipher 4 (RC4) stream cipher. RC4 uses a 40-bit shared key combined with a 24-bit Initialization vector (IV) (a data block used to ensure distinct ciphertexts). The reuse of the IV is a major vulnerability. There are many other publicized vulnerabilities that prove WEP to be easily broken. Therefore, this protocol is now obsolete and no longer permitted to be implemented in new routers and devices. Since WEP is obsolete and not used in the UAVs research it will not be used as an input.

b) WPA

Wi-Fi Protected Access (WPA) was developed to address the faults found in WEP. The WPA uses the same RC4 encryption process but uses a Temporal Key Integrity Protocol (TKIP) with Message Integrity Check (MIC). TKIP uses a longer 48-bit initialization vector hashed together with a key mixing to generate a sequential key and a MIC. Other improvements include the use of separate keys for authentication, encryption, and integrity. While WPA enhanced security, new methods were developed to crack WPA. It is vulnerable to de-authentication dictionary attacks, MitM attacks and DoS.

The Beck-Tews' Attack uses de-authentication and a DoS or Address Resolution Protocol (ARP) poisoning attack to exploit a weakness in TKIP that allows an attacker to

decrypt ARP packets that consist of the source and destination IP and the source MAC address, and inject traffic into a network. In the research paper "Practical attacks against WEP and WPA" by Tews and Beck (2008), WPA is compromised by exploiting the TKIP "by modifying a chopchop attack. A chopchop attack works by taking one byte of data from an encrypted packet, substituting values for that byte, and recalculating the encryption checksum. The modified packets are then sent to an access point, which simply discards them until a valid checksum is eventually substituted by the attacker" (1). In the Beck-Tews attack, the attacker de-authenticates the access point then captures an ARP packet. Then the attacker uses a dictionary attack to get the MIC key which enables the attacker to be able to inject custom packets into the network. This attack may be used to against a UAV, causing the operator to lose control of the UAV, interrupt communications between the sensor and GCS or cause the UAV to shut down. The operator may experience video loss, the drone crash or fly away.

In the Hole196 attack, a MitM attack is used. As depicted by Ahmad (2010), the attacker becomes an authorized user on the network by creating a malevolent ARP frame with the same IP as the default gateway. Then the attacker sends an ARP request forcing the target device to update their ARP tables. The target device then forwards that data with the attacker private key. As a result, data can now be decrypted, allowing the attacker to see private data traffic from other authorized Wi-Fi users in the network. In practice this attack may lead to an attacker gaining access to confidential information in the UAS or taking control of the UAV. If the attacker is just eavesdropping on information being sent, attack symptoms may be limited. However, if the attacker takes control of the UAV the operator might see the UAV crash or fly elsewhere.

Routers with the WPS feature are vulnerable to an attacker exploiting the flaw that allows the attacker to recover the WPS Pin using a brute force attack. As Carranza (2017) suggests "by attacking the Wi-Fi Protected Setup (WPS) passcode using a brute force dictionary attack, it is possible to circumvent the use of password-based network encryption and gain access to the wireless network content." After the WPS is recovered, the pre-shared key can be recovered enabling the attack to gain access to the network. A WPS attack can be used to gain access to information or mount further attacks. This attack

may lead to information stolen from the UAS, a packet injection attack, and loss of control. The operator may experience loss of video, the UAV crash or fly elsewhere.

Researcher Jens Steube discovered a new method of dictionary attacks on Wi-Fi when attempting to break the WPA security scheme. In his post (2018) he details a procedure in which an off-line dictionary attack can be performed by attacking the Pairwise Master Key Identifier (PMKID). In this attack, an attacker uses brute force or a dictionary attack. The attacker makes a request to the PMKID and then the PMKID dumps the information into a file. Then the attacker will use brute force or a dictionary attack to crack the WPA PSK password to gain access to confidential information. An attacker may perform this attack on the Wi-Fi used in the communication link. The operator may be unaware that this attack is happening.

c) WPA2

The WPA2 protocol was created to be an enhancement over the WPA. As Khasawneh (2014) suggest "Despite the advantages provided by WPA, it still has some weaknesses regarding the authentication and data integrity processes. Therefore, WPA2 was developed," One difference between WPA2 uses an Advanced Encryption Standard (AES) in combination with Cipher Block Chaining Message Authentication Code Protocol (CCMP) instead the TKIP in WPA. The AES processes data blocks of 128 bits, using cipher keys of 128, 192, or 256 bits. CCMP is a security protocol used to protect data integrity by encrypting data. WPA2 also uses AES-CTR for encryption in place of RC4. Counter-Mode provides more data privacy. Like WPA, WPA2 is susceptible to a dictionary attack, an evil twin attack, a Hole 196 attack and a DoS attack. WPA2 is also vulnerable to a key reinstallation attack (KRACK) and a PMKID attack, which are discussed below.

In a KRACK attack, the attacker exploits a vulnerability in the four-way handshake that WPA2 security protocols use to authenticate their users when connecting to the network. In WPA2 the pairwise master key used is derived from the pre-shared key during the four-way handshake. This allows for an attacker to sniff the four-way handshake and perform a dictionary attack to obtain the password. According to Kohlios (2018) "With this vulnerability, an adversary can spoof the packets to make it look like they are coming

from the target client and preform attacks such as a de-authentication attack. In the KRACK attack, the attacker sets the counters to their initial values and can then replay messages and decrypt them" (284). The KRACK attack exploits the vulnerability of WPA2 which allows keys to be reinitialized and allows a client to transmit management frames in plaintext packets to the AP. This attack can lead to access to the UAS to gain or misuse other information. The operator may be unaware that this attack is happening.

d) WPA3

The latest security standard WPA3 was developed to improve security protections in existing WLAN. The session key size for WPA3 is 192 bits instead of the 128 bits WPA2 uses for security during the authentication stage. WPA3 uses the password-based Simultaneous Authentication of Equals (SAE). SAE requires a new interaction with the network every time a device requests an encryption key. Due to the SAE key exchange, WPA3 is more resilient to KRACKs as well as dictionary attacks. WPA3 is still susceptible to some of the same attacks that WPA and WPA2 are susceptible to such as MitM attacks, evil twin attacks, PMKID attack. Although WP3 itself is no longer susceptible to the particular dictionary and de-authentication attacks discussed above, these attacks can be performed via performing a downgrade attack first. It is also vulnerable to a side channel attack.

A transition mode was developed in the WPA3 in order to support older clients that only support WPA2. In this mode a Wi-Fi network can support the usage of both WPA3 and WPA2. In Vanhoef and Ronen's paper (2018) they discovered that an attacker could create a rogue network and force clients that are using WPA3 to transition to the rogue WPA2 network. After the transition, the WPA2 handshake is captured using a brute-force or dictionary attack and can be used to recover the password of the network. An adversary may leverage this attack on an UAS's communication link to steal information. The operator may be unaware that this attack is happening.

Another downgrade attack Vanhoef and Ronen discovered is against the Dragonfly handshake used in WPA3. In this downgrade attack, the victim is forced to use a weak security suite. "The client initiates the handshake by sending a commit frame that includes

the security suite it wishes to use. If the AP does not support this suite, it responds with a decline message, forcing the client to send a commit frame using another suite. This process continues until a security suite is found that is supported by both sides. An attacker can impersonate an AP and forge decline messages to force clients into choosing a weak security suite" (Vanhoef and Ronen, 2018). After an attacker performs this downgrade attack, the attacker can perform WPA2 attacks such as a KRACK. The operator may be unaware that this attack is happening.

In a side-channel attack on WPA3, attackers with access to a client device connecting to a network can also look at its memory access patterns. An attacker can use a browser-based Java script code when the device is in the middle of a Dragonfly handshake to reveal information about the password being used. After the information is revealed, the attacker uses a dictionary attack to recover the password. In Rodday's paper (2015), he describes how a side channel attack can be used to recover an UAV's firmware encryption key and use the key to decrypt the firmware. After decrypting the firmware, the attacker can steal information. The operator may be unaware that this attack is happening.

e) Wi-Fi Security Risk values

Based on the rationale and comparisons of the different Wi-Fi security protocols defined in this section, risk ratings can be assigned. The risk ratings are assigned as a high for WPA, medium for WPA2, or low risk for WPA3. Table 15 shows the rankings and risk ratings of each of the Wi-Fi security discussed in this section.

Table 15. Wi-Fi security risk rating.

Security Standard	Risk Rating
WPA	High
WPA2	Medium
WPA3	Low

GPS Modes

Global Navigation Satellite Systems (GNSS) is the generic term for satellite-based systems that provide geospatial positioning, while the Global Positioning System (GPS) is a method of GNSS used in the United States for both civilian and military applications. Given that GPS is owned and operated by the U.S. Department of Defense, alternative forms of GNSS will not be considered within the scope of this document. GNSS is a key capability of both autonomous and operator controlled UAS. GPS is most commonly used for navigation which is a central component of UAS operation in that it allows the operator, and the UAS, to know the precise location of the UAV during operations. There are a variety of GPS "modes," both civilian and military, that vary in efficiency and reliability. Some of these modes are encrypted to protect against interference and spoofing attacks according to Kaplan and Hegarty (2005). Given that GPS signals are transmitted from satellites using RF signals, GPS is associated with a variety of vulnerabilities for a UAS. The vulnerability of the GPS connection for each UAS varies depending on the GPS mode being used. In relation to the decision matrix, the operator would select which GPS mode they are using as an input.

GPS signals are based on Pseudo Random Noise Code (PRN) which is, at a high level, a complicated digital code modulated onto a carrier frequency which contains information that can be used to determine geospatial position. Signals are broadcasted at three carrier frequencies L1, L2, and L5 (L1 = 1575.42 MHz, L2 = 1227.60, L5 = 1176.45):

- C/A Code is the legacy GPS method and is the basis for civilian GPS use. It is transmitted on a single carrier frequency, L1. The signal has a 1.023 MHz chip rate and repeats every 1023 bits which results in a repeated code every 1ms. Each satellite has a unique PRN code.

- P Code is a legacy GPS method primarily used for military applications. It is transmitted on two carrier frequencies, L1 and L2. According to Kaplan and Hegarty (2005), the signal has a 10.23 MHz chip rate and repeats approximately every 38 weeks with each satellite repeating a portion of the code every 7 days. Each satellite transmits a different portion of the P code sequence. P code is

much more accurate when compared to C/A code because of the ability to perform ionospheric corrections due to the use of two separate carrier frequencies. P code can be encrypted in which case it is called P(Y) code.

- L2C code is a more recent addition to civilian GPS applications. L2C is transmitted at the L2 carrier frequency. L2C is composed of two PRN codes, civil moderate length code (CM) and civil long code (CL). The CM has 10.230 chip and repeats every 20ms. The CL has 767.250 MHz chip and repeats every 1.5s. L2C is transmitted at a higher effective power than C/A code and therefore can be more easily received. According to Qaisar and Dempster (2016), the use of dual-frequency receivers enables the use of both L2C and C/A which provides faster signal acquisition and greater reliability comparable to, and in some cases better, than military codes such as P code.
- L5 code is the future of civilian GPS applications. It is transmitted on a single carrier frequency, L5. According to Leclere, Landry and Botteron (2018), L5 benefits from higher transmit power, wider bandwidth, and improved signal structure which make it the most reliable GPS method for civilians. Two PRN codes are used in L5, in-phase code (I5-code) and quadrature phase code (Q5-code). Similar to the L2C code, L5 code can be used with C/A for increased reliability and accuracy.
- M-Code is a GPS method developed for military applications to be resistant to jamming. The M-code signal is transmitted on both L1 and L2 carrier frequencies with a classified frequency offset. According to Kaplan and Hegarty (2005), the M-code signal employs a variety of mechanisms to counter cyber threats such as encryption, spoofing detection and rejection, and spot beam transmission. Specific details on M-code are not available in an unclassified environment. However, M-code was designed specifically for security and anti-jamming and therefore it will be considered the most effective GPS method from a cybersecurity perspective.

Based on the rationale and comparisons of the different GPS modes defined in this section, risk ratings can be assigned. The risk ratings are assigned as a high, medium, or low risk. Table 16 shows the rankings and risk ratings of each of the GPS modes discussed in this section.

Table 16. GPS mode risk values.

GPS Mode	Risk Ratings
C/A	High
P	Medium
L2C	Medium
P(Y)	Low
L5	Low
M	Low

1) GPS Attacks

Global Positioning System (GPS) is a major key to operating the UAV safely, as these systems rely heavily on GPS data to locate themselves, the ground station, and their targets. The UAV GPS is typically used to determine the relative positioning and speed of the vehicle. Tracking the UAV or steering the UAV can be done by using the position provided by the receiver. GPS navigation techniques can offer consistent accuracy if satellite signals can be accessed during the UAV's mission.

An UAV relying on GPS-based navigation is susceptible to attacks, and particularly susceptible to spoofing and falsified signals, along with jamming. GPS spoofing is a prominent security threat that targets UAVs. This attack happens when an attacker alters an UAV's GPS signals in order to capture it. Spoofing is one of the most harmful attacks for GPS device, as it gives a false sense of physical location, and results in mission path diversions. The false estimate of the UAV position in the on-board navigation system can be a result of spoofed data received through the GPS sensors. According to Javaid (2012), UAVs are also vulnerable to falsified signals. Simply delaying the GPS reading could cause incorrect positioning and action. Likewise, an attacker can use a local transmitter under the same frequency, as this signal would be stronger than the original satellite signal, and as a result, the spoofed GPS-signal will override current satellite-signal. Since civilian GPS devices are unencrypted and extremely vulnerable to spoofing attacks, "it is relatively easier to launch such an attack due to the availability of off-the-shelf GPS signal generators" (Jensen 2019). We focus here on data authenticity and spoofing, despite the

data protection being described as encryption, as the stated goals of GPS "encryption" is spoofing protection, not confidentiality protection. Lastly, "Jamming sends electromagnetic noise at radio frequencies with the purpose of overriding the same radio and GPS signals the drone uses to operate. Jamming involves transmission of high and/or low power noise signals to render all communication receivers in the area non-functional" (Jensen 2019).

Table 17. GPS attack risk rating.

GPS Attack Category	Level of Consequence	Technical Capability	Symptoms
Availability	Low	Low	• Loss of connection • Loss of control • Loss of network resources
Access Control	High	High	• Loss of connection • Altered C2 communications • Loss of control • Altered data • Loss of data

2. Operator Input – Operational Environment Information

The following section identifies the operational environment information that the operator will input into the matrix. The following inputs will act as a modifier to the risk ratings of the other operator inputs such as the C2 Link.

Range

A portion of the cyber-attacks are dependent on the adversary transmitting a RF signal that is received at the UAV at a higher, or at least equal, signal strength compared to the operator's signal. Attacks of this nature may include jamming, spoofing, and other RF-based attacks. RF transmissions are attenuated over distance therefore the farther the UAV is from the operator, and the GCS, the lower the operator signal strength will be at the UAV. In the same way, the lower the operator signal strength is at the UAV, the higher

the risk that an attack will be successful. The impact of range on the probability of attack is dependent on the Wi-Fi standard used by the operator. This relationship, as well as the available inputs for the operator, were discussed in Section 4.1.2f and are displayed in Table 14.

Geography

As stated in the previous section, the risk of a successful RF-based cyber-attack, such as jamming or spoofing, is increased by interrupted or low GCS signal strength at the UAV. The geography of the operational area can have a detrimental effect on the signal strength received by the UAV. The communication links discussed in this paper are primarily LOS which means that the transmitter must have a direct line-of-sight to the receiver. Obstructions in this line-of-sight will interrupt or attenuate the signal strength at the receiver. Therefore, operations in areas with many obstructions, such as forests or mountains, increases the risk that a RF-based cyber-attack will be successful. Table 18 shows a set of possible geography operator inputs and associated risk modifiers.

Table 18. Geography input risk.

Geography	Risk Modifier
Plains	None
Forest	Low
Mountains	Medium

Adversary

The technical capability of the adversary determines the level of cyber-attack that the adversary can launch. For this example, the potential adversaries have been split into three categories indicating their respective development, and therefore, technical capabilities. For the current mission, the operator inputs the adversary's level of technical sophistication, which impacts the level of attack and therefore the overall risk, of the mission. Table 19 identifies the potential adversary inputs and the attack capabilities of each.

Table 19. Adversary input risk.

Adversary Rating	Technical Capability
First World Country	High
Second World Country	Medium
Third World Country	Low

B. EXAMPLE MATRIX WALKTHROUGH

The example inputs and criteria for this example matrix have been identified and defined. Now each step in the matrix will be explained in sequential order to show how the matrix can be used to determine the overall risk. The operator inputs in Table 20 will be used for this demonstration.

Table 20. Demonstration operator inputs.

Operator Input	Operator Selection	Risk Rating
Wi-Fi Protocol / Range	802.11ac / 255m < 270	Medium
Wi-Fi Security	WPA3	Low
GPS Mode	M-code	Low
Geography	Plains	N/A
Adversary	Third World	Low

Most Likely Cyber Attacks Output

As stated in Chapter III, the "most likely cyber-attacks" are determined by a combination of the operator input "adversary" and the constant input "cyber-attacks." In this example, the operator has chosen a third world adversary, capable of low capability attacks, which results in the "most likely cyber-attacks" output below which will be used in the determination of risk in the following sections.

Table 21. Most likely GPS attacks.

GPS Attack Category	Risk Rating	Technical Capability	Symptoms
Availability	Low	Low	• Loss of connection • Loss of control • Loss of network resources
C2 Attack Category	Risk Rating	Technical Capability	Symptoms
Availability	Low	Low	• Loss of connection • Loss of control • Loss of network resources

Risk Output

C2 Attack Risk

The C2 attack risk is derived from a combination of the consequence of the cyber-attacks and the probability of a successful cyber-attack. Both of these variables are derived from different elements of the matrix inputs. The first step is to identify the consequence of the most likely C2 attacks using the operator inputs in Table 20. The result is shown below.

1. C2 Attack Consequence = Availability Attack Consequence = Low

The next step is to derive the probability of the potential C2 attacks. This step is completed by combining the geography, Wi-Fi standard and range, adversary capability, and Wi-Fi security. Note that in the demonstration inputs chosen, geography "plains" does not modify the probability of attack and therefore does not factor into this calculation.

2. Probability of Successful Attack = Medium * Low * Low = Medium

The final step is to determine the C2 attack risk. This is completed by combining the consequence of the most likely C2 attacks and the probability of successful attack.

3. C2 Attack Risk = Consequence * Probability = Low * Medium = Medium

GPS Risk

In the same way as the C2 attack risk, the GPS attack risk is derived from a combination of the consequence of the attack and the probability of a successful attack. Both of these variables are derived from different elements of the matrix inputs. The first step is to identify the consequence of the most likely GPS attacks using operator inputs in Table 20. The result is shown below.

1. GPS Attack Consequence = Availability Attack Consequence = Low

The next step is to derive the probability of the potential C2 attacks. This step is completed by combining the geography, GPS Mode, and adversary capability. Note that in the demonstration inputs chosen, geography "plains" does not modify the probability of successful attack and therefore does not factor into this calculation.

2. Probability of Successful Attack = Low * Low = Low

The final step is to determine the GPS attack risk. This is completed by combining the consequence of the most likely GPS attacks and the probability of successful attack.

GPS Attack Risk = Consequence * Probability = Low * Low = Low

Operator Output

Based on the risk derived in the previous sections, the information in Table 22 will be displayed to the operator identifying the most likely cyber-attacks, the risk of each attack based on the mission parameters, and the symptoms of each attack that the operator should look for during the mission to identify if an attack has been launched.

Table 22. Matrix output.

Most Likely C2 Attack Category	**Risk**	**Symptoms**
Availability	Medium	• Loss of connection • Loss of control • Loss of network resources
Most Likely GPS Attack Category	**Risk**	**Symptoms**
Availability	Low	• Loss of connection • Loss of control • Loss of network resources

V. NIST CYBERSECURITY FRAMEWORK

The National Institute of Standards and Technology (NIST) created a framework for improving cybersecurity. The NIST Cybersecurity Framework can be used to improve understanding of cybersecurity, minimize cybersecurity risks, and improve protection on networks and data. The framework provides an outline of best practices to help identify, protect, detect, respond, and recover. The NIST (2018) states that these practices will "aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities." In this section the cybersecurity risk matrix will be associated with each level of the NIST cybersecurity framework.

A. IDENTIFY

The Identify function helps develop an understanding of the cybersecurity vulnerabilities present in UAS, personal, assets and data. Identifying the cybersecurity risks of the UAS and the resources that support critical functions helps develop a risk management strategy. Based on the NIST (2018), the matrix can help identify the following:

- The data, personnel, devices, systems, and facilities that enable the UAS to achieve mission goals are identified and managed consistent with their relative importance to mission objectives and the UAS's risk strategy.
- The UAS's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
- The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
- The environment the UAS will operate in will be identified.

- The UAS vulnerabilities, threats to internal and external organizational resources, and risk response activities will be identified.

- A Risk Management Strategy for the UAS including establishing risk tolerances will be identified.

B. PROTECT

The Protect function defines necessary precautions and supports the ability to limit or contain the impact of a potential cybersecurity event. Cyber resiliency can be ensured by the complying with the protect function of the NIST cybersecurity framework. Complying with the protect function can also improve awareness, secure data, maintain and help deploy protective technology. Based on the NIST (2018) Cybersecurity Framework, the cybersecurity risk matrix can help:

- Control access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

- Ensure the UAS's personnel are provided cybersecurity awareness training and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.

- Establish data security protection consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

- Implement information protection processes and procedures to maintain and manage the protections of information systems and assets

- Protect organizational resources through maintenance, including remote maintenance, activities.

- Prepare for inadvertent events that may put data at risk.

C. DETECT

The Detect function may strengthen the detection of cybersecurity events. This function strengthens the protection against attacks on an UAS network. Based on the NIST (2018) Cybersecurity Framework the following example outcomes can be achieved:

- Detected events can be analyzed to understand attack targets and methods.
- Impact of events are determined.
- Incident alert threshold can be established.
- The physical environment can be monitored to detect potential cybersecurity events.
- Device activity can be monitored to detect potential cybersecurity events.

D. RESPOND

The Respond function helps identify steps that need to be performed after a detected cybersecurity event. This NIST Cybersecurity Framework function will also help increase the ability to reduce the impact of a potential cybersecurity attack. Based on the NIST (2018), the cybersecurity risk matrix can contribute to developing a plan for

- Identifying parts/subsystems that may be at risk.
- Keeping UAS operations up and running.
- Responding to a cybersecurity incident.
- Investigating and containing an attack.

E. RECOVER

The Recover function can help identify necessary steps to recover from a cybersecurity attack and restore any capabilities lost. This function can also reduce recovery time by reducing the impact of a cybersecurity attack by being aware of response and recovery activities. Based on the NIST (2018), Cybersecurity Framework the

cybersecurity risk matrix can assist in updating a cybersecurity policy and plan with lessons learned.

VI. CONCLUSION AND FUTURE WORKS

Chapter VI of this thesis presents the conclusions derived from the results of the example cybersecurity risk management decision matrix. In addition, a future works section is included to suggest further areas of study related to the creation of a cybersecurity risk management decision matrix.

A. CONCLUSION

This research develops a cybersecurity risk assessment framework for COTS UAS tactical operators to generate risk matrices based on UAS-specific and adversary-specific information. By applying a systems engineering approach to the development of a matrix methodology, commands will now be able to create their own cybersecurity risk management decision matrices using the operational environment, the current adversary, and system vulnerabilities. Following the proposed methodology, the sample cybersecurity risk management decision matrix demonstrated the process of creating a matrix that tactical operators could use in the field. While the goals of the project and the major stakeholder needs and requirements have been addressed, there are specific expanded requirements beyond the scope of this technical report. Knowing that future COTS UAS developments may change the protocols used and vulnerabilities, the most appropriate solution is to provide a method that commands can utilize to periodically refresh cybersecurity risk management decision matrices.

By exploring the different protocols used in COTS UASs, an increased understanding of the associated level of security is achieved. This information aided in understanding the process of applying specific protocols to the cybersecurity risk management decision matrix. Validating the cybersecurity risk management decision matrix through the NIST cybersecurity framework allowed the project team to see if the proposed methodology is effective. Through the use of this cybersecurity risk management decision matrix, the tactical operator can determine the level of cybersecurity risk that the COTS UAS faces in the operational environment against the adversary. Additionally, there

are the following two key takeaways through this work developing the cybersecurity risk management decision matrix.

A framework is more valuable than a rigid solution

While conducting research, it became apparent that a single cybersecurity risk management decision matrix would not suffice due to the differing needs of commands and missions. By focusing on the architecture, methodology, and process for creating a cybersecurity risk management decision matrix, we allow for commands and tactical operators that understand their own personal tactical needs to develop a matrix that works best for them in the operational environment. This provides the commands and tactical operators more flexibility while keeping the ability to use a cybersecurity risk management decision matrix. Since the operators have the flexibility to tailor the matrix to their current mission needs, the output of the matrix will theoretically produce a more accurate result. In addition to a more accurate matrix, the framework is able to keep pace with changing operational conditions.

The future is uncertain

Due to technological advancements and the obsolescence of technology, it is important to note the cybersecurity risk management decision matrix should be updated periodically to keep up with the existence of new technologies, new adversarial capabilities, and the risk level associated with certain protocols. For the matrix architecture, methodology, and process for creating the matrix to be effective, the matrix must be updated to keep pace with time. Commands and tactical operators must remain vigilant with the upkeep of the matrix to reap its full benefits. With the passing of time inputs, risk ratings, and outputs may change but the commands and tactical operators will be better equipped to handle the changing problem space using the cybersecurity risk management decision matrix methodology and process.

B. FUTURE WORKS

While conducting research and development of the cybersecurity risk management decision matrix, there were several potential needs identified. These needs could spur

future research in other, more specific areas of study regarding the cybersecurity risk management decision matrix for COTS UAS. This section of Chapter VI identifies what these needs are and outlines how further study of these needs would be beneficial to stakeholders.

Real World Validation Exercise of Matrix

While the validation of the cybersecurity risk management decision matrix using an example scenario is an important step in validating the matrix, it is also important to ensure this risk management decision tool is tested in a real-life application or training exercise. Delivering the matrix to a group of tactical operators to use would aid in finding any shortcomings of the matrix design. Through using the matrix, the tactical operators will be able to provide valuable feedback so any adjustments to the matrix can be made. It is preferable to validate the matrix through real-life testing as it is the actual environment in which the matrix will be used. Finally, this real-world validation gives the tactical operators the opportunity to tailor the models to their own cybersecurity risk assessment needs.

Portable System for Use of Matrix

Since the cybersecurity risk decision management matrix is created in Excel, future work needs to assess which platforms best support this matrix. Considerations need to be taken into account as to what the operators already have on hand or what additional equipment would be needed to support this matrix. Given the matrix will be hosted on an electronic platform, other cybersecurity concerns may need to be considered when offloading this information from the device. Another area of exploration could be putting the matrix on a web or phone-based application. Along with a portable system for the risk matrix, a method of training tactical operators how to use the matrix needs to be established.

Expansion of Other Protocols and Vulnerabilities

This study focuses heavily on RF, GPS, and Wi-Fi vulnerabilities and potential attacks due to those protocols being commonplace in the use of COTS UAS; however,

there are other protocols with vulnerabilities that may be exploited. For instance, there are currently UAVs that utilize 5G cellular networks or Bluetooth instead of Wi-Fi to connect the aerial vehicle to the operator (Javaid 2012, 3) Since this method of communication is not widely used in COTS UASs, it was left out of the design of the matrix. It would be useful to perform more research in this area to create an all-encompassing list of current protocols as well as their vulnerabilities. It should also be noted that, as time passes, prevailing technologies will change. Because of this, GPS and Wi-Fi may be replaced by a superior, more secure method of performing the same function. Research in the methods of how the cybersecurity risk management decision matrix could be updated to keep pace with changing technology would provide an invaluable resource to stakeholders since the matrix could be utilized with the day's current technologies.

Further possibilities in the realm of expanding the matrix to include additional protocols and vulnerabilities would be the creation of an exhaustive list of potential attacks that could occur within each protocol. For instance, GPS includes attacks such as message modification, spoofing, jamming, altering navigational waypoints, embedding errors in the GPS, and message injecting (Horowitz 2016; Manesh 2019). This list could then be used to produce a ranking order of severity and risk for each attack to be an input to the matrix.

While flying ad-hoc networks (FANETs) are not mentioned in this study, it may be worthwhile to invest time in researching this subject in relation to the cybersecurity risk matrix. As an emerging technology, FANETs consist of multiple UAVs communicating in an ad-hoc manner which allows expanding "the connectivity and communication range at geographical areas with limited cellular infrastructure" (Mozaffari et al. 2019, 4). If FANETs were being utilized in a mission scenario, the interruption of the network could pose additional risk to the mission as it links multiple UAVs together. This would become another input to the matrix affecting risk.

Time-Phased Use of Matrix

Another area of further study on this subject matter to be considered is a time-phased approach to utilizing the cybersecurity risk management decision matrix. This time-phased cycle starts during the acquisition phases, and continues through the pre-mission,

during mission, and post-mission phases. Since there are different operational risks at each phase, there are more inputs to consider. During the acquisition phase some form of supply chain risk management should be used to assess whether the cyber integrity of the COTS UAS remains intact. This includes understanding where the UAV was manufactured, assembled, and how it was distributed before being delivered to tactical units. Exploration into the pre-mission, during mission, and post-mission phases will also likely produce different outcomes for how the tactical operator should proceed based on the risk level identified in the matrix. These considerations should be evaluated further to gain insight on how the matrix will be utilized or expanded upon throughout the different phases identified.

THIS PAGE INTENTIONALLY LEFT BLANK

SUPPLEMENTAL

Interactive Matrix for Assessment of COTS UAS Cybersecurity Risk

Chapter IV provides a detailed example of the creation and use of a COTS UAS cybersecurity risk matrix. The purpose of the chapter was to define the thought process behind the creation of the matrix and to serve as an example of how the end user would go about defining inputs, assigning risk ratings, and developing the risk outputs. The example inputs and criteria for the example matrix were identified and defined. A scenario consisting of a single set of available inputs was used to portray how the outputs were calculated in a step by step method. The supplemental matrix is an interactive version of the example matrix explained in Chapter 4. It allows users select from all the available inputs. The matrix also contains software which automates the calculation of outputs based on the inputs chosen by the operator. Please note that the supplemental matrix is not intended to be used in an operational scenario. The operator should have more accurate and relevant operational information on the matrix inputs that is not available to the public due to the sensitivity of the information. Those interested in obtaining the supplemental should contact the NPS library.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Abbaspour, Alireza, Kang Yen, Arman Sargolzaei, and Shirin Noei. 2016. "Detection of Fault Data Injection Attack on UAV Using Adaptive Neural Network." *Procedia Computer Science*, no. 95: 193. https://www.sciencedirect.com/science/article/pii/S1877050916324851.

Abdelrahman, R.B, Mustafa, A.B and Osman, A.A. 2015. "A Comparison between IEEE 802.11a, b, g, n and ac Standards." *IOSR Journal of Computer Engineering* vo. 17, no. 5: 26.

Ahmad, Sohail. 2010. *WPA Hole196 Vulnerability: Exploits and Remediation Strategies*. AirTight Networks, Mountain View, CA.

Beck, Martin, and Erik Tews. 2008. "Practical Attacks Against WEP and WPA." *Research Gate*. January 2008. https://www.researchgate.net/publication/220332983_Practical_attacks_against_WEP_and_WPA.

Benson, Pam, and Micheal Sefanov. 2009. "Iraqi Insurgents Hacked Predator Drone Feeds, U.S. Official Indicates." CNN. December 17, 2009. https://www.cnn.com/2009/US/12/17/drone.video.hacked/index.html.

Blanchard, Benjamin, and Wolter Fabrycky. 2006. *Systems Engineering and Analysis.* Upper Saddle River. N.J: Pearson Prentice Hall.

Buede, Dennis. 2016. *The Engineering Design of Systems: Models and Methods,* 3rd ed. Hoboken, NJ: John Wiley & Sons.

Carranza, Aparicio, Josue Magallanes, Casimer DeCusatis, and Javier Espinal. 2017. "Automated Wireless Network Penetration Testing Using Wifite and Reaver." 15th LACCEI International Multi-Conference for Engineering, Education, and Technology.

Network Penetration Testing Using Wi-Fite and Reaver." *Research Gate*. January 2017. https://www.researchgate.net/publication/319342934_Automated_Wireless_Network_Penetration_Testing_Using_Wi-Fite_and_Reaver

Deng, Jing, Richard Han, and Shivakant Mishra. 2005. "Defending Against Traffic Analysis Attacks in Wireless Sensor Networks." University of Colorado. 2005. https://www.usenix.org/legacy/event/sec04/tech/wips/posters/05-deng-wireless.pdf .

Fournier, Guillaume, Paul Audren, Pascal Cotret, and Valerie Tong. 2017. "DroneJack: Kiss Your Drones Goodbye!" HAL. June 2017. https://hal.inria.fr/hal-01635125/document.

Ganotra, S. 2015 *"Outdoor 802.11ac AP Performance Report by Miercom."* https://blogs.cisco.com/networking/outdoor-802-11ac-ap-performance-report-by-miercom.

Hartmann, Kim, and Christoph Steup. 2013. "The Vulnerability of UAVs to Cyber Attacks: An Approach to the Risk Assessment." 5th International Conference on Cyber Conflict (CYCON 2013). 2013. https://ccdcoe.org/uploads/2018/10/26_d3r2s2_hartmann.pdf.

Horowitz, Barry. 2016. "Cybersecurity for Unmanned Aerial Vehicle Missions." *SIGNAL Magazine*. April 1, 2016. https://www.afcea.org/content/?q=Article-cybersecurity-unmanned-aerial-vehicle-missions.

Javaid, Ahmad, Weiqing Sun, Vijay Devabhaktuni, and Mansoor Alam. 2012. "Cybersecurity Threat Analysis and Modeling of an Unmanned Aerial Vehicle System." *Research Gate*. November 2012. https://www.researchgate.net/publication/235676360_Cyber_security_threat_analysis_and_modeling_of_an_unmanned_aerial_vehicle_system.

Jensen, Jeremy. 2019. "Drone Jammer 101 – An Inside Look at Counter UAS Technology." *UAV Coach*. May 30, 2019. https://uavcoach.com/drone-jammer/.

Kamkar, Samy. 2013. "SkyJack." Github. December 2, 2013. https://github.com/samyk/skyjack.

Kaplan, Eliot, and Christopher Hegarty. *Understanding GPS: Principles and Applications.* 2005. Second Edition. Artech House Publishers. November 30, 2005

Karimibiuki, Mehdi, Michal Aibin, Yuyu Lai, Yuyu, Raziq Khan, Ryan Norfield, and Aaron Hunter. 2019. "Drones' Face off: Authentication by Machine Learning in Autonomous IoT Systems." *Research Gate*. October 2019. https://www.researchgate.net/publication/336411334_Drones'_Face_off_Authentication_by_Machine_Learning_in_Autonomous_IoT_Systems.

Katz-Haas, Ra⊙ssa. 1998. "Ten Guidelines for User-Centered Web Design." Usability Interface. July 1998. file:///C:/Users/alexa/Downloads/9807-webguide.pdf.

Khasawneh, Mahmoud, Izadeen Kajman, Rashed Alkhudaidy, and Anwar Althubyani. 2014. "A Survey on Wi-Fi Protocols: WPA and WPA2." *Research Gate.* March 2014. https://www.researchgate.net/publication/290743584_A_Survey_on_Wi-Fi_Protocols_WPA_and_WPA2.

Kohlios, Christopher, and Thaier Hayajneh. 2018. "A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3." Electronics. Last modified October 30, 2018. file:///C:/Users/alexa/Downloads/electronics-07-00284.pdf.

Leclère, Jérôme, René Landry, and Cyril Botteron. 2018. "Comparison of L1 and L5 Bands GNSS Signals Acquisition." U.S. National Library of Medicine. August 23, 2018. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6165328/.

Mansfield, Katrina, Timothy Eveleigh, Thomas Holzer, and Shahyar Sarkani. 2013. "Unmanned Aerial Vehicle Smart Device Ground Control Station Cybersecurity Threat Model." In *2013 IEEE International Conference on Technologies for Homeland Security*: 772. https://ieeexplore.ieee.org/abstract/document/6699093?section=abstract.

Mozaffari, Mohammad, Walid Saad, Mehdi Bennis, Young-Han Nam, and Merouane Debbah. 2019. "A Tutorial on UAVs for Wireless Networks: Applications, Challenges, and Open Problems." *IEEE Communications Surveys & Tutorials* vol. 21, no. 3 (March): 2334–2360. https://doi.org/10.1109/COMST.2019.2902862

National Institute for Standards and Technology. 2018. "Cybersecurity Framework." 2018. https://www.nist.gov/cyberframework.

Newman, William, and Michael Lamming. 1995. *Interactive System Design*. Boston, MA: Addison-Wesley.

Pärlin, Karel, Muhammad Alam, and Yannick Le Moullec. 2018. "Jamming of UAV Remote Control Systems Using Software Defined Radio." Research Gate. May 2018. https://www.researchgate.net/publication/324278456_Jamming_of_UAV_Remote_Control_Systems_Using_Software_Defined_Radio.

Pastor, Enrie, Juan Lopez, and Pablo Royo. 2007. "UAV Payload and Mission Control Hardware/Software Architecture." *IEEE Aerospace and Electronic Systems Magazine*, June 2007. https://libguides.nps.edu/citation/chicago-ad#magazine

Qaisar, Sana, Andrew Ullah, and Dempster Graham. 2016. "Cross-correlation Performance Comparison of L1 & L2C GPS Codes for Weak Signal Acquisition." University of New South Wales. 2016. file:///C:/Users/alexa/Downloads/qaisardempster2008a.pdf.

Riahi Manesh, Mohsen, and Naima Kaabouch. 2019. "Cyber-Attacks on Unmanned Aerial System Networks: Detection, Countermeasure, and Future Research Directions." *Computers and Security*. 2019. https://doi.org/10.1016/j.cose.2019.05.003.

Rodday, Nils, Aiko Pras, and Ricardo de Oliveira Schmidt. 2016. "Exploring Security Vulnerabilities of Unmanned Aerial Vehicles." University of Twente. July 2015. https://www.jbisa.nl/download/?id=17706129.

Samland, Fred, Jana Fruth, Mario Hildebrandt, Tobias Hoppe, and Jana Dittmann. 2012. "AR.Drone: Security Threat Analysis and Exemplary Attack to Track Persons." https://www.researchgate.net/publication/258713432_ARDrone_Security_threat_analysis_and_exemplary_attack_to_track_persons.

Sánchez, Helem, Damiano Rotondo, Marc Vidal, and Joseba Quevedo. 2019. "Frequency-Based Detection of Replay Attacks: Application to a Quadrotor UAV." *Research Gate*. October 2019. https://upcommons.upc.edu/bitstream/handle/2117/183340/ICSC19_0068_FI-1.pdf?sequence=1&isAllowed=y.

Sciancalepore, Savio, Omar Ibrahim, Gabriele Oligeri, and Roberto Pietro. 2019. "Detecting Drones Status via Encrypted Traffic Analysis." *Research Gate*. May 2019. https://www.researchgate.net/publication/332874164_Detecting_Drones_Status_via_Encrypted_Traffic_Analysis.

Sharp, Helen, Anthony Finkelstein, and Galal Galal. 1999. "Stakeholder Identification in the Requirements Engineering Process." November 12, 1999. http://www0.cs.ucl.ac.uk/staffhttp://www0.cs.ucl.ac.uk/staff/A.Finkelstein/papers/stake.pdf/A.Finkelstein/papers/stake.pdf.

Sommerville, Ian, and Gerald Kotonya. 1998. *Requirements Engineering: Process and Techniques.* Hoboken, NJ: John Wiley & Sons.

Steube, Jens. 2018. "New Attack on WPA/WPA2 Using PMKID." *Wi-Fi CERTIFIED WPA3 Technology Overview* 1 (August): 1. https://cert.europa.eu/static/SecurityAdvisories/2018/CERT-EU-SA2018-019.pdf.

Tung, Yu-Chih, Sihui Han, Dongyao Chen, and Kang G. Shin. 2014. "Vulnerability and Protection of Channel State Information In Multiuser MIMO Networks." The University of Michigan. November 7, 2014. https://rtcl.eecs.umich.edu/papers/publications/2014/paper-ccs.pdf.

U.S. Air Force. 2005. *SMC Systems Engineering Primer & Handbook: Concepts, Processes, and Techniques*. Washington, DC: U.S. Air Force.

Vanhoef, Mathy, and Eyal Ronen. 2019. "Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd." Cryptology ePrint Archive, Report 2019/38. Last Modified August 2, 2019. https://eprint.iacr.org/2019/383.

Vanunu, Oded, Dikla Barda, and Roman Zaikin. 2018. "DJI Drone Vulnerability." Center Point Research. November 8, 2018. https://research.checkpoint.com/2018/dji-drone-vulnerability/.

Vasconcelos, Gabriel, Gabriel Carrijo, Rodrigo Miani, Jefferson Souza, and Vitor Guizilini. 2016. *The Impact of DoS Attacks on the AR. Drone 2.0.* Recife, Brazil: IEEE.

Vemi, S.G., and Christo Panchev. 2016. "Vulnerability Testing of Wireless Access Points Using Unmanned Aerial Vehicles (UAV)." Coventry University. January 2015. https://pureportal.coventry.ac.uk/en/publications/vulnerability-testing-of-wireless-access-points-using-unmanned-ae-2.

Waliullah, Md. and Gan, D. 2014. *"Wireless LAN Security Threats & Vulnerabilities: A Literature Review." International Journal of Advanced Computer Science and Applications*, vol. 5, no. 1: 181.

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