Cyber Risk Assessment and Scoring Model for Small Unmanned Aerial Vehicles

THESIS

Dillon M. Pettit, Captain, USAF

AFIT-ENG-MS-20-M-055

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT-ENG-MS-20-M-055

CYBER RISK ASSESSMENT AND SCORING MODEL FOR SMALL UNMANNED AERIAL VEHICLES

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

in Partial Fulfillment of the Requirements for the

Degree of Master of Science in Cyberspace Operations

Dillon M. Pettit, B.S.

Captain, USAF

March 2020

AFIT-ENG-MS-20-M-055

CYBER RISK ASSESSMENT AND SCORING MODEL FOR SMALL UNMANNED AERIAL VEHICLES

THESIS

Dillon M. Pettit, B.S.
Captain, USAF

Committee Membership:

Scott R. Graham, Ph.D.
Chair

David R. Jacques, Ph.D.
Member

Lt Col Patrick J. Sweeney, Ph.D.
Member

Stephen J. Dunlap, M.S.
Member

Abstract

The commercial-off-the-shelf small Unmanned Aerial Vehicle (UAV) market is expanding rapidly in response to interest from hobbyists, commercial businesses, and military operators. The core commercial mission set directly relates to many current military requirements and strategies, with a priority on short range, low cost, real time aerial imaging, and limited modular payloads. These small vehicles present small radar cross sections, low heat signatures, and carry a variety of sensors and payloads. As with many new technologies, security seems secondary to the goal of reaching the market as soon as innovation is viable. Research indicates a growth in exploits and vulnerabilities applicable to small UAV systems, from individual UAV guidance and autopilot controls to the mobile ground station devices that may be as simple as a cellphone application controlling several aircraft. Even if developers strive to improve the security of small UAVs, consumers are left without meaningful insight into the hardware and software protections installed when buying these systems. To date, there is no marketed or accredited risk index for small UAVs. Building from similar domains of aircraft operation, information technologies, cyber-physical systems, and cyber insurance, a cyber risk assessment methodology tailored for small UAVs is proposed and presented in this research. Through case studies of popular models and tailored mission-environment scenarios, the assessment is shown to meet the three objectives of ease-of-use, breadth, and readability. By allowing a cyber risk assessment at or before acquisition, organizations and individuals will be able to accurately compare and choose the best aircraft for their mission.

To my wife,

Without your unfailing support and unwavering persistence, I would not have been able to achieve as much as have been able to at AFIT. May I never forget the sacrifices that my career has imposed on yours. You are the greatest partner any man could imagine. Thank you.

To my son,

Never lose your instinct to explore the world and to question every assumption.

To my father,

By putting in the hard work daily, I can honestly say that my achievements are merely an extension of yours.

Acknowledgements

I would be remiss not to acknowledge the unique support of my research advisor, Dr. Scott Graham, who harnessed my interests and strengths to the betterment of the US Air Force. Your expert advice was fundamental throughout my thesis work and I appreciate your "philosophizing".

To my entire committee, Dr. David Jacques, Mr. Stephen Dunlap, and Lt Col Patrick Sweeney: Each of you brought unique perspective to my research that I would never have been able to achieve without. Thank you for allowing for all of my questions and molding the researcher I have become.

Dillon M. Pettit

Table of Contents

Page

List of Figures

List of Tables

List of Algorithms

List of Acronyms

AI	Artificial Intelligence
AIA	Aerospace Industries Association
BBN	Bayesian Belief Network
C2	Command and Control
CA	Certificate Authority
CAT	Cyber Action Team
CISA	Cybersecurity and Infrastructure Security Agency
COBIT	Control Objectives for Information and related Technology
COTS	Commercial Off The Shelf
CPS	Cyber Physical System
CRISM	Cyber Risk Scoring and Mitigation Tool
CSF	Cybersecurity Framework
CSRI	Cyber Security Risk Index
CVE	Common Vulnerabilities and Exploitations
CVSS	Cyber Vulnerability and Scoring System
DHS	Department of Homeland Security
DIY	Do-It-Yourself
DJI	DJI Sciences and Technologies Limited
DoD	Department of Defense
DoS	Denial of Service
EW	Electronic Warfare
FAA	Federal Aviation Administration
FDA	Food and Drug Administration
FIRST	Forum of Incident Response and Security Teams

GAO Government Accountability Office

GPS Global Positioning System

GWOT Global War on Terror

ICOMC2 Insitu's Common Open Mission Management Command and Control

IDS Intrusion Detection System

IOT Internet of Things

IP Internet Protocol

ISM Industrial, Scientific, and Medical

ISMM Information Security Maturity Model

ISRAM Information Security Risk Analysis Method

ISS Impact Sub-Score

IT Information Technology

ITAR International Traffic in Arms Regulations

JAUS Joint Architecture for Unmanned Systems

MAC Media Access Control

MDR Message Drop Rate

MISS Modified Impact Sub-Score

MitM Man in the Middle

MTTSD Mean Time to Shut Down

NAS National Airspace System

NASA National Aeronautics and Space Administration

NATO North Atlantic Treaty Organization

NIST National Institute of Standards and Technology

NVD National Vulnerabilities Database

OS Operating System

OTA Over-The-Air

PKI Public Key Infrastructure

PLC Programmable Logic Controller

RC Remote Control

RF Radio Frequency

RMF Risk Management Framework

RPV Remotely Piloted Vehicle

RTOS Real Time Operating System

SANS System Administration, Networking, and Security

SCADA Supervisory Control and Data Acquisition

SD Secure Digital

sUAV Small Unmanned Aerial Vehicle

U.S. United States

UAV Unmanned Aerial Vehicle

URAF Unmanned Aerial Vehicle Traffic Management Risk Assessment Framework

USB Universal Serial Bus

UTM Unmanned Aerial Vehicle (UAV) Traffic Management

CYBER RISK ASSESSMENT AND SCORING MODEL
FOR SMALL UNMANNED AERIAL VEHICLES

I. Introduction

1.1 Background and Motivation

The desire of man to fly is almost as old as time itself. Since the dawn of flight, aircraft have evolved to meet new demands and innovations, through the 20^{th} century and into the 21^{st}. While UAVs have been around since the earliest days of aircraft, technology in the last two decades has allowed an explosion of options that allow for militaries and commercial organizations alike to consider the aerial automation of missions like never before. In particular, small UAVs provide a lower cost of entry and less overhead, with much of the same aerial advantages as larger vehicles.

As with all computer devices, small UAVs come with risks associated with their missions, both physical and cyber related. The physical risks of collisions and damage to structures or people is reflected in United States (U.S.) government regulations and licensing through the Federal Aviation Administration (FAA) [5]. In contrast, the cyber risks accepted by organizations and individuals has received very little attention and oversight by regulators. Most organizations do incorporate some sort of cyber risk framework to manage risks, but these frameworks are reliant on lackluster risk assessments for small UAVs.

1.2 Problem Statement

In some sense, manufacturers currently control small UAVs cyber security standards by setting their own levels of protection, which may not be acceptable with consumers. Organizations have little measurement or insight into the risks accepted with purchasing and operating these vehicles as there is no formal method of comparison, as may be seen with other vehicle safety [6]. Additionally, while manufacturers may have a vested interest in protecting their devices from outside compromise, the cost of cyber security efforts and overhead of components and software compete with financial and physical constraints.

1.3 Research Objectives

This research defines a new cyber risk assessment for small UAVs using the lessons learned from assessments in related systems. This research then tests and analyzes this new scoring system by presenting case studies that represent the breadth of models and mission scenarios for small UAVs. The research objectives of this work are outlined below:

- Assess whether any cyber or physical risk assessments of similar domains accurately quantify the cyber risk of small UAVs.
- Determine the success criteria a small UAV cyber risk assessment should meet, based on similar domain assessments.
- Define a new small UAV cyber risk assessment tool (assuming none exists).
- Establish the objectives a hardware-in-the-loop simulation of a small UAV should meet to best bring awareness to potential vulnerabilities.

1.4 Hypothesis

The hypothesis of this research is that no cyber risk assessment tool currently exists and no similar domain assessment accurately portrays the risk of small UAVs to its operators/owners. If none exist, a new tool will need to be built using the lessons learned and scoring models of similar domains that have seen success.

1.5 Approach

The approach consists of first analyzing and comparing many of the similar domains' risk assessments for applicability to small UAVs and defining the best set of objectives for a new risk assessment based on the unique characteristics. Utilizing the closest risk assessment to the required need, a new cyber risk assessment specific to small UAVs will be defined with as little deviance from the scoring model as possible to maximize the value of the chosen tool's lessons learned. The new tool will then be analyzed against a multitude of case studies to verify its ability to easily and accurately quantify associated risk of the vehicles to mission scenarios. Lastly, from the analysis of the case studies, a proposal for objectives that a hardware-in-the-loop simulation for small UAVs must meet will be presented.

1.6 Assumptions and Limitations

The analysis of similar domains' risk assessments assumes that all practical assessments have been discovered. It is expected that there are many risk assessments of use to this research that are not public domain or unclassified that may relate to this research. This research also assumes that all publicly available specifications and configurations of utilized small UAVs (under 55 pounds per FAA regulations) are correct as this research does not personally verify any of this data. This research is

limited to risk assessments for only small UAV platforms due to the unique characteristics, though there may be benefits or applicability of the new tool to larger UAVs. Analysis is limited to only case studies with no simulations or operational testing, which meets the goal to move the risk assessment forward in the life-cycle process.

1.7 Contributions

The contributions of this thesis to the field of small UAVs are outlined below:

- **Risk Assessment Gap:** Discovered a gap in cyber security of small UAVs for a cyber risk assessment.
- **Quantitative Cyber Risk Assessment Tool:** A three phase quantitative assessment of small UAVs from 14 sub-metrics that rate the qualitative security of the vehicle.
- **Quantitative Analysis:** Analysis of the granularity of the scoring tool for breadth and spacing of possible scores.
- **Qualitative Analysis:** Demonstrated the risk assessment's ease of use and accuracy through use of publicly available source materials without operational testing.
- **Simulation Objectives:** Defined objectives for hardware-in-the-loop simulation of small UAVs with the goal of better defining the risk associated with use of the vehicles.

1.8 Organization

This thesis is organized as follows:

Chapter II introduces UAV technology and architecture, with corresponding research into security and vulnerability. This is followed by introducing risk frameworks and assessments across the life-cycle of a vehicle. It also presents ongoing related work and identifies areas requiring further research.

Chapter III presents a new quantitative cyber risk assessment specifically tailored to small UAVs. The framework is defined in three sequential phases of Base, Temporal, and Environmental factors relating to the associated risk of the UAV. Definitions and limits of each of the 14 sub-metrics are then provided to allow quick and easy categorization. Each sub-metric can take on one of several discrete levels. The numerical values assigned to each level per sub-metric form the input to the associated algorithms to produce a final overall risk score.

Chapter IV lists the case study scenarios' assumptions, control factors, and variables. A description of the methodology for conducting a risk assessment is also presented in this chapter. The results, analysis, and observations of the experimental activities are then expanded on from the case studies. Analysis of the case studies focuses on the statistical significance of the risk scores along with a qualitative analysis of its accuracy. Finally, it discusses benefits, drawbacks and challenges, and security and privacy concerns with the implementation presented.

Finally, Chapter V concludes with a summary of the work presented and the contributions to the field. In addition, recommendations for those utilizing similar tools or frameworks are presented. Future work areas for this research involve further analysis of the risk assessment through historical and / or operational data, correlation to hardware-in-the-loop simulation of small UAVs, and refinement of the algorithms and numerical values to better represent small UAVs.

II. Background and Related Work

2.1 Overview

UAV technology has progressed in parallel with manned aircraft, though their missions and characteristics differ. In the same vein, many UAV vulnerabilities are similar to computer system vulnerabilities, though there are significant differences between the two that warrant separate vulnerability and risk assessment. Chapter 2 discusses the history of small UAVs with emphasis on generalized architecture of the platforms. This is followed by discussion of current research on UAV vulnerabilities grouped by category. Lastly, some background on risk and cyber risk frameworks shows potential for adoption as a UAV cyber risk assessment.

2.2 Brief UAV History

UAVs have been historically built for military applications and continued by hobbyist enthusiasm. By definition, UAV includes any device that can sustain flight autonomously, with similar sub-cultures of Remotely Piloted Vehicles (RPVs) and drones [7]. UAVs are able to either maintain a hover or move completely via computer navigation, whereas RPVs require control instructions throughout flight and drones have even more limited mission and sophistication. In use, the terminology between the three vehicle types is flexible, and a risk assessment for a UAV could cover all of them. William Eddy used cameras attached to lighter-than-air frames during the Spanish-American War for the first use of a drone in combat [7]. As UAV operations and innovations continued through the Vietnam War, Desert Storm, and especially the Global War on Terror (GWOT), the size, mission, and shape of UAVs have morphed in a utilitarian manner to match the needs of the military. Within the last decade, civilian enthusiasts have had increasing access to personal airframes

mainly for photography and video capture.

The exact definitions between sizing tiers have not been standardized between countries, though practically they consist in some format of very small, small, medium, and large. An example grouping from the Department of Defense (DoD) is shown in Figure 1. Very small UAVs exist at a miniaturization of aerodynamics that result in very low Reynolds numbers and are usually less than 20 inches in any dimension. Small UAVs tend to be a range of popular model aircraft used by hobbyists and have at least one dimension greater than 20 inches. While their range may be short, their size and mobility allows for access not normally available to individuals. Medium and Large UAVs are too large for an individual to carry and may even use full runways like light aircraft, which allows for heavier payloads and greater mission duration. Small Unmanned Aerial Vehicles (sUAVs) fly by the same aerodynamics as manned aircraft using lift and drag, plus control for pitch, roll, and yaw. Their internal architecture however differs greatly by removing the human pilot from the vehicle. Instead of a pilot, sUAVs are controlled by varying degrees of autonomy of their autopilot.

2.3 Generalized UAV Architecture

UAVs take a multitude of forms and designs based on mission and user base, from hand-held copters to jet-powered aircraft. Small UAVs follow the general component break out shown in Figure 2, with six common components on the device and a ground station of some sort. The Basic System is a generalized term for the Operating System (OS), which is usually proprietary to the manufacturer and tailored per vehicle, frequently providing near real time control. Modern UAV designs typically combine the Basic System with the autopilot controller, but they are split here to be more general. Communication Links in Commercial Off The Shelfs (COTSs) UAVs are most commonly wireless Radio Frequency (RF) in the public access Industrial,

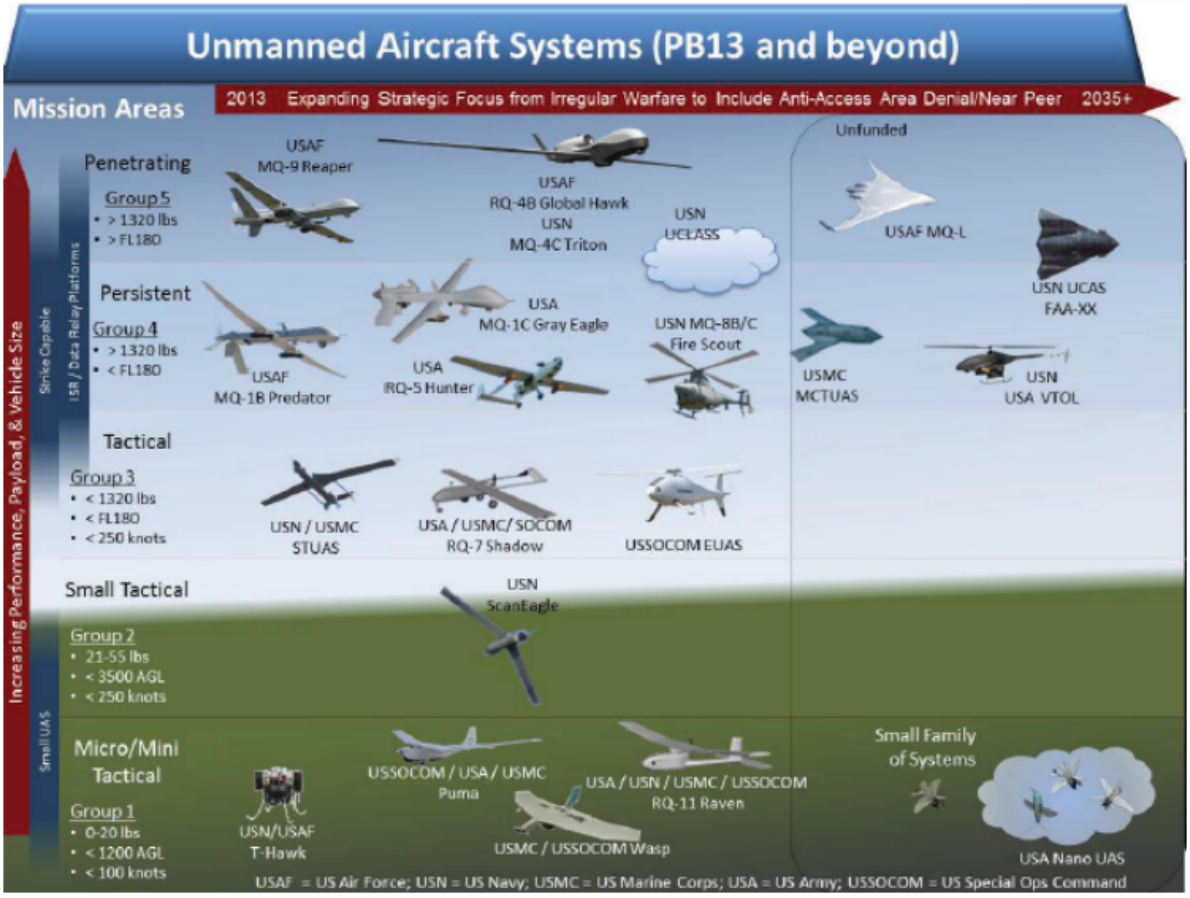

Figure 1. DOD Unmanned Systems Categories [1].

Scientific, and Medical (ISM) bands of 2.4 and 5.8 GHz, the LTE bands, and 915 MHz (433 MHz outside the U.S.). Sensors refer to components that are attached to either aid navigation of the system, such as LIDAR to monitor nearby structures, or for specific mission purposes. Avionics consume sensor input, such as Global Positioning System (GPS) and inertial modules, and provide flight control. For the payload, a weapon component has been seen within military operations, though the vast majority of sUAVs are used for military or hobbyist reconnaissance with only an additional sensor component such as a camera. As defined for UAV, some form of autonomous control is built into the vehicle's navigation, so the autopilot component is separated

from the Basic System.

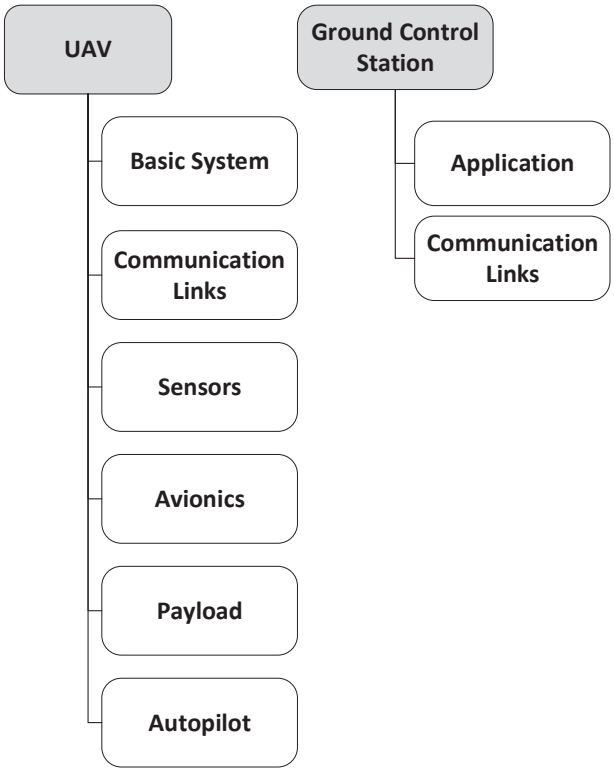

Figure 2. Components of Typical UAV.

The ground station can be decomposed into the Application component and Communication links, though these are typically contained within the same device such as a tablet, phone, or laptop. The complexity and portability of ground stations vary widely from simple RF remote controls to multi-server backends. Examples of these differences can be seen in the common Chinese DJI Sciences and Technologies Limited (DJI) brand, which utilizes both manufacture specific hardware and a smartphone application. The software is extremely portable through mainstream app stores and can be updated over reliable connections. The hardware connects to the user's smartphone to provide controls to the sUAV with separate antennas and power

supply for better coverage. The application can also be used without the hardware through a laptop to program mission states via cable. Some DJI models even allow simple remote controls or beacons without application software, though their mission sets are more rudimentary. Each of these configurations introduce risk characteristics by connecting the device to the greater world differently.

The sUAV Command and Control (C2) architecture may be centralized with a remote operator, or decentralized, as in the case of a group of cooperating sUAVs [8]. With the wide spread of designs, the architectures are best understood on a continuum between the two extremes of fully autonomous systems to completely centralized drones that require all C2 input from a user. By the definition, complete centralization would have almost no autopilot features as all command and control would come from the ground station or other entity. At the other end of the spectrum, the boundary is being pushed experimentally for Artificial Intelligence (AI)-controlled swarm UAVs where each unit communicates with other agents, but controls itself to collectively meet the group's mission. The norm for COTS sUAVs, however, is human control (at the supervisory level) with autopilot for structural avoidance and fail-safes [9]. It is common for systems to change C2 structure between missions or even on the fly depending on available components and mission need.

There are different paradigms for the amount of C2 inputs to the system to ensure mission success, known as Command, Request, or Exception [10]. The Command paradigm means that the UAV only operates from user commands. The Request paradigm means that users send commands only as requests for the system to accept or deny. Exception paradigm means that commands are sent rarely to change autopilot decisions. A particular system may change paradigms mid-mission based on its rule set and the occurrence of events. The different paradigms lead to differing risk in relation to control hijacking.

2.4 UAV Cyber Incidents and Research

Publicly released cyber incidents with and against UAVs have been limited, with the most well-known consisting of the Iranian incident in December 2011 [11]. While confirmation of the exact means of Iranian capture is speculatory [11], the incident highlights the vulnerability of UAVs in a combat zone and the need for cybersecurity in future UAV models to maintain control for mission success. One model for categorizing threats to computer devices was developed by Microsoft and follows the STRIDE acronym [12]. These threats were then correlated to properties of computer security [13], shown in Table 1.

Table 1. STRIDE Model and Related Properties.

Threat	Property
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-Repudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Escalation of Privilege	Authorization

Vulnerability of UAVs has been better defined with the multitude of research being conducted as the cost of systems has dropped, especially for small UAVs. Following the STRIDE model for UAVs, each threat has been studied by the research community at length and a quick summary using the model is provided here.

2.4.1 Spoofing

Instead of blocking signals being utilized by the UAV, one method of attack that has been widely documented by research is breaking the integrity of the navigation signal, with the most common being GPS [14]. GPS works by having the satellite constellation broadcast GPS messages toward Earth, which allows a device to triangulate its own three dimensional location on Earth. The signals, coming from satellites, can

be overridden fairly easily in localized areas, especially by military forces wishing to deny adversaries, as shown in Figure 3. By sending false GPS signals, an adversary can cause UAVs to falsely identify their current location and, as seen in the Iranian incident, be led to a specific location or forced to crash. GPS signals are also used for timing on systems, especially Supervisory Control and Data Acquisition (SCADA) devices far from other sources. GPS spoofing has been shown in timing attacks to be able to change phase settings on high-voltage power lines [15] and cause Denial of Service (DoS) through communication protocols [16]. Navigational security can be gained either by duplicate sensors tracking out of band of each other or by Intrusion Detection Systems (IDSs) that track received inputs and decide if a GPS attack is occurring, though the latter lacks the innate ability to recover current or projected location or timing.

2.4.2 Tampering

The corruption of integrity of signals in and out of a UAV is categorized under Tampering. The signal in question can be data or control signals, though the physical and digital evidence is significantly different [17]. Figure 4 details a control and data signal tampering situation since the attacker has not removed the remote control laptop of the victim from the network. Control tampering is usually simpler in terms of variance of timing since the UAV is somewhat autonomous depending on control architecture; however, a near complete Command architecture requires quick and efficient changes to prevent simple DoS of the device through high latency of C2. High latency in returning data feeds may also serve as evidence of tampering occurring to the victim, though simpler data such as location may show less latency as the change requires less byte manipulation [18]. The result of tampering may be a forced crash or loss of control, or may be as slight and unnoticeable as simulated locations or new

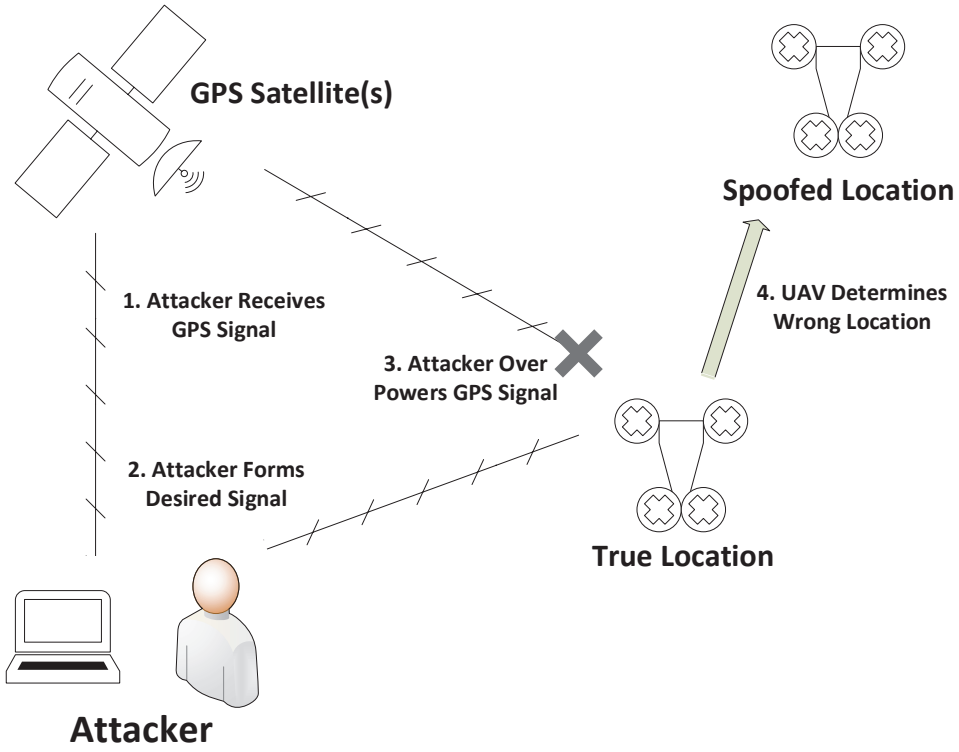

Figure 3. GPS Spoofing on a UAV.

control settings.

2.4.3 Repudiation

Non-Repudiation is when the "sender is provided with proof of delivery and the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data" [19]. From this, the threat of repudiation is any allowed denial by either party; Public Key Infrastructure (PKI) compromises are an example of this threat [20]. Commonly joined with other STRIDE threats, repudiation threats represent a legal risk to any organization or user online [12]. UAVs are particularly threatened by repudiation threats since many small UAVs do not use a PKI protocol

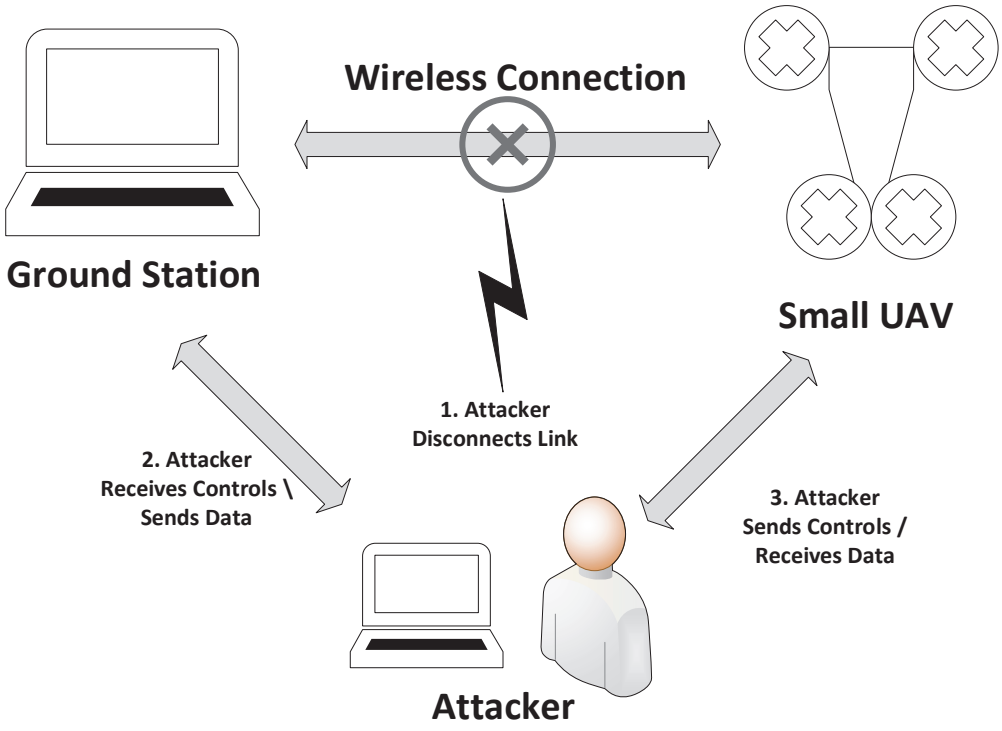

Figure 4. Tampering via Man in the Middle Attack.

and use less secure methods for validating messages. For those UAVs that do properly implement PKI, a compromise of a Certificate Authority (CA) can allow for false positive validation of messages between an attacker and either a ground station or UAV, as seen in Figure 5 [21]. The implicit trust of physical components within a vehicle has less viability over the last decade, though most wireless protocols have some form of identification using a Media Access Control (MAC) or Internet Protocol (IP) address. Remote Control (RC) signals or physically installed Secure Digital (SD) card or Universal Serial Bus (USB) are examples of implicit physical trust giving an attacker an access vector, which may be a threat to the proper user [12].

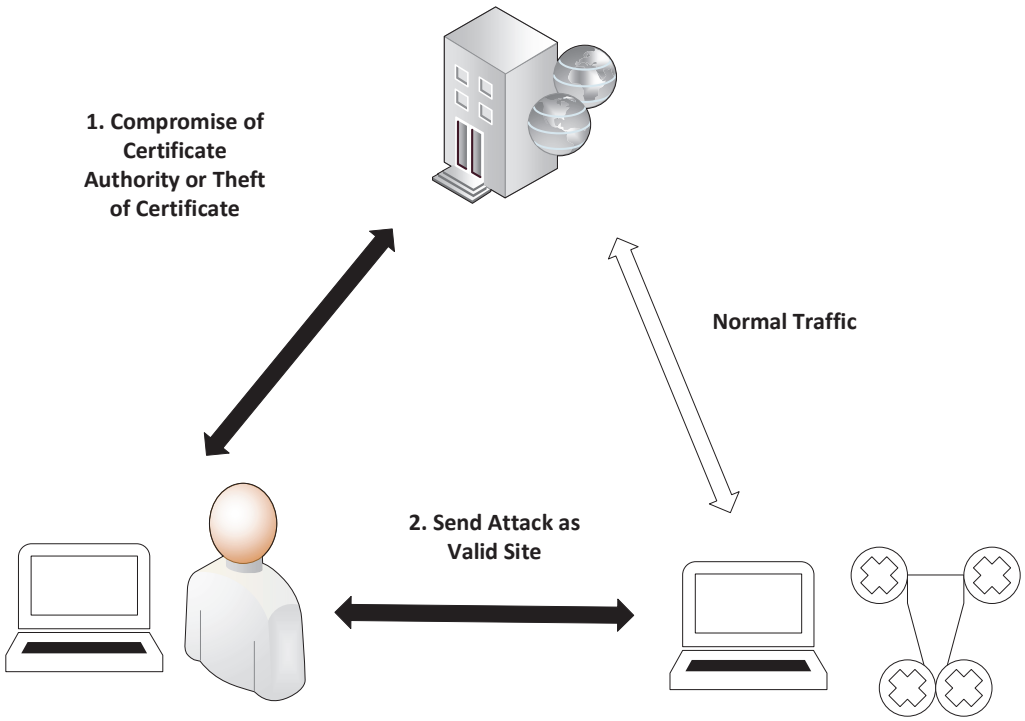

Figure 5. Repudiation Threat through Compromise of Certificate Authority.

2.4.4 Information Disclosure

From the confidentiality aspect of security, the data signal and control signal can be targeted for simple sniffing of the wireless communication, as graphically shown in Figure 6. For simplicity and reduced latency, some sUAV communications tend to operate un-encrypted allowing for easy sniffing of all traffic [22]. If the control stream is captured, the navigational commands are known to the adversary along with the UAVs current and projected location, as well as any transmitted information about the payload. If the data stream is compromised, whatever the device is streaming back to the controller can be captured, which may include sensitive video/audio streams or other sensor data. While usually more of a concern for sensitive government or

military missions, civilians should also be concerned about the risk to their personal information and devices caused by these signals being broadcast in the open [22]. The vulnerability of data leakage depends on the size of fingerprint, degree of signal obscurity, and location. The fingerprint size will vary widely based on the wattage of the transmitter sending the signal and the network's coverage, especially with swarm or ad hoc UAV networks [8]. While most COTS sUAVs operate on the ISM Wi-Fi bands and 915 / 433 MHz, it is possible for UAVs to use any radio medium to transmit; the probability of finding and listening over those channels changes over time. The location of the network in relation to potential listeners also varies across the globe from urban locations to remote deserts, though these distant locations may include expert or known adversarial forces with motive to attempt eavesdropping.

2.4.5 Denial of Service

The easiest and most common vulnerability of sUAVs is DoS attacks [18] by either Electronic Warfare (EW) or accidental electromagnetic interference [17], as shown in Figure 7. Since sUAVs almost exclusively communicate over wireless channels, their shared command and data lines are by definition vulnerable, though the extent is defined by power of signal and amount of signal reuse. For COTS UAVs specifically, command and data is sent over the Wi-Fi bands and 915 / 433 MHz, which is well utilized within urban environments, though a small amount of sUAVs operate over the less power demanding Bluetooth protocol at 2.45GHz. Conflict of signals may lead to slower data transmission rates, corruption of data, or even loss of signal [18]. The Message Drop Rate (MDR) statistic is used to define the weakness of the signal, agnostic to the exact factor causing the loss, whether internal, external, or malicious [17]. As seen in the Iranian incident, UAVs respond differently to loss of command signal, with common methods being hovering, immediate controlled landing, or return

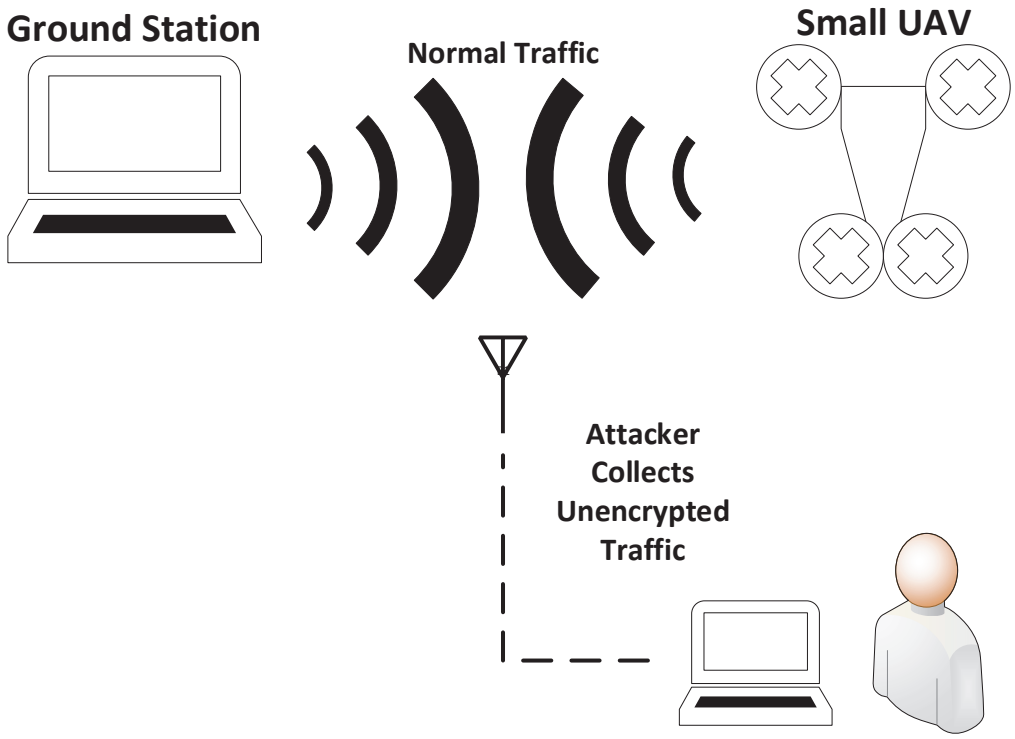

Figure 6. Collection of Un-encrypted Traffic between UAV and Ground Station.

to a home location or last known good signal. If just degraded, the observable physical indicators may be limited to either halting or delay in response time [18].

2.4.6 Elevation of Privilege

Similar in compromising integrity of signals, the control signal has been shown by researchers to be vulnerable to hijacking in UAVs. Similar to Figure 4, the control signal operates by a variety of protocols to stream commands to the device and can be hijacked if another entity is able to convince the device that they are the valid ground station, usually by elevation of privilege from a valid signal. This is different from just a Man in the Middle (MitM) attack where the integrity of the

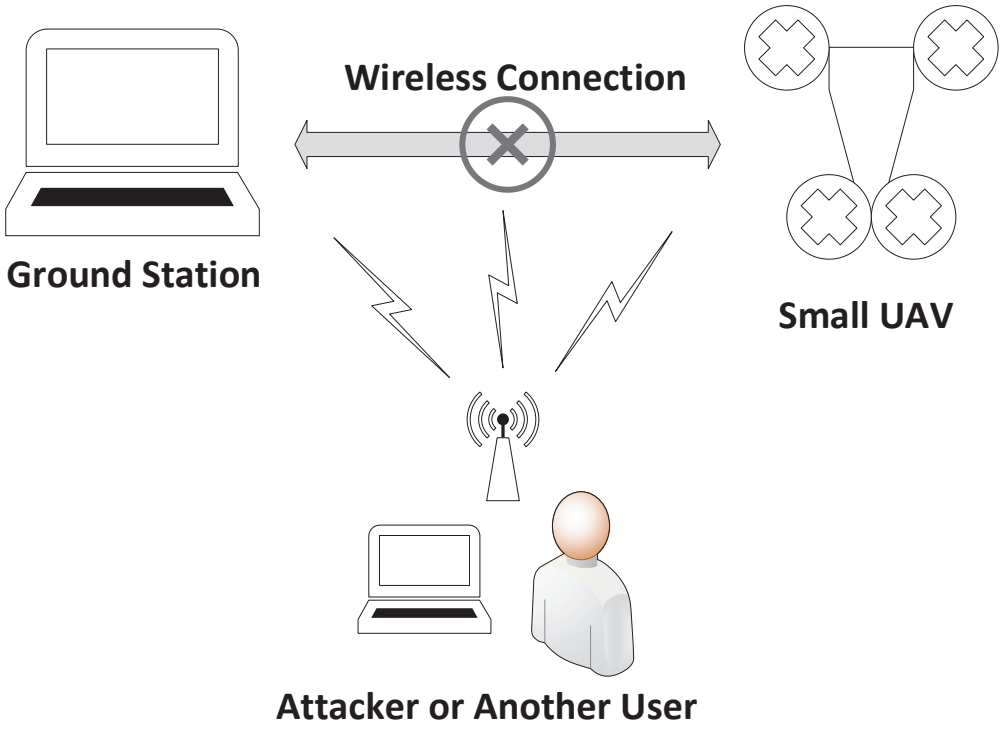

Figure 7. Denial of Service on UAV.

traffic is compromised; elevation of privilege takes primary control of the vehicle away from the original user. Common network attacks that have been shown to work also on UAV networks includes MitM and de-auth/authentication attacks [23]. By convincing the device of a new controller, the device can be sent any valid command and is totally compromised. Also available to adversaries is the tactic of sending bad commands to create fatal errors in the Real Time Operating System (RTOS) and thus system failure, resulting in a crash or failsafe controls such as returning to the home waypoint [22]. More sophisticated attacks are possible through misdirection or deception against the original user for other effects. For example, an attacker can mimic the original user's commands in most cases, but make the user think that the

vehicle is broken to cause loss of confidence in the vehicle or to accelerate replacement, similar to the Stuxnet virus [24].

2.5 Current UAV Frameworks and Index

The field of risk management with UAVs is a multi-dimensional issue. As cyber-physical devices, the risk in question depends on the viewer's perspective. Risk is first defined, then risk in the specific context of UAVs is studied in greater detail moving from higher level operational risk to determining risk prior to purchase. With each step, the pros and cons of determining risk at that level is discussed for determining the most beneficial point to complete, and therefore design, a cyber risk assessment.

2.5.1 General Risk

Quantitative risk assessments are not unique to computers and have existed within the field of commerce (e.g. insurance and investments). The most generalized description of risk is well-known as the product of Cost and Likelihood. Cost is the loss or recovering price tag in the event of a failure. Likelihood is the probability of failure over time or the rate of failure in a specific time frame. Note that the existence of a theoretical failure event does not necessarily result in a risk. For example, if the event were impossible, or if a failure state had no associated cost, there would be no risk. Figure 8 depicts a larger general quantitative assessment process where R(min), R(max) define risk limits, L(max) defines one-time loss limit, and C is the budget [2].

The process shown in Figure 8 takes into account the four options of risk treatment that are available to organizations, which are as follows: Avoidance, Acceptance, Reduction, and Transference [2]. Avoidance is the worst case treatment where the cost has surpassed the max loss value and the probability of compromise is reaching one. Acceptance is the opposite treatment where cost and probability are at levels

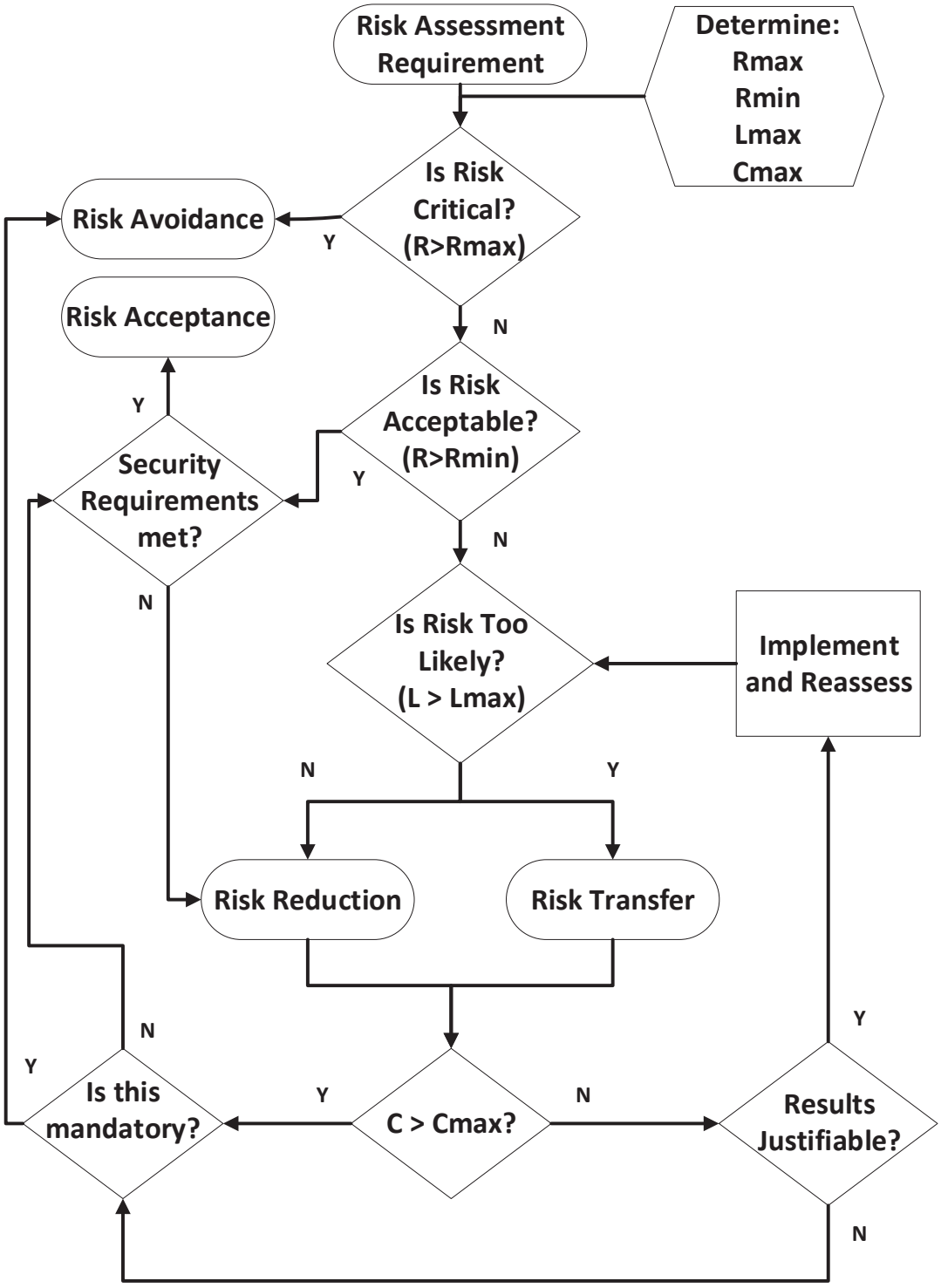

Figure 8. Risk Management Process.

that meet risk management goals. Reduction is the treatment option when the risk level is within requirements, but not below minimum risk (where default treatment is to make no further changes). The last treatment option is Transfer, where the risk is within requirements, but the recovering cost is too much and insurance should be considered. Figure 9 then shows a general view of how best to determine which option to take based on probability of loss (row), loss value (L), and acceptable risk amount (R) which will vary between organizations and over time.

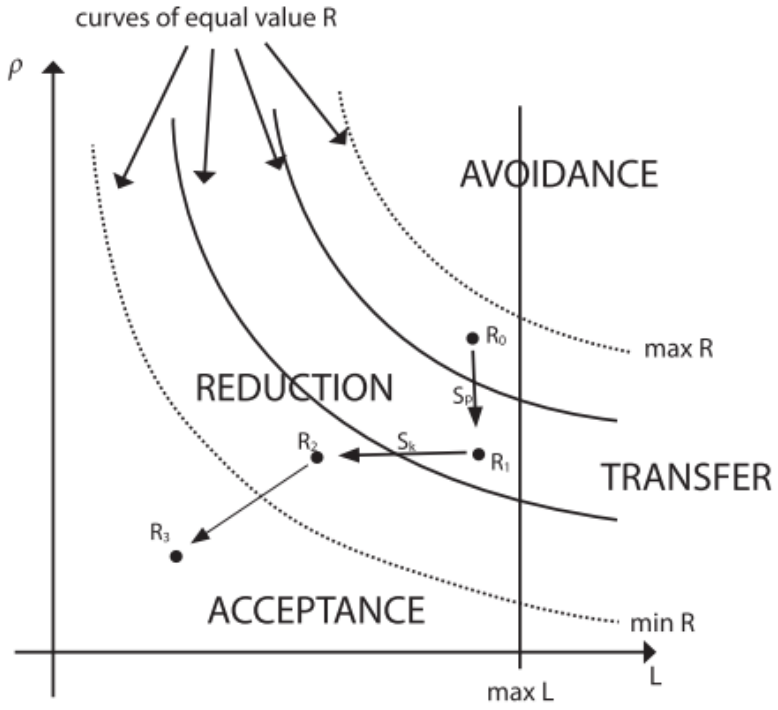

Figure 9. Risk Treatment [2]

A risk framework is the process of defining a policy for managing risks such that strategies employed lead to acceptable risk states [25]. There is no one framework that could be applied to every industry due to different weighting of risk states and definitions of failure. Common frameworks include Risk Management Framework (RMF) as used by the DoD, Cybersecurity Framework (CSF) built for critical infras-

tructure, Information Security Maturity Model (ISMM) and Control Objectives for Information and related Technology (COBIT) [26].

Risk assessments are a sub-set of risk frameworks and attempt to define the risk associated with an individual system versus presenting a process for managing this risk over the long term [25]. Traditional networked computers have been formally assessed as early as 2000 with the first quantitative assessment, Information Security Risk Analysis Method (ISRAM) [26]. The largest separation between risk frameworks and risk assessments is the lack of strategy after defining risk of a device or system, other than an implicit directive to reduce risk. A categorization of risk into tiers is not a risk framework either as it lacks definition into acceptable risk levels and course of action due to the categorization.

All UAV security improvements created due to the vulnerabilities discussed above have been baked-in to new models by manufactures at their discretion for their profit, with very few software patches. Traditional risk frameworks for managing these vulnerabilities disregard UAVs as outside the scope of the Information Technology (IT) networks due to complexity. While UAVs do tend to never connect to organizational networks, the physical proximity, increasing connectivity of devices, and the surge of mission uses will not allow the next generation of frameworks to opt-out of managing the risk intrinsic to all devices with remote capabilities. While many risk frameworks exist for organizations based on size, sophistication, and security, the National Institute of Standards and Technology (NIST) created RMF is the standard adopted by the U.S. DoD for mission assurance and provides flexibility for variations in systems [26]; however, the Government Accountability Office (GAO) found that UAVs, encompassed in Internet of Things (IOT) devices, were not managed by the risk frameworks in practice [26]. Risk frameworks and assessments from pure operational to near-pure UAV assessment will now be discussed to show current research into or

around UAV risk assessments.

2.5.2 Operational Risk Assessment

The research arm of the FAA for the incorporation of small UAVs into the National Airspace System (NAS) is National Aeronautics and Space Administration (NASA) [27]. Due to various commercial ventures requesting access, NASA started development of the UAV Traffic Management (UTM) system in 2014 with the publication of their 15 year plan, with a planned five years until initial deployment [28]. The patent for the UTM was published in 2016 with the addition of classes of airspace based on location, vehicle and population density, and environmental hazards [5]. The basis of connection to this new UTM would include the use of approximately ten new communication protocols as standard on all UAVs, which would each receive flight plan constraints for the individual UAV autopilot to navigate around in real-time called the Unmanned Aerial Vehicle Traffic Management Risk Assessment Framework (URAF), following the logical process shown in Figure 10 [5]. NASA has continued development of the UTM with three studies completed in 2017. The first was a prototype testing of the communication and software systems, plus the first publishing of the philosophies and principles of designed URAF [27]. Across six different FAA UAV test sites, 17 unique aerial vehicles, and 60 additional simulated vehicles, the UTM successfully commanded 102 flights simultaneously with a reported vehicle non-conforming rate of 32.5% [27]. These non-conforming flights represented risk of mid-air collision or collision with building or person that was calculated to be above the nominal risk level.

NASA's URAF Philosophies:

1. Flexibility whenever possible, Structure when necessary

2. Risk-based airspace requirements

NASA's URAF Principles:

1. All UAS, operators, and communications are authenticated before use of the airspace.

2. UAS will avoid each other and other objects.

3. UAS will stay separated from manned aviation.

4. All of the constraints, including dynamic constraints for public safety operations, are available to all stakeholders for common situational awareness.

5. Access will be fair and efficient.

The risk calculation software of the URAF was simultaneously being developed by the next two publications. The first of these analyzed the complexity and accuracy differences between standard and probabilistic risk models to be used in the UTM [29]. With the determination that Bayesian Belief Network (BBN) models would be best able to keep real-time risk estimation, the authors laid out the model for two failure types (return to base and un-powered descent) using six input sensors [29]. The second research effort built and tested the BBN using Hugin Developer suite [30]. The BBN was developed for both of these scenarios using the expected inputs of aircraft down-link, population density, and known environment hazards to calculate the real-time risk through calculations of the probability of expected failure states and the pre-determined possible severity [30].

The URAF's risk modelling software is device agnostic, except for size and weight, which means that the system in no way quantifies cyber risk threat for these UAVs though such efforts would cause "off-nominal trajectories" [30] which NASA and the FAA are attempting to reduce. While regulation of sUAV production to meet the requirements of communicating with the NAS may coincidentally provide some level of

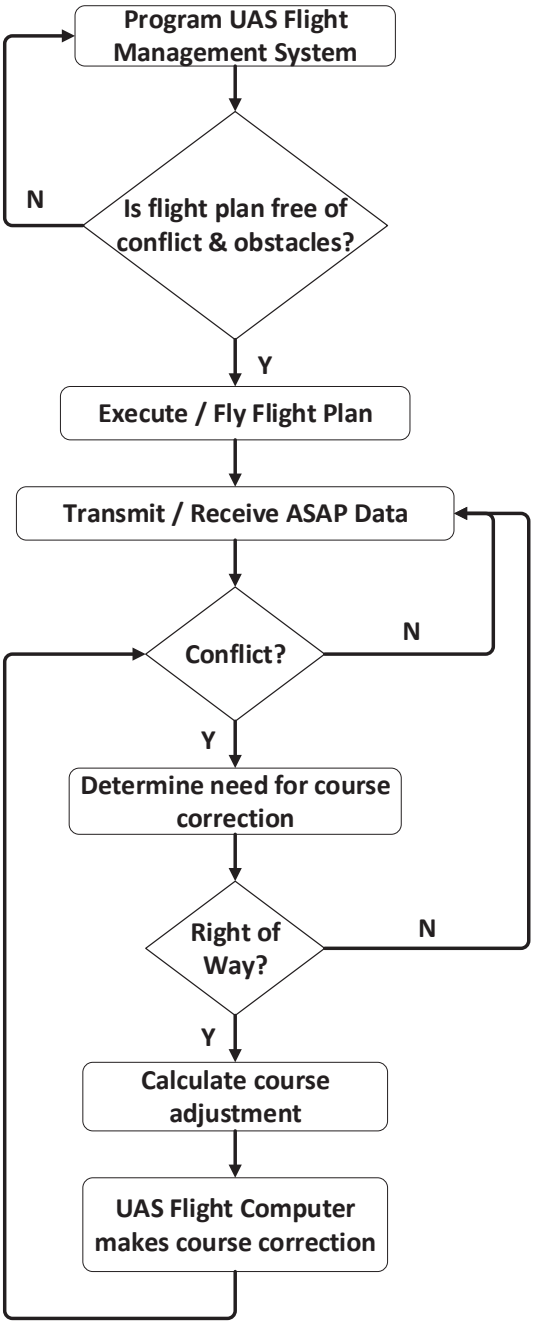

Figure 10. UAV Traffic Management (UTM) Control Flow.

risk reduction for cyber threats, the lack of this goal in their design will mean that this improved posture will be undocumented and ineffective due to conflicting differences between operational risk and cyber risk (large UAVs such as those employed by the military already have to meet aircraft regulations). Traditional aircraft manufacturing also has no cybersecurity regulations for design and no standard for the amount of risk that is acceptable for commercial operation [31]. For an example of a potential cybersecurity regulation introducing operational risk, latency due to encryption on a communication link may lead to mid-air collision. Protection of UAVs against cyber threats therefore needs to occur sooner than the operational level and with specific cyber mindedness.

2.5.3 Network Risk Assessment

Operational risk does not define all of the risk associated with incorporating computers into mission sets today. Cyber attacks and accidents are another aspect of risk that may be missed by solely viewing physical interactions of systems, as seen in the FAA's URAF. When observing operational computer networks directly, cyber risk tends to be the main focus, as seen next with cyber risk frameworks, insurance modeling, and critical infrastructure.

Cyber Risk Framework: The lead organization for reducing cyber risk for the Department of Defence, and setting a popular standard for enterprise and critical infrastructure risk management, is National Institute of Standards and Technology (NIST) [26]. NIST first published the Cybersecurity Framework (CSF) as a tool to provide a "voluntary risk-based cybersecurity framework to help organizations manage cybersecurity risks" [32]. While CSF is designed directly for critical infrastructure and higher risk systems, a parallel framework was also published for enterprise networks as the Risk Management Framework (RMF) directly for the Department of

Defense [26]. The RMF process is a six step qualitative study and mitigation strategy as shown on Table 11. For devices on the network and their connections, a secure baseline configuration is built following common secure networking and configuration techniques. Devices that do not meet the traditional mitigation strategies, for example IOT devices, are simply segmented away from the network or expelled [26]. Living document style reporting and individualized baselines do allow for flexibility in classifying devices, even IOT, which are commonly missed by current scanning tools. UAVs fall into this hands-off category and a risk scoring system would be a boon to managing their risk within RMF instead of rejecting.

Insurance Modeling: As a growing variation of quantitative cyber risk, insurance policies have been diverting some of the risk of exploitation since 1997 when the Internet use globally was only 1.7% of the population [33]. Insurance companies function on a strategy of taking premiums upfront to cover the risk of failure in the future and spread out the cost for the user, whether for disaster, health care, or cyber attack. The Internet has since exploded in size with the total cyber insurance market estimated at $3 to 3.5 billion in 2017 [34], with cyber crimes costing the global economy an estimated $450 billion in 2016 [35]. The companies that issued cyber insurance premiums totaling $1.35 billion in 2016 [36] did so based more on an abstract perception of risk due to a lack of historical data to determine probability and actual monetary damage for previous attacks, especially when the damage is information theft or leakage [37]. The most common and simple equation for insurance is based on historical average of cost per incident times the probability of incident in the near future [38], which requires the very information that is lacking or obscured for cyber incidents. To reconcile this discrepancy in information, several research models have been developed to validate insurance investment though fewer have published methods of quantitative risk indexes. Research suggests that cyber insurance is fea-

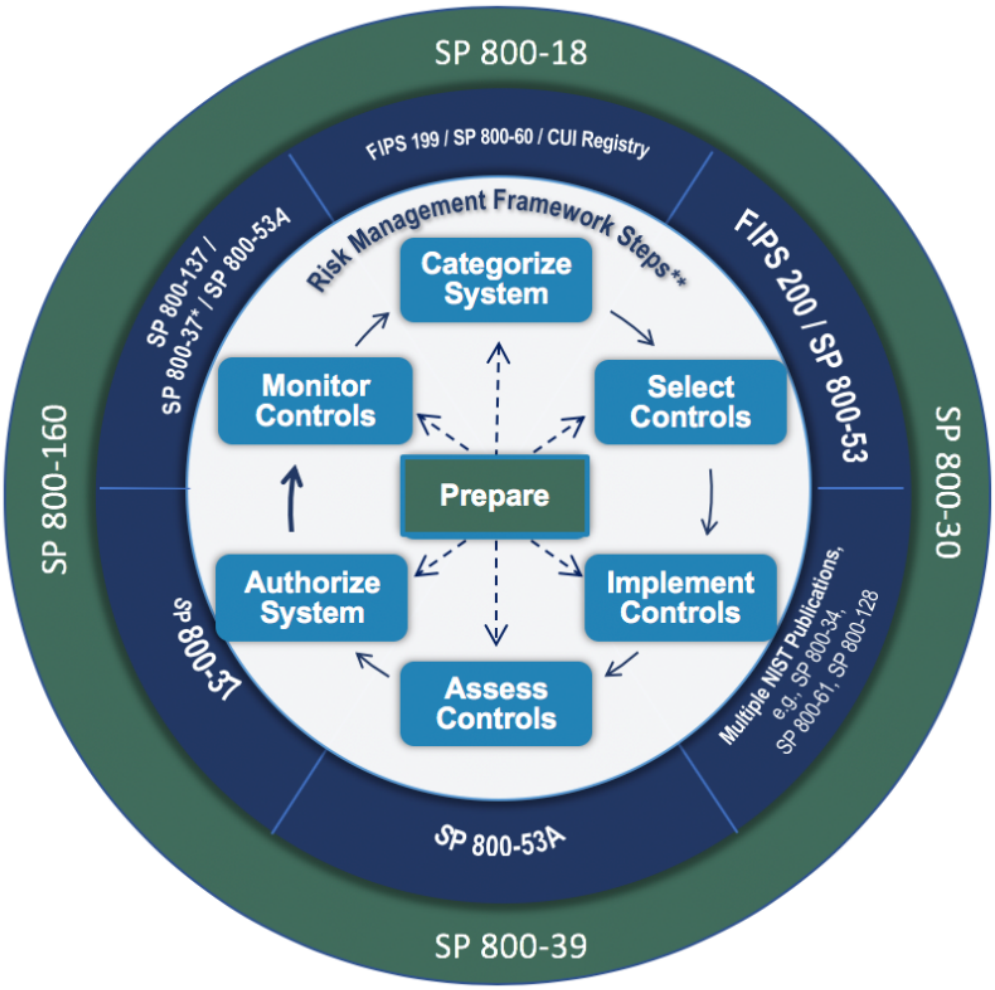

Figure 11. Risk Management Framework [3].

sible and a positive for security, as long as the premiums charged are tied directly to self-protection strategies employed by the organization [39]. For quantifying this risk versus protections, the largest issue is not previous historical data which will continue to grow over time, but mapping all possible attack vectors in the insured system which requires knowledge of all locations of valuable information and employee accesses and habits [40].

The most promising method to grasp the state of a computer network from the

cyber insurance industry is presented by the Cyber Risk Scoring and Mitigation Tool (CRISM) which operates continuously as a specially designed IDS developed at Old Dominion University [38]. Based on the recent use of plug-in devices by automobile insurance companies, CRISM maps out a connected network, uses National Vulnerabilities Database (NVD) to determine and prioritize vulnerabilities present, calculate likelihood of exploitation via BBN, then scores the risk of the network in near real-time to allow for monitoring, as shown in Figure 12 [38]. First published in 2017, CRISM is still in development, unlike CSF and RMF which are in wide-spread practice [26].

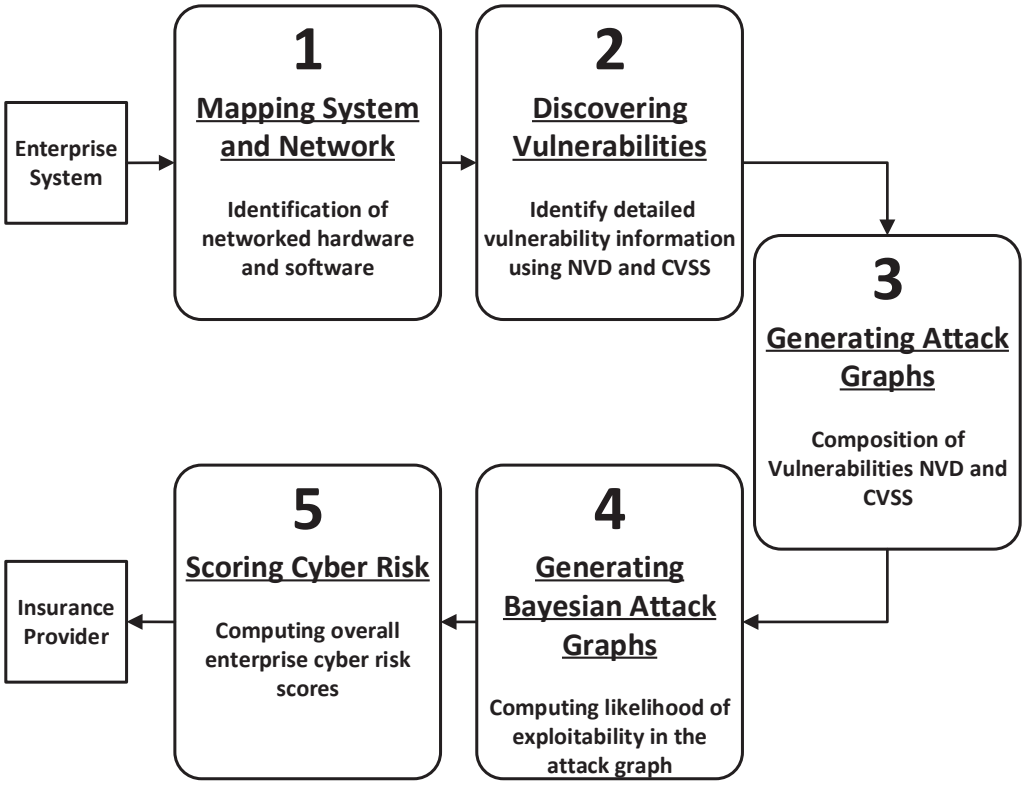

Figure 12. Five phases of the CRISM tool.

Critical Infrastructure: Industrial Cyber Physical System (CPS) and SCADA have been utilized to gradually reduce required human interaction in safety-compromised work areas and in wide distributed networks. Physical sensors formerly required eyes to read, determine system state, and adjust actuators to keep processes within safety

limits and manufacturing effectiveness. As CPS stations are utilitarian and usually connected to physical sensors for input, protection schemes need to adjust for their physical process monitoring, closed control loops, attack sophistication, and legacy technology [41]. Regular IT exploitation follows a typical path that ends at an IT node with information which is valuable in itself; whereas industrial CPS exploitation usually requires further exploitation to influence physical processes to either ruin or shut down systems [42]. Research into adding cybersecurity to CPS systems skyrocketed after the discovery of the sophisticated Stuxnet virus in a nuclear plant. The nuclear plant in question has been studied, with its cybersecurity posture matching industry standards and much of the IT standards [43]. At the direction of Department of Homeland Security (DHS), NIST published the CSF to directly define the risk framework for critical infrastructure in the U.S. [44]. The core of the framework is the process of Identify, Protect, Detect, Respond, and Recover [44]. While the framework does reduce the footprint and likelihood of attack, there is no assessment of the risk state of the system nor a method of comparison between systems [45]. Even within a review of 24 critical infrastructure cyber risk assessments, all lacked either initial network mapping, historical data driven statistics, or only relied on known vulnerabilities [46].

Attempting to overcome these current assessments' shortcomings, Cyber Security Risk Index (CSRI) is a proposed and beta risk assessment specifically using Bayesian Networks since systems should be defined through CSF [47]. To cover the cyber-to-physical risk, the most common technique is to use Markov chains in conjunction with the Bayesian Networks which allows for distinct states along with probabilities of events [48]. A major drive to Bayesian networks is the complex states that physical processes may enter, which differ on Mean Time to Shut Down (MTTSD). While the probabilities to reach across the IT network to the Programmable Logic Controllers

Table 2. Cybersecurity Framework Core and Sub-Categories.

Core Phases	Sub-Categories
Identify	• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy • Supply Chain Risk Management
Protect	• Identity Management and Access Control • Awareness and Training • Data Security • Information Protection Processes and Procedures • Maintenance • Protective Technology
Detect	• Anomalies and Events • Security Continuous Monitoring • Detection Processes
Respond	• Response Planning • Communications • Analysis • Mitigation • Improvements
Recovery	• Recovery Planning • Improvements • Communications

(PLCs) follow well-documented methods and means through NVD or Cyber Vulnerability and Scoring System (CVSS), detection, and vectors at the PLCs require expert weighting and most likely proprietary input [45]. CSRI shows particular promise to the critical infrastructure field since penetration testing is near impossible and simulations are difficult without the hardware in the loop [47]. Detection before shut down is limited within industrial CPS to IT IDSs that are built to overcome the unique aspects within industrial networks [41]. Even with research progressing to better characterize the risk statically and dynamically present in industrial CPS, there are no open-source rating systems in circulation, though cybersecurity companies specializing in control systems are starting to use them to better define current risk and prioritize defensive actions. While a SCADA risk index has potential for use within the UAV community, the lack of an operational open-source index, smaller scale of systems, and the shorter lifespan of systems reduce direct applicability to sUAVs.

2.5.4 Vulnerability Severity Scoring

Today's most utilized quantitative vulnerability severity assessment tool is CVSS [49], maintained by Forum of Incident Response and Security Teams (FIRST) Inc. As an "open framework for communication of the characteristics and severity of software vulnerabilities" [4], CVSS provides data points to the NVD and Common Vulnerabilities and Exploitations (CVE) databases, which are from there utilized by risk frameworks to define vulnerability of networks. The most current version 3.1 calculates a Base score from 0.0 to 10.0 through eight metrics seen in Table 13. This Base score is then modified by Temporal and Environmental factors to give the final score also ranging from 0.0 to 10.0 and is specific for the investigated network or device. An Extensions Framework optionally allows for the manual adjustment of factors for specific fields, although there is no published framework for UAVs.

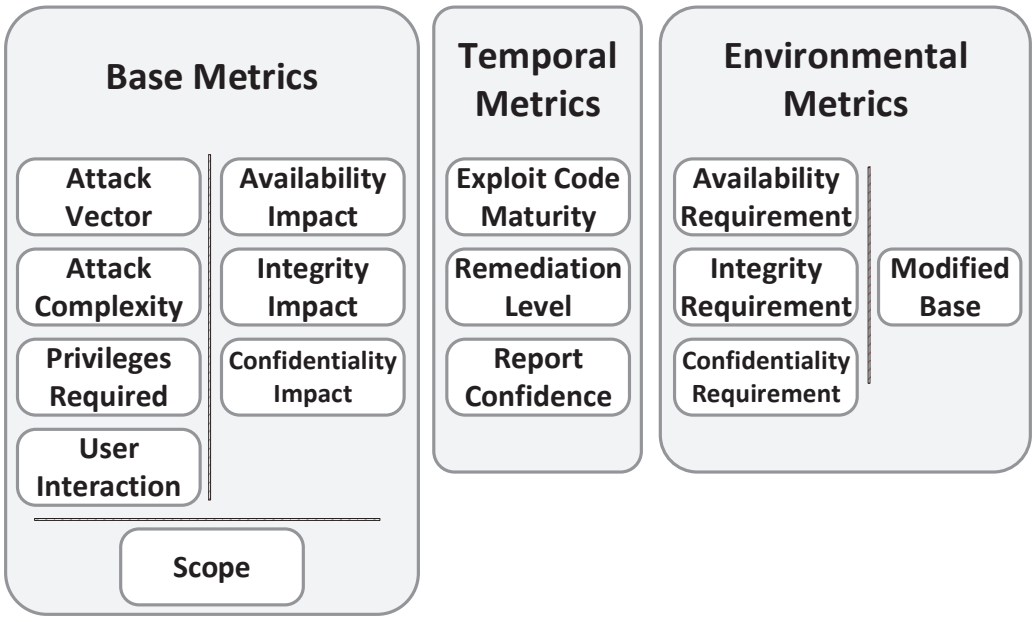

Figure 13. CVSS v3.1 Metrics [4].

Since risk is most commonly defined as the product of cost and likelihood, CVSS is designed only to better define the cost variable to a customer [4]. Several proposed risk frameworks attempt to utilize CVSS directly by setting the likelihood probability to one for worst case [50], to another constant, or to a value that increases or decreases over time. In addition to not predicting likelihood, CVSS also does not define devices and thus does not take into account device mission, which is of critical value to UAVs [11]. CVSS provides the most robust, widely applied, and therefore useful scoring system for cyber devices on the market. More discussion on the CVSS framework and calculations can be found in Chapter 3 as the framework is a basis for the risk assessment built in this research.

2.5.5 Pre-operational Risk Assessment

In the attempt to move risk assessments earlier in the life cycle process, there are several research fields that have researchers working to build risk assessments meant for acquisition, of which traditional aircraft, healthcare, and a UAV specific assessment will be discussed.

Traditional Aircraft: With nearly all on-board components being seen on both traditional aircraft and small UAVs, a cyber risk assessment for aircraft could be assumed to be the best translation to sUAVs, especially taking into account cyber-physical aspects that are not seen in other IT fields. Regrettably, the commercial aircraft industry does not currently have any cyber assessments for risk [31]. While industry standards for the design of aircraft information systems exist that incorporate defense in depth (RTCA SC-216 and EUROCAE WG-72), there is no measure of how well these standards were implemented or any comparison between vehicles, and no expected updates to either standard through 2021 [31]. The Aerospace Industries Association (AIA) Civil Aerospace Cybersecurity subcommittee identified that each manufacturer and operator defines their own risk framework and assessment of cyber risk on their aircraft; therefore, there is no commercial aviation cyber safety Cyber Action Team (CAT) to set standards and respond to incidents [31]. As one of the key priorities of the report, the AIA subcommittee published the statement that the industry needs "a risk managed approach...to architect future secure systems" and "better global visibility...to address aviation ecosystem threats and risks" [31].

Healthcare: Within the healthcare field, only 61% of organizations are currently using cyber risk management [51]. Since cyber flaws were only being treated as device flaws that were corrected through long-term regulations by the Food and Drug Administration (FDA), Stine proposed a medical device risk assessment that would allow for understanding of risk in hospitals, prioritization of devices requiring ad-

ditional protection, and ease of calculation for the low cyber awareness of general healthcare practitioners [50]. Stine created a cyber risk scoring system through two steps: severity of worst case scenario and the amount of security features present. The worst case scenario was judged on the System Administration, Networking, and Security (SANS) objectives [52] with five available severity tiers. For each attribute and tier, Stine manually developed constants that could be summed for the overall risk of the device, with the highest risk tier being the basis and a 2:1 ratio of equivalency to the next lower tier [50]. Each attribute tier was described in healthcare laymen terminology of cyber effects and was focused on the worst case scenario of misdiagnosis or causing human death in another manner. This mission focus captures the unique characteristics and requirements of healthcare devices versus other risk frameworks for IT networks. Shown in Table 3, the attributes and tiers are built with the attacker's purpose in mind, instead of simple IT sanitation.

Table 3. SANS Objectives.

Action	System Component
Loss of:	View Control
Denial of:	View Control Sensors
Manipulation of:	View Control Sensors Safety

The second stage of Stine's scoring system was the employment of security features within or connected to the device in question to reduce the previously calculated step. The security features were designed as a nine question survey which should all be answerable by a professional or from the specifications guide for the device. The questions were borrowed from Microsoft's STRIDE model which was described

in the first part of this chapter, but also proposed each defensive attribute as one or two questions to better define characteristics of proper risk management in cyber as seen in Table 4 [50]. For each positive response to a question, the proportion of that category is reduced from the appropriated SANS objectives.

Table 4. STRIDE Properties with Defining Security Questions.

Property	Security Question
Authentication	Does the system use multi-factor authentication? Does the system enforce secure credential creation, usage, and maintenance principles?
Integrity	Can the system detect and prevent manipulated parameters? Does the system protect against tampering and reverse engineering? Were secure software design principles followed during development?
Non-Repudiation	Does the system verify and log all user actions with attribution?
Confidentiality	Does the system follow industry standard encryption practices to secure connections?
Availability	Was the system built and tested for high availability (e.g., fuzz testing and load testing)?
Authorization	Does the system allow for management of all users and privileges?

While Stine met the set goals of Ease of Use, Low Cost, and Understandable Results [50], the scoring system lacked significant scoring fidelity due to the limited scored attributes, though this in some part is due to the wide range of healthcare devices. The use of manually crafted constants to define the risk of an attribute's severity to the overall risk of the device also requires significantly more application to devices to prove the accuracy of use.

Small UAV: Hartmann and Steup's scoring system shows the current threshold for a quantifiable cyber risk score, though with significant shortcomings. The authors define the general internal network of UAVs with the most vulnerable components as communication links, sensors, data storage, and autopilot configurations [53]. By defining the hardware and software of each of these components through a survey of the market, corresponding attributes were defined with the autopilot being simplified to its fail-safe state and the sensors being increased to four configurations and three

combinations. The attribute of Environment was also added in with the imperative that any risk assessment for UAVs must include the risk inherit to the operational environment and the mission set [53]. Each of these attributes then were judged according to Confidentiality, Integrity, and Availability (CIA) with a subjective assessment of values from zero to one based on the author's perceived associated risk . The summation of these values were then used as the calculated risk of device with larger values corresponding to more risk. Lacking in categorization of risk and what values are acceptable, the simple calculation lacked detail describing what the risk value meant. Though stating that mission sets must be included, the authors also failed to create any attribute for calculation or factoring. The use of defining key components through surveying the breadth of common configurations for use in defining risk is useful due to the lack of databases of known vulnerabilities.

Though there are several risk assessments around the employment of sUAVs, none mentioned here properly capture the cyber risk of the unique devices to an organization's greater network. While many organizations do employ cyber risk frameworks to make a concerted decision based on the risk present, the decision is built on little information if the device is assessed incorrectly or not at all. Operational risk of sUAVs is important to safety, as tackled in NASA's UTM; however, the real-time assessment treats all aircraft as nearly identical except for physics, which is simply incorrect for cyber threats. Risk assessments from parallel cyber security realms show important lessons learned and build out valuable objectives for a sUAVs risk assessment. In the next chapter, a new cyber risk assessment is defined using the foundation of CVSS and all of the lessons learned from previous attempts.

III. Risk Scoring System

3.1 Framework Overview

With the growing number of small UAVs being used for private and public mission sets, a framework is required for determining the differing risks between devices. This framework identifies component based security weaknesses and merges that with mission and environment requirements for a quantification of risk. A risk framework for UAVs must be easily understood by consumers and raters and general enough to allow for applicability across the rapidly changing designs coming to market.

3.2 Framework

To accomplish the ease of use objective, the CVSS scoring system is foundational to the design of this framework. CVSS provides common nomenclature for cyber risk managers currently securing networks and verified quantification constants in their algorithms proven over years and volume of use. The model of Base metric modified by Temporal and Environment metrics provides a contemporary risk framework to ease adoption. As described in Chapter 2, CVSS does not score risk, but severity of vulnerabilities, so substantive changes are required to shift the focus to device risk and to adapt to the UAV domain in particular. A simple extensions framework as provisioned in version 3.1 would not update the original scoring system to rate any metric outside of severity of vulnerabilities as the extensions framework merely tweaks constants within the equations. This framework redefines several sub-metrics, while maintaining as much of the CVSS structure as possible. This should allow mission owners with limited knowledge of cyber risks to define and rate UAVs for their organizations, providing insight into the risks of any device considered for acquisition.

The breadth and variability objective of this framework is accomplished also

through the foundation of CVSS as a 0.0 to 10.0 scoring system with risk categories from High to Low. The simplicity of the final score allows for quick yet accurate comparison of potential devices on the market. CVSS reaches this final score through nuanced math equations that include prioritization of risks, unique modifications, and breadth of the vulnerabilities. All of this is abstracted to a final score for consumers without loss of fidelity.

Lastly, general applicability for the breadth of the UAV market looking to the future is built in to the framework through the use of abstracted questions with example configurations. The current market provides a baseline for this scoring framework, but is not limited by this as new models are developed. It is expected that major changes to the market in the form of new regulations or sensors may require updates to this framework, but not at the same rate as new vehicles being released which would be unmanageable. By providing a volume of grading sub-metrics, new releases to UAV configurations can be reflected immediately and provide insight to the new risk accepted by consumers to their missions.

3.2.1 Base Metrics

Attack Vector (AV) is the sub-metric of connection of the device to potential attackers. Similar to IT networked devices, the required logical location of an attacker directly correlates to the risk of the device being attacked due to the size of the potential attacker pool and increased automation of scanning and exploiting, as shown in Table 5. A UAV with Direct connection to the Internet with an IP address is the most at risk variation as commands could be crafted from anywhere. The more common case is that the Ground Controller has access to the Internet, whether through cable, Wi-Fi, or mobile services. This configuration reduces risk by requiring an attacker to compromise, prior to attacking the device, the ground controller or a third-party

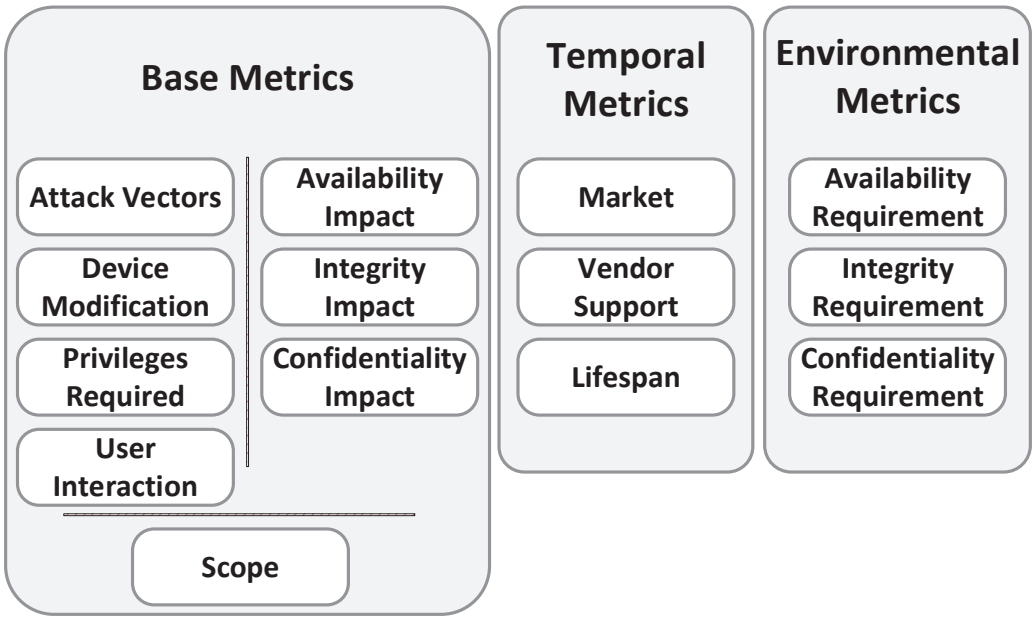

Figure 14. New Proposed sUAV Risk Assessment Metrics.

server which may be acting as the ground controller through the laptop or phone. Less risk is assumed if the ground controller or mission data is Air-Gapped from the UAV through use of a separate memory device or disabling of connections to the ground controller, which require persistent compromise of the ground controller. Lastly, if no Internet connection is involved with the UAV at any time, then an attacker must be physically present to override or block command and data signals. This None value is most commonly found with cheaper RC variants of UAVs, or those configured for fully automated missions with no human-in-the-loop.

The second sub-metric of the Base Score is Device Modification (DM), which analyzes how standard the device is to its brand's advertising or specifications, and is shown in Table 6. The most common COTS UAVs purchased have a base-line model with few (if any) variations, and all of them represent a higher level of risk since the attacker has less device discovery and more confidence of repeatability between the

Table 5. Attack Vector Values.

Base Level	Description
Direct	The UAV is bound to the network directly and the set of possible attackers extends to the entire Internet. Such a device is often termed "remotely exploitable" and can be thought of as being exploitable at the protocol level one or more network hops away.
Ground Controller	The UAV is indirectly bound to the entire Internet through the ground controller. An attacker may utilize persistent or live exploitation to the ground controller for persistent or live exploitation of the UAV.
Air-Gapped	The UAV is not bound to the network and the attacker's path is via persistent read/write/execute capabilities on the ground controller. Either the attacker exploits the vulnerability by accessing the ground controller while not connected to the UAV or the attacker relies on persistent code to modify commands live to the UAV.
None	An attack requires the attacker to be physically present to manipulate the vulnerable component. Physical interaction may be brief or persistent.

same models. The other extreme is a complete Do-It-Yourself (DIY) UAV that has no standard configuration and is close to being unique. The DIY UAV will most likely utilize standard protocols and hardware, but risk has been lessened by the increase in discovery and decrease in repeatability available to an attacker. If a standard UAV has one or more custom modifications, including payload(s), then the device may be labelled as having a High Device Modification as the attacker can not assume standard interactions.

Table 6. Device Modification Values.

Base Level	Description
Low	Specialized modifications or extenuating circumstances do not exist. An attacker can expect repeatable success when attacking the vulnerable UAV.
High	The UAV has one or more custom modifications or extenuating circumstances. That is, a successful attack cannot be accomplished at will, but requires the attacker to invest in some measurable amount of effort in preparation or execution against the unique vulnerable UAV before a successful attack can be expected.

Privileges Required (PR) is the sub-metric that defines the software design of com-

ponents implementing appropriate privilege delineation, as shown in Table 7. Unlike common IT networks, UAVs typically have the assumption that the connected user, whether physically or wirelessly, is the administrative user with the only other privilege level being a kernel variety that is used by the OS. Authentication for communication and commands, and authentication prior to access at rest show High levels of separation.As an example of Low value, the wireless protocol of a UAV requires some authentication such as through 802.11 and only flight logs are stored openly via physical memory card then the default Low value is appropriate. If the communication protocols allow any signal received to be executed or valuable flight data and commands are accessible physically by any user with a cable, then the level of privileges required is None.

Table 7. Privileges Required Values.

Base Level	Description
None	The attacker does not require authentication prior to attack, and therefore does not require any access to settings or files of the vulnerable system to carry out an attack.
Low	The attacker requires privileges that provide basic user capabilities that could normally affect only settings and files available to any connection physical or logical. Alternatively, an attacker with Low privileges has the ability to access only non-sensitive resources.
High	The attacker requires privileges that provide significant control over the vulnerable UAV allowing access to device-wide settings and files.

The next sub-metric of the Base Score is Scope (S), which is an evaluation of risk associated with an attack on the device spreading to other devices. While many UAVs are operated within a one user / one device schema, ad hoc networking and swarm technologies are gaining viability, with the risk levels shown in Table 8. The addition of trust of connected agents to a targeted UAV increases the risk of association with compromised agents and increases the likelihood of an attack on the device in question, similar to IT networks. The connection can vary from command signals to simple navigational directions, but a single vulnerable device has the potential to

wreck others in the network or compromise a mission. The NAS is not included in this sub-metric's assessment as the NAS includes calculations from internal sensors and every other vehicle in the airspace for validation, though its risk does also increase with compromised integrity. If the system in question is networked with other UAV systems, then the Scope is rated Changed. Otherwise, the sub-metric is rated Unchanged.

Table 8. Scope Values.

Base Level	Description
Unchanged	An exploited UAV can only affect resources local to that device or ground controller. In this case, the vulnerable device and the impacted device are the same.
Changed	An exploited UAV can affect other devices beyond the local scope. In this case, the vulnerable device and the impacted device may be different as the vulnerable device can impact others.

The next sub-metric of the Base Score is User Interaction (UI), which is the evaluation of the risk associated with not including a human in the loop, with the risk levels shown in Table 9. As explained previously, architectures range from fully autonomous, to supervisory, to full control. When a UAV has complete control of its flight, assuming some preset mission parameters, the user does not have the ability to override incorrect decisions made by the system. This autonomy may be a necessity arising from communication restrictions such as distance or a design feature to fire and forget. With any amount of user interaction, errors or compromises to the mission may be counter-acted, such as GPS spoofing being counter-acted with new way points or direct first-person control. If an attacker is able to make changes to the system without authorized user interaction, then the sub-metric is rated None. A system that is programmed in such a way that requires human-in-the-loop would be rated as Required interaction.

The next three sub-metrics of the Base Score are related to the impact of an attack on the device. The first is the Confidentiality Impact (C), which analyzes

Table 9. User Interaction Values.

Base Level	Description
None	The vulnerable system can be exploited without interaction from any user.
Required	The system requires authorized user interaction for system or mission changes. Attacker must social engineer their attack for the authorized user to accept.

the securities in place on the device to lessen the threat of a confidentiality breach. Confidentiality is the security objective of restricting access to information at appropriate pre-determined levels. Security activities enforcing this include encryption of data at rest and Over-The-Air (OTA), as explained in Table 10. "Encryption of data storage" assumes authorization protocols are in place to access data logs, mission data, and user settings, each of which may contain sensitive information. OTA encryption, which may be enforced by the wireless protocols utilized or manually with in-house encryption, ensures that sensitive data in transit between device and ground controller is not eavesdropped on or collected. Not all data on or transiting a UAV may be considered sensitive information by the user, and as such lower coverage or levels of encryption may be considered sufficient security with lower associated risk.

Table 10. Confidentiality Impact Values.

Base Level	Description
None	There is no confidentiality security in place, resulting in all resources within or transmitting from the impacted UAV being divulged to an attacker. Alternatively, there is no security protection of some specific restricted information, and this sensitive information presents a direct, serious impact to the user.
Low	There is some confidentiality security in place. Access to some restricted information is not secured, but the amount or kind of loss is limited. The information unsecured does not cause a direct, serious loss to the user.
High	There is no loss of confidentiality within the impacted UAV or in its communications due to proper security in place.

The next impact sub-metric is Integrity Impact (I), which analyzes the securities in place on the device and on its communication links to enforce integrity, as shown

in Table 11. Integrity is the security objective of verifying that information present is the correct or intended information, and the information has not been tampered with by an attacker. These securities usually are included based on the type of protocols used for communication with check sums, cryptography methods, or through self-diagnostics.

Table 11. Integrity Impact Values.

Base Level	Description
None	There are no protections of integrity in place on the UAV. The attacker is able to modify any/all files without detection. Alternatively, only some files can be modified, but malicious modification would present a direct, serious consequence to the impacted component.
Low	There are some protections in place, but modification of data is possible. However, attacker does not have control over the consequence of a modification, or the amount of modification is limited. The data modification does not have direct, serious impact on the impacted component.
High	There is no loss of integrity within the impacted UAV or in its communication links.

The last sub-metric of the Base Score is Availability Impact (A), and the levels are shown in Table 12. Availability Impact analyzes the level of security allowing for continued availability of communication links, whether from an attack or from non-malicious electromagnetic interference. Availability is most commonly secured through multi-channel communication and is important for both the command and data signals. Multi-channel communication may be built into a wireless protocol or be present via hardware in multi-protocol communications. If the redundant channels are only minor (such as changing Wi-Fi channels) or require a hard switch (such as turning off the current channel and switching to another wireless medium), then the security level is shown as the Low level as availability was lost briefly or had increased probability of control or reception being regained.

Table 12. Availability Impact Values.

Base Level	Description
None	There is no availability security, resulting in the attacker being able to fully deny access to resources of the impacted UAV; this loss is either sustained or persistent. Alternatively, the attacker has the ability to deny some availability, but the loss of availability presents a direct, serious consequence to the impacted UAV.
Low	There are some protections to availability in place, or the protections are not persistent. The resources in the impacted UAV are either partially available all the time, or fully available only some of the time, but overall there is no direct, serious consequence to the impacted component.
High	There is no impact to availability within the impacted UAV's communication links or there is no threat to availability. For example, a pre-programmed UAV which only collects information locally may be considered fully available as no signals are present to be lost, as long as the device continues operation.

3.2.2 Temporal Metrics

A significant aspect of cyber risk is its ability to change over time. The temporal sub-metrics each represent aspects of the risk of the device that are evaluated at certain instant in time that is also understood to change after a period of time. From an attacker's perspective, time is of the essence and having exploits and tools available prior to targeting greatly decrease the time and cost of carrying out an attack.

The first sub-metric of the Temporal Score is Market (M), which is an assessment of how common the device is around the world and potentially how valuable the UAV is to attackers. Taking directly into account an attacker's motivation, risk is increased if the reward to effort ratio is greater, as shown in Table 13. This metric is constantly changing as the market evolves due to country relations, large organizations make trade deals, and new regulations impact the viability or marketability of UAVs. The market share of each brand and model are normally published at least annually, if not a quarterly basis, especially if the company is publicly traded. For value of an UAV, the principal players of the UAV industry include, but are not limited to, first-world

military inventories, distribution companies, and other large companies that may use UAVs to provide services.

Table 13. Market Values.

Temporal Level	Description
High	50% or more of the market share is held by the UAV brand or the UAV is used by more than one major customer. The device then is expected to hold significant value in the eyes of an attacker.
Medium	More than 25% but less 50% of the market share is owned by the UAV brand or the UAV is used by exactly one major customer. The device then is expected to hold some value in the eyes of an attacker.
Low	Less than 25% of the market share is held by the UAV brand and the UAV is not used by any major customer. The device then is expected to hold low value in the eyes of an attacker.
None	The UAV is either non-standard or homemade, and therefore holds near 0% of the market share. The device then is expected to hold almost no value in the eyes of an attacker.

The next sub-metric of the Temporal Score is Vendor Support (VS) which evaluates the rate or quality of updating a UAV's software and defined in Table 14. Often termed "hotfixes" or "patches", the vendors of computer products still within marketability will release updates in code in response to uncovered vulnerabilities or new features. While UAV vendors release significantly less patches than the IT sector due to the lifespan of device marketability, cyber risk is significantly reduced when time, money, and people are invested to secure current released software. Vendors are not the only party interested in securing software, but the user or research communities often step up to release optional patches when vendors refuse and there is user interest. This metric intrinsically decreases over time as use and interest fade with the release of new models with better features.

The third and last Temporal Score sub-metric is Lifespan (L) which is the evaluation of the expected time remaining of service. Risk is increased when more time is available for the device to be discovered and attacked, as shown in Table 15. While individuals or smaller organizations may not have concrete decisions in place at ac-

Table 14. Vendor Support Values.

Temporal Level	Description
Unavailable	There is no vendor support and no active community support for the UAV. The device is no longer sold new by the vendor and vendor will not provide support for current inventories. An in-house build, though still supported by staff, would still be categorized as no vendor support due to level of support and increased risk.
Low	There is no official vendor support, but there is active community support providing updates or workarounds to vulnerabilities. The device is most likely no longer being sold new by the vendor, though some support may be provided by exception or contract.
Medium	There is occasional official vendor support and there is active community support for the UAV. The device is most likely still being sold new by the vendor, though at least one newer, similar model is marketed by the same vendor.
High	There is active official vendor support and active community support for the UAV. The device is most likely the premier model marketed by the vendor.

quisition, most large organizations determine a life-cycle management plan for new assets where some defined mission life is expected. Different than normal IT equipment in some ways, the life expectancy of a small UAV is most likely less than the planned life-cycle for an organization, so when new models will be purchased needs to be taken into account.

Table 15. Lifespan Values.

Temporal Level	Description
High	The expected lifespan of the UAV for missions is greater than the expected support of the device by the vendor or greater than 2 years.
Normal	The expected lifespan of the UAV for missions is within the expected support of the device or between 1 and 2 years as a normal lifespan.
Low	The expected lifespan of the UAV is less than 1 year and is expected to be discontinued from missions soon.

3.2.3 Environment Metrics

Vital to any UAV risk assessment, mission risk is rated within the Environment metric modifier. The mission requirements are similar to the original CVSS definition

due to the whole device or system being rated for mission requirements, instead of an individual vulnerability. The whole device, here the UAV platform, may be designed for multiple mission sets and therefore must be rated for the highest requirement in each sub-metric. The mission metric is divided into Confidentiality Requirements (CR), Integrity Requirements (IR), and Availability Requirements (AR), following the basic definition for cyber security. Each sub-metric is rated one of three possible levels which are defined in Table 16 and are as follows: High, Medium, Low. Unlike CVSS which includes a Not Defined level, this framework requires a determination of mission requirements with Medium level being the default by having a neutral modifying effect on the Base metric.

Table 16. Environment Sub-Metric Values.

Requirement Level	Description
High	Loss of [Confidentiality — Integrity — Availability] is likely to have a **catastrophic** adverse effect on the organization or the mission.
Medium	Loss of [Confidentiality — Integrity — Availability] is likely to have a **serious** adverse effect on the organization or the mission.
Low	Loss of [Confidentiality — Integrity — Availability] is likely to have a **limited** adverse effect on the organization or the mission.

Included within the Environmental Score of CVSS is the Modified Base Scores, which are duplicates of the Base Score sub-metric that are adjusted for the specific situation of the device in question. CVSS Base Score sub-metrics are supposed to be analyzed network and mission agnostic for the vulnerability in question such that the metrics would then be static for any customer using a device that would be vulnerable. Only the Modified Base Score would be updated for a new customer to reduce duplicate effort. This assessment analyzes each device with its prospective mission and environment in the Base Score, such that no new information would be gleaned in the

Modified Base Score. For UAVs specifically, the mission and environment are necessary to risk assessments [11] and are not viable without them. Removing the Modified Base Score sub-metrics from the scoring system is simple as the CVSS default is to use the original Base Score sub-metrics. In the future, should a risk assessment of an UAV be beneficial separate from mission and environment, this assessment can be simply reverted by re-adding the Modified Base Score sub-metrics in the Environmental equations instead of the Base sub-metrics. The Modified sub-metrics are the same levels and definitions, instead modified for an organization's specific use.

3.3 Scoring System

The risk scoring system is designed to take each of the metrics defined in Section 3.2 and to calculate an overall risk score. For ease of use, the score is limited to values between 0.0 and 10.0 in increments of tenths, which directly corresponds to 101 possible risk states. The values of sub-metrics are derived from the open-source values of CVSS, which is to leverage the long-term value of testing and refining that CVSS placed into their vulnerability severity assessment. Due to the design of each of this framework's sub-metrics in line with CVSS's sub-metrics, the values of severity should be close and directly related to values of risk. The equations are borrowed from CVSS due to the direct connection between their assessment and this assessment.

3.3.1 Base Score

The Base Score is calculated first using the first eight sub-metrics that all revolve around device design and securities. This score is not necessarily accurate for any future assessment or for a different customer since the use cases, configurations, and payloads are considered. Each of the sub-metrics in the Base Score have a constant value assigned based on the value determined, as shown in Table 17. Each sub-metric

is seen to be ranked from value correlated to highest risk to lowest risk, though each sub-metric is not valued completely equal.

Table 17. Base Sub-Metric Values.

Attack Vector	Direct	0.85
	Grnd Controller	0.62
	Air-Gapped	0.55
	None	0.2
Device Modification	Low	0.77
	High	0.44
Privileges Required	None	0.85
	Low	0.62 (0.68 if Scope Changed)
	High	0.27 (0.50 if Scope Changed)
User Interaction	None	0.85
	Required	0.62
Confidentiality, Integrity, Availability Impact	None	0.56
	Low	0.22
	High	0

Using the Base Score values of Table 17, the Base Score is then calculated using Algorithm 1. The sub-metric variables were assigned in Section 3.2 within the definitions of each sub-metric. As intermediaries, Impact Sub-Score (ISS) is calculated from the Impact sub-metrics and Exploitability is calculated from four related sub-metrics. Scope lastly is used as a modifier to both intermediaries using factors determined by CVSS. These constants, along with the chosen values of each sub-metric, result in a minimum 0.0 and maximum 10.0 value. The influence of each metric has been balanced over time and testing by CVSS for their vulnerabilities and directly relate to this framework's risk metrics.

3.3.2 Temporal Score

The Temporal Score is calculated next after the Base Score using the three associated sub-metrics. The Temporal Score is the new score for the device as the Base Score of risk is potentially reduced by factors relating to time. Each sub-metric value

Algorithm 1 Base Score Calculation

$ISS = 1 - [(1 - C) * (1 - I) * (1 - A)]$
if $S = Unchanged$ **then**
  $Impact = 6.42 * ISS$
else
  $Impact = 7.52 * (ISS - 0.29) - 3.25 * (ISS - 0.02)^{15}$
end if
$Exploitability = 8.22 * AV * DM * PR * UI$
if $Impact <= 0$ **then**
  $BaseScore = 0$
else
  if $S = Unchanged$ **then**
    $BaseScore = Roundup(Min[Impact + Exploitability), 10])$
  else
    $BaseScore = Roundup(Min[1.08 * (Impact + Exploitability), 10])$
  end if
end if

determined earlier is assigned a constant related to their associated risk value. As seen in Table 18, the highest risk values correspond to a value of 1, which means that the Base Score is not reduced in any manner due to factors of risk associated with time. This highest value could be considered the default as it assumes the worst case temporal state for each sub-metric and does not have an effect on the Base Score. The Temporal sub-metric values are directly borrowed from CVSS and the connection between temporal factors with vulnerability severity and risk have been shown.

Table 18. Temporal Sub-Metric Values.

Market	High	1
	Medium	0.97
	Low	0.94
	None	0.91
Vendor Support	Unavailable	1
	Low	0.97
	Medium	0.96
	High	0.95
Report Confidence	High	1
	Normal	0.96
	Low	0.92

The calculation of the Temporal Score is shown in Algorithm 2. As each sub-metric value is a percent of the risk that is still valid, simple multiplication of each sub-metric with the original Base Score results in the new Temporal Score.

Algorithm 2 Temporal Score Equation.

$$TemporalScore = Roundup(BaseScore * M * VS * L)$$

3.3.3 Environmental Score

The Environmental Score uses the assessed sub-metrics in relation to requirements of the device in its required or proposed mission sets. Constants are assigned to each level as shown in Table 19. A Medium value could be understood as the default as the constant assigned would have no effect on the Temporal Score for that sub-metric.

Table 19. Environmental Sub-metric Values.

Confidentiality Requirement &	High	1.5
Integrity Requirement &	Medium	1.0
Availability Requirement	Low	0.5

Progressing from the Temporal Score, the process to determine the Environmental Score is shown in Algorithm 3. The two intermediaries, similar to the Base Score algorithm, are Modified Impact Sub-Score (MISS), Modified Impact, and Modified Exploitability. The "Modified" terminology is used to separate these terms from the Base Score and do not use actual modified values like CVSS as explained earlier in the chapter. The MISS is a modification of the ISS by varying the sub-metrics of Confidentiality, Integrity, and Availability Impact by the associated Environmental sub-metrics. Scope again is used as a modifier to the MISS as determined by CVSS. Modified Exploitability is the same as Exploitability intermediary, but simply used in separate equations. The Environmental Score is then calculated using the sub-metrics of the Temporal Score and Base Metrics, with a maximum cap of 10.0 score.

Algorithm 3 Environment Modification Equations

$//EnvironmentalScore \leftarrow$ {C,I,A Requirements , Modified Base Metrics}
$MISS = Min\{1 - [(1 - CR * C) * (1 - IR * I) * (1 - AR * A)], 0.915\}$
if $S = Unchanged$ **then**
$ModifiedImpact = 6.42 * MISS$
else
$ModifiedImpact = 7.52 * (MISS - 0.029) - 3.25 * (MISS * 0.9731 - 0.02)^{13}$
end if

$ModifiedExploitability = 8.22 * AV * DM * PR * UI$

if $ModifiedImpact <= 0$ **then**
$EnvironmentalScore = 0$
else
if $S = Unchanged$ **then**
$EnvironmentalScore = Roundup(Roundup[Min([ModifiedImpact + ModifiedExploitability], 10)] * M * VS * L)$
else
$EnvironmentalScore = Roundup(Roundup[Min(1.08 * ModifiedImpact + ModifiedExploitability), 10)] * E * RL * RC)$
end if
end if

3.3.4 Final Score

The final score used to define the overall cyber risk of the small UAV in regards to the device, timing, and mission-environment is the Environmental score that was described last in the previous section. This score will only range from 0.0 to 10.0, though this is due to some amount of capping at either end. Rounding up to the nearest tenth allows for ease of use and a significant number of possible values. Both of these assertions will be analyzed in Chapter 4 through the use of case studies.

A new score would need to be calculated if any of the sub-metrics were to change, which covers UAV model changes, configuration changes to applicable software or hardware, changes over time, and changes to the mission set. By attempting to make the qualitative sub-metrics as quick and easy as possible to assess, re-calculations for

different potential acquisitions is expected. By calculating for each potential scenario, the customer is able to make the most informed risk decision in selecting a new small UAV.

IV. Case Studies and Analysis

4.1 Case Study Build and Scoring

To demonstrate and analyze this risk assessment methodology, five models of UAVs were evaluated across three major mission-environment scenarios plus one additional as the worst case. By scoring across the total of 16 case studies, the objectives of breadth and variability, general applicability, and ease of use should be made evident for the scoring system presented in the Chapter 3. To accomplish this, each model was first defined with specifications relevant to the scoring system, then each mission-environment was defined and scored based upon each model. Minor changes to mission-environments were adjusted subsequently and scored under each sub-section.

4.1.1 Small UAV Models

Model 1: The first model to be used in this case study is one of the highest rated consumer UAVs currently on the market: the Chinese-made DJI Mavic 2 Pro. The Mavic 2 Pro was released in mid-2018 and rivaled the best of its competitors for "camera performance, video transmission, fight time, flight speed, less noise, omnidirectional obstacle sensing, intelligent flight modes and its unique Hyperlapse feature" [54]. The Mavic 2 Pro quad-rotor has a maximum flight time of 31 minutes, maximum speed of 45 mph, and hover at windspeeds up to 25 mph, all while being sold for under $2,000 [54]. The Mavic 2 Pro is controlled via the DJI GO 4 app from a user's phone connected to a DJI controller, which sends commands and receives data over Wi-Fi protocol standards and both frequencies by default [55]. The DJI brand is well-known for their autopilot obstacle avoidance of which the Mavic 2 boasts 360 degree vision. The user is always in control of the UAV per FAA regulations, and the

Mavic 2 Pro features multiple control failure protocols such as returning to a home waypoint. DJI is known as a brand for their closed systems and protocols with the data being encrypted with AES-256 standard [55]. DJI is plagued by rumors of supply chain vulnerabilities with DHS Cybersecurity and Infrastructure Security Agency (CISA) placing the company on an industry alert [56]. While DJI has officially denied all allegations to the U.S. Senate sub-committee on Security, some industries are taking precautions with acquiring new UAVs from this manufacturer [56].

Model 2: The second model to be used for case studies in this paper is the well-publicized U.S.-made Falcon 8+, of which the Shooting Star version is most known for its light displays at Disney Parks [57]. The Intel-produced Falcon 8+ model was released in 2015 and is meant for missions of mapping structures and terrain [57]. The Falcon 8+ is an octo-rotor design and boasts a maximum flight time of 26 minutes, maximum speed of 22 mph, and hover at windspeeds up to 27 mph [57]. Engineered specifically for Intel's waiver with the FAA to allow the Intel Cockpit to operate upwards of 1,500 UAVs at one time, the individual price tag of $30,000 is a bit misleading since they are contracted by mission and not purchased one-off [58]. The Falcon 8+ is controlled exclusively through the single Intel ground controller Cockpit, sending commands and receiving data through both Wi-Fi frequencies with manual control of a single device possible for emergencies [57]. The Falcon 8+ runs an open-source Linux OS, uses Wi-Fi encryption for data transmission, but does not use encryption for data at rest [57]. While operating multiple UAVs, all mission data is processed at Intel data centers since missions have reportedly generated over 18TB of data [58].

Model 3: The third model is the French-made Parrot Anafi, which represents the cheaper yet capable UAV models for comparison. Produced by Parrot who is known for the under $1,000 market, the Anafi ($600 currently in the U.S.) represents the

professional tier for Parrot while still being accessible by hobbyists. The Anafi is a quad-rotor model advertising 25 minutes of flight time, 33 mph maximum horizontal speed, and hover control up to 31 mph without wind [59]. Parrot utilizes a unique controller that the user's smartphone attaches into for navigation and the standard software build requires full control during missions with a few pre-programmable fail-safe controls [59]. The controller utilizes both Wi-Fi frequency standards for control and data, and features no security for data at rest or over the air. The smartphone app is the ground controller and, while usually connected to Parrot servers, can operate away from network [59].

Model 4: The fourth small UAV model is the Insitu ScanEagle 3, which represents a non-copter design (pusher motor) yet fits the requirements for these small UAV case study scenarios. This Boeing-owned sUAV is not International Traffic in Arms Regulations (ITAR) listed like its previous version ScanEagle 2 due to an unknown amount of change in design under "Unmanned aerial vehicles (UAVs) specially designed to incorporate a defense article" [60]. ITAR listing represents additional regulations placed by the U.S. to better control the sale of arms to friends and potential adversaries. None of these regulations specifically reduce cyber risk directly, though U.S. manufacturing and design may influence customer trust in the product [61]. The ScanEagle 3 is utilized here as a similar-to-ITARs small UAV and is common within the inventories of many nations' militaries, specifically coastal forces [60]. This vehicle is rated up to 20 hours flight endurance, 92 mph maximum speed, and recovery with crosswinds of up to 18 mph, all of this on top of a max payload weight of 20 lbs [60]. The ScanEagle 3 has the price tag to match at around $3.2 million for four vehicles and the related infrastructure to launch and recover [62]. The ScanEagle 3 contains the Athena 111m autopilot that is normally seen on larger runway restricted UAVs [63] and is capable of handling the pneumatic launching process [64]. The ground station

of the ScanEagle 3 is the Insitu's Common Open Mission Management Command and Control (ICOMC2) which is an open-architecture application with numerous plug-ins that can be loaded to nearly any laptop for control of multiple aerial vehicles while remote from online connection [65]. The ICOMC2 controller has significant fail-safe measures including real-time operational risk tracking amongst multiple aircraft and uses Joint Architecture for Unmanned Systems (JAUS) SAE AS-4 messaging protocol to provide additional availability and security over-the-air [65]. Made specifically for sensitive information collection, the ScanEagle 3 implements encryption both for data stored locally as well as control authorization [65].

Model 5: The fifth and last model used in this selection of case studies is a DIY small UAV utilizing the open-source software, closed-source hardware of a Pixhawk 4 autopilot from U.S. Holybro [66]. With a low capital threshold, DIY sUAV frames can be built from kits or even 3D printed, then mount the autopilot, sensors, controls, and power source. Due to the wide variations possible, the model used in this case study is theoretical except for the security features that apply to the risk assessment. This model will utilize a radio frequency standalone remote controller that directly controls the model. The Pixhawk 4 autopilot features pre-programmed fail-safe protocols that allow the aircraft to return to mission start coordinates [66]. All changes to configurations are done over the USB port via cable, from an air-gapped laptop that utilizes the ArduCopter software. This sUAV has additional software written to encrypt all stored data on board and password protected to stop unauthorized re-programming. Due to the home-made frame and ease of upgrading components, the life expectancy of this sUAV is less than the average sUAV.

4.1.2 Mission-Environment Scenarios

The three scenarios presented next represent a swath of the missions and environments that small UAVs may be found operating today. These scenarios are built to give the information required to complete the risk assessment while demonstrating the breadth of missions and environments that the assessment can cover. The last scenario, number four, is a worst case scenario where only the highest risk values for each sub-metric as chosen, which is used to show boundary conditions of this assessment methodology.

Mission 1: As the simplest of mission scenarios, an individual user purchases a single UAV for their agricultural business to monitor crops and livestock. Since video streaming is the only mission, the device bought will only be used in a standard out-of-the-box configuration. The terrain is almost completely flat with no buildings or very few trees within the operating area. The user plans to operate the UAV manually only to fly first-person video capture with no data storage. The user plans to utilize the aircraft for only a single season to test out its effectiveness. As an independent farmer, the user does not consider data captured to be confidential or sensitive. With full access to the area and a low operating ceiling, manual recovery after losing signal is easy. The user plans to utilize a tablet as the ground controller without access to the Internet while operating.

The sub-metrics shown in Table 20 show lowest risk in user mission requirements (Environmental) and standard device risk values across Base sub-metrics. Since the user in Scenario 1 does not have concerns for supply chain risk, the manufacturer is not a factor across Confidentiality, Integrity, or Availability Impact sub-metrics. The scores shown in Table 21 clearly separate the third model, the Anafi, from the rest for the lack of any security features, though it is the cheapest option for the mission. The rest of the final scores are close, with the first and fourth model having

the same lowest risk score. The sub-metrics for these two models is different only by the swapping the C and A sub-metric values.

Table 20. Mission-Environment 1 Sub-metric Values.

	Base							Temporal			Environmental		
	AV	DM	PR	UI	C	I	A	M	VS	L	CR	IR	AR
Mavic	0.55	0.77	0.27	0.62	0	0.22	0.22	1	0.95	0.92	0.5	0.5	0.5
Falcon 8+	0.55	0.77	0.62	0.62	0	0.22	0.22	0.97	0.95	0.92	0.5	0.5	0.5
Anafi	0.55	0.77	0.62	0.62	0.56	0.56	0.56	0.97	0.97	0.92	0.5	0.5	0.5
ScanEagle	0.55	0.77	0.27	0.62	0.22	0.22	0	1	0.95	0.92	0.5	0.5	0.5
Pixhawk	0.55	0.44	0.27	0.62	0.22	0.22	0.22	0.97	0.97	0.92	0.5	0.5	0.5

Table 21. Mission-Environment 1 Scoring.

	Base Score	Temporal Score	Final Score
Mavic	3.1	2.8	1.7
Falcon 8+	3.9	3.4	2.3
Anafi	7.3	6.4	4.7
ScanEagle	3.1	2.8	1.7
Pixhawk	3.8	3.3	2.0

Mission 2: The user organization is purchasing a fleet of UAVs for their delivery and distribution business. The devices will require modification in-house to allow the carrying and releasing of small packages. To meet regulations, each UAV will be controlled by individual ground controllers and the devices will not be networked to each other. The delivery area is a 10 minute radius around the distribution center or mobile host ground vehicle and the area is defined as a suburban home community with no nearby airports. The organization plans on utilizing these aircraft for three years, at which point they plan to purchase a new fleet. The flight data stored on each device is considered sensitive to the company due to research plans to expedite deliveries. The delivery area has many civilians and homes, so uncontrolled landings are highly dangerous. The ground controllers are computers that are networked directly to the Internet for data processing off-site.

Mission 2 sub-metrics are shown in Table 22 and reflect the increasing risk and

concern from the owning organization compared to Scenario 1. The Base sub-metrics differ first by the modification required to complete the mission and also by the organization's growing concern over the Chinese influence on the first model's supply chain, specifically to Confidentiality Impact, but not Availability since the organization does not plan for global use of this fleet. The Temporal sub-metrics again show the same Market and Vendor Support values seen in Scenario 1; however, the Lifespan value reflects the longer planned usage, though the fifth model (the DIY model) is known to be unable to fulfill the specified lifetime and would require earlier replacement. The final scores are shown in Table 23 with nearly all of the models reflecting the higher risk pairing any model to the mission and environment. The small increase with the first model, the DJI Mavic Pro 2, under the C sub-metric clearly removes the UAV from the lowest risk category that it was in for the previous scenario due to the increase in supply chain risk per the priorities of the commercial organization. Across all models due to the mission parameters, sub-metrics of Access Vectors, Lifespan, and Confidentiality / Integrity / Availability Requirements were all increased in risk tier. Device Modification was decreased for all but the DIY Pixhawk 4 in risk tier.

Table 22. Mission-Environment 2 Sub-metric Values.

	Base							Temporal			Environmental		
	AV	DM	PR	UI	C	I	A	M	VS	L	CR	IR	AR
Mavic	0.62	0.44	0.27	0.62	0.22	0.22	0.22	1	0.95	1	1.5	1	1.5
Falcon 8+	0.62	0.44	0.62	0.62	0	0.22	0.22	0.97	0.95	1	1.5	1	1.5
Anafi	0.62	0.44	0.62	0.62	0.56	0.56	0.56	0.97	0.97	1	1.5	1	1.5
ScanEagle	0.62	0.44	0.27	0.62	0.22	0.22	0	1	0.95	1	1.5	1	1.5
Pixhawk	0.55	0.44	0.27	0.62	0.22	0.22	0.22	0.97	0.97	0.92	1.5	1	1.5

Mission 3: This mission scenario is a North Atlantic Treaty Organization (NATO) military organization purchasing a fleet of UAVs to map and track potential enemy positions. The UAVs require a separately procured camera-sensor suite, though the software will remain standard. The fleet will be pre-programmed with mission data

Table 23. Mission-Environment 2 Scoring.

	Base Score	Temporal Score	Final Score
Mavic	3.8	3.7	4.4
Falcon 8+	3.4	3.2	3.7
Anafi	6.8	6.4	6.4
ScanEagle	2.9	2.8	3.3
Pixhawk	3.8	3.3	3.9

from a stand-alone ground controller and only interface with mission-partnered UAVs as a swarm, meaning the scope will change if one is compromised. The military organization plans a life cycle of two years for the fleet before replacing aircraft. Since all data captured is stored on the device until mission is complete, all mission data is extremely sensitive.

Mission 3 sub-metrics are shown in Table 24 and reflect the first of the scenarios where the Scope is Changed, meaning higher values for Privileges Required and different algorithm equations which results in overall higher risk scores. Additionally, the Chinese DJI model has significantly higher risk impact compared to the first scenario since a military organization other than China would be wary of its supply chain. The other manufacturers were not similarly adjusted, which would be reasonable to any NATO member. The Availability Requirement is set to the lowest risk value due to the open terrain and pre-programmed mission parameters, even though the mission is high-risk and the user is not immediately in the control loop. The final scores are shown in Table 25 with the second and fourth models (Intel and Insitu, respectively) vying for lowest scores. Due to the higher priority to the supply chain risk, the DJI model now has the same overall high risk score as the low security Anafi.

Worst Case: As the edge case to test the robustness of the scoring system, the worst case scenario sets each of the sub-metrics to the highest risk tier and numerical value. The sUAV here has direct logical connection to the Internet, has no modifications, no privileges required for access, is connected to other devices for attack,

Table 24. Mission-Environment 3 Sub-metric Values.

	Base							Temporal			Environmental		
	AV	DM	PR	UI	C	I	A	M	VS	L	CR	IR	AR
Mavic	0.2	0.44	0.5	0.85	0.56	0.22	0.56	1	0.95	0.96	1.5	1.5	0.5
Falcon 8+	0.2	0.44	0.68	0.85	0	0.22	0.22	0.97	0.95	0.96	1.5	1.5	0.5
Anafi	0.2	0.44	0.68	0.85	0.56	0.56	0.56	0.97	0.97	0.96	1.5	1.5	0.5
ScanEagle	0.2	0.44	0.5	0.85	0.22	0.22	0	1	0.95	0.96	1.5	1.5	0.5
Pixhawk	0.2	0.44	0.5	0.85	0.22	0.22	0.22	0.97	0.97	0.92	1.5	1.5	0.5

Table 25. Mission-Environment 3 Scoring.

	Base Score	Temporal Score	Final Score
Mavic	6.8	6.3	6.4
Falcon 8+	3.4	3.1	4.2
Anafi	7.0	6.4	6.4
ScanEagle	3.3	3.1	4.2
Pixhawk	6.1	5.3	4.9

and does not have a user in the loop. The sUAV has no confidentiality, integrity, or availability securities in place to temper the impact of a compromise. To be scored highest within the Temporal sub-metrics, the device is very common on the market, yet has no vendor or community support. For whatever mission this device should be used for, the device is expected to be in use in the current configuration for a long period of time (more than 2 years). Lastly to set the Environmental sub-metrics, the device's mission has a high confidentiality, integrity, and availability requirement. The values associated with such scoring are shown in Table 26 and the final scores are shown in Table 27. To be expressed at length in Section 4.2.2, the scores shown in Table 27 are capped by the CVSS algorithm at 10.0 and not naturally achieved.

Table 26. Worst Case Sub-metric Values.

	Base							Temporal			Environmental		
	AV	DM	PR	UI	C	I	A	M	VS	L	CR	IR	AR
Worst Case	0.85	0.77	0.85	0.85	0.56	0.56	0.56	1	1	1	1.5	1.5	1.5

Table 27. Worst Case Scoring.

	Base Score	Temporal Score	Final Score
Worst Case	10.0	10.0	10.0

4.2 Analysis

Below we discuss the presented implementation's benefits and challenges. The risk assessment tool is rated against the three objectives of Breadth and Variability, General Applicability, and Ease of Use. These are suggested by related research in cybersecurity risk assessments [50, 53]. The scope of this paper does not analyze the assessment against any live situations or historical information, which may provide additional and different insights for adjustments.

4.2.1 Benefits

The first observation of the case studies is the spread of scores based on the limited number of examples. Even with just 16 total example scenarios including the worst case, the scores cover 83% of the possible scores. A best case scenario was specifically excluded as one of the examples as it presents trivial information that can easily be achieved. A UAV with high securities within Confidentiality, Integrity, and Availability Impact sub-metrics will force the overall Base, Temporal, and Environmental Scores to 0.0 without variations. The objective of reaching breadth of the scoring range to allow for maximum variations of risk scores is therefore achieved. Across the three scenarios where risk to the buyer was increasing, the scores for almost all models increased as well. Additionally, between models, the DJI, Intel, and Insitu's models provided more security than the Parrot, which is factored into the cost of the UAV, and their scores were noticeably lower for the majority of missions. One exception to this was in Scenario 3 where the DJI's rumored supply chain risk is heavily factored for a non-Chinese military organization and that risk is shown by scores close to the

unsecured Anafi. Scenario 2 had a purchasing organization only slightly influenced by this possible risk, and the Mavic 2 Pro showed significantly better final scores compared to the Anafi. The objective of the risk assessment showing variability and general risk correlation is therefore achieved.

For General Applicability, the tool was successfully able to apply to all of the models and scenarios. This is in sharp contrast to the direct CVSS sub-metrics which has several that do not apply based on the scope of component versus system level view and assuming traditional network setup. The models included a pusher motor fixed wing sUAV with the ScanEagle 3, showing how the assessment is able to account for different designs. Many physical design features of aircraft may not affect the cyber risk; however, there are some correlations, such as with the additional weight allowable for a higher end autopilot.

The last proposed objective, Ease of Use, is a more subjective characteristic, but it is determined to be achieved in this risk assessment based on the required documentation to complete the scores in the case studies. For all five models presented, all of the sub-metrics were determined from the specification documentation that is published online and from other easily accessible advertisements. This means that nearly anyone, with the risk assessment's guide, could determine their organization's or their personal scores with some amount of accuracy. There is no in-depth cyber forensics or testing utilized for any of the sub-metrics, though research into vulnerabilities can still be taken into account, as seen with the supply chain risk of DJI.

4.2.2 Drawbacks & Challenges

The spread of scores is seen to be limited by CVSS's built-in caps to make sure that the scores do not go above 10.0, which it may in the worst case. Running the algorithm for the worst case found that a number of possible high ranged risk values

are lost, such as those to 10.8 for Base Score (if Scope Unchanged, then no values lost) and those to 10.9 on the Final Environmental Score. These caps result in lost variability between scores at the top end of the risk spectrum by setting them equal at the maximum 10.0 score. CVSS accepts this loss with the assumption that any risk framework utilizing their assessment will make strides to reduce and cover this glaring vulnerability to the network [4]. Working with system risk here, the same assumption can be made for this risk assessment that few systems will actually achieve an above maximum score and the users will put more effort to lower that score through security features or by choosing another available model so the maximum score will not persist long term.

Another drawback of this risk assessment through the case studies is the actual level of usability by potential users. By focusing on the acquisition phase, the level of cybersecurity knowledge is expected to be low, but the translation done by the assessment of cyber principles is expected to bridge that gap. To fully verify this objective, it may require human studies or live production level results, which are outside the scope of this paper. The analysis of documentation required for accessibility and legibility shows promise, but does not prove the objective.

4.2.3 Simulation Objectives

In light of the development and analysis of this cyber risk assessment, consideration is required for a next stage in development. One such avenue of interest is hardware-in-the-loop simulation. Simulations have been used for decades to allow for low cost testing in a sandbox environment to test the boundaries and flaws of software and hardware by inputting all controls and variables. Specifically with cyber-physical machines, providing as much of the hardware without significantly raising the cost of testing can allow for more accurate testing by using the real parts and illuminate pre-

viously unknown relations or interactions between the cyber and physical domains. Hardware-in-the-loop simulations have seen a surge in use within the SCADA and critical infrastructure domains where sensors and actuators have a higher ratio of the components in a system.

Based on this research, one of the main objectives of this style of simulation is to verify the configuration and protocols utilized by a small UAV. The cyber risk assessment proposed here makes the underlying assumption that the publicized specifications are accurate. While further research with this assessment can determine with historical data how accurate this assumption has been, new models would require operational testing to validate. Operational usage was one of the key avoidance goals within this assessment as it does not allow for pushing forward the cyber risk calculation into the life-cycle of the vehicle. By creating a hardware-in-the-loop simulation, this testing could be achieved much earlier in the cycle and provide confidence in the risk assessment's score and confidence to an organization of their overall mission's risk.

Other objectives for small UAV testing based on this research is to test unique configurations and protocols that are not utilized outside of the UAV domain. Small UAVs commonly use similar protocols, such as Wi-Fi and even to some extent the OSs, which come with more oversight from many research communities and interested parties. The more unique characteristics that should be tested for within a hardware-in-the-loop simulation for small UAVs are geo-fencing, cyber-physical fail-safes, and signal input / output. An unseen vulnerability of mobile devices including phones and UAVs is software that is triggered by GPS location data that changes the expected interactions with the device [67]. Within simulations, GPS spoofing is nearly a requirement and geo-fencing may be able to be discovered with fuzzing. This testing is of particular interest to organizations or nation-states where the supply chain is

less trustworthy and the device is expected to move through contested locations. For cyber-physical fail-safes, the hardware to software interactions for the boundaries of expected flight require additional testing that can not be determined within a software only simulation. While manufacturers tend to advertise featured fail-safes such as "Return Home" and "Controlled Descent" that are used in this risk assessment, the physical interactions with cyber components present some unknown results when outside the expected input. By adding in hardware to the simulation, these software fail-safes can be tested away from operational hazards. Lastly, closed-system signal analysis may provide an avenue to quantitative risk assessment and provide insight to vulnerabilities such as "Call Home" features. Since attackers require some access to a device to compromise a system, the signals to and from a UAV may provide some measure of the device's risk to hacking. While these measurements would give direct numerical information on the system that could be used for a quantitative scoring, the exact correlations to risk and how to measure risk outside of signals is currently unknown. "Call Home" features installed by manufacturers or attackers could be tested through simulation, though triggering these messages may be difficult, especially if the OS knows that it is in a simulation. Hardware-in-the-loop may provide that extra stimulus to trick the software in to sending out information that could be collected and tracked during simulation.

V. Conclusion

5.1 Summary

This chapter summarizes the work performed for this research including the design and development of the new cyber risk assessment for small UAVs. Each objective introduced in Section 1.3 is restated before a summary of how this research successfully reached that objective. Lastly, recommendations and lessons learned for future work with the risk assessment and other cyber security topics with small UAVs are discussed.

5.2 Research Contributions

Assess whether any cyber or physical risk assessments of similar domains accurately quantify the cyber risk of small UAVs. This research is focused on the assessment of the cyber security state of a small UAV through the use of a tool to quantify the risk. No official or formal cyber risk assessments for small UAVs were discovered in this research, though some proposals have been made in academia [53]. Since Hartmann and Steup's research failed to reach their own objectives [11], risk assessments in related domains were also analyzed for viability to adaptation to small UAVs. While URAF provided operational risk assessment and CVSS scored cyber vulnerability severity, no individual assessment analyzed could be directly utilized to score cyber risk.

Define a new small UAV cyber risk assessment tool (if none exists). Due to the success and close proximity of FIRST's CVSS tool, their model was used as the foundation of the new proposed cyber risk assessment. Using qualitative security questions that could be determined without operational testing and expert knowledge of individual vehicles, the new assessment determined 14 sub-metrics and calculated

a final score for the UAV specific to the planned operational mission and environment. By scoring all scenarios from 0.0 to 10.0, the final score allowed for ease of interpretation of the score in relation to similar vehicles or changes in the vehicle's configuration or other variables.

Determine the objectives of success a small UAV cyber risk assessment should meet, based on similar domain assessments. By the fact that a cyber risk score could be calculated from the publicly released specifications and desired mission requirements, the ease-of-use objective was met by this tool without use of a device specific expert. The ease-of-use objective allows for the cyber risk assessment to be used as early as possible in the life-cycle of the vehicle and would allow a customer's risk framework to make informed decisions about acquisitions of a new vehicle or fleet.

The granularity of the risk assessment tool was analyzed by the characteristics of its breadth and variability through the case studies. While the algorithms and possible numerical values of the tool do require capping at both extremes, the amount of lost potential scores was found to be insignificant, especially in light of the meaning of such scores to any risk framework. The rounding up to the nearest tenth of each score and the final score was demonstrated to provide significant numbers of unique scores across all case studies and almost all unique scores per scenario. This variability allows for informed comparison between similar vehicles for the same mission-environment scenario or any other change in variable.

Through all of the case studies, the cyber risk assessment met general applicability to all models and scenarios. Small yet significant security changes to the case studies resulted in some related change in the resulting risk score. Qualitatively, the tool captures the unique configurations and uses of small UAVs across infrastructures and industries which increases the tool's viability to nearly any UAV customer. These

models were analyzed with several mission-environment scenarios that provided the rest of the required variables to calculate the risk scores. These scenarios meet the objective missed by Hartmann and Steup that any cyber risk assessment of UAVs must include the terrain and mission set of the vehicle [11].

Stine's cyber risk assessment objectives were all found to be useful and good measure of the tool [50]. While slightly adapted for usability by non-cybersecurity professionals, Stine's Ease-of-Use, Low Cost, and Easily Understood Results were utilized successfully in this research named as Ease of Use, General Applicability, and Breadth and Variability, respectively. Stine's healthcare focus was not entirely dissimilar to small UAVs due the embedded nature of its electronics, breadth of devices / modifications, and the trusted yet mobile nature of the scored devices. In comparison, Hartmann and Steup provide no objectives of measure for their scheme, though they discussed important details to be included in a UAV cyber risk assessment [53].

Establish the objectives a hardware-in-the-loop simulation of a small UAV should meet to best bring to light potential vulnerabilities. The overall objective for a simulation of a small UAV being tested for cyber insecurities is to verify that configurations and protocols meet manufacturer specifications. This objective is important in light of trust issues in the supply chain related to nation-state tensions between the number one small UAV manufacturer, the Chinese DJI, and the rest of the world. With specifications verified, only device specific protocols would need to be further researched through simulation for vulnerability due to the wide research of vulnerabilities on common configurations and protocols, such as Wi-Fi or the OS. Other objectives to verify through simulation include the following: GPS spoofing to actively fuzz the OS for fencing, physical maneuvering for cyber fail-safe protocols, and signal input / output for verification of signal generation in

light of "phone home" code.

5.3 Future Work

Given the importance of the work presented and continuous technology developments in small UAV cyber security and risk assessment, there are many areas that could be further explored, matured, or developed. Listed below are topics of interest that would expand the scope of this research:

- **Ease of Use Study:** The analysis presented in this research on ease of use of the tool is based on the availability of required specifications and requires data points into the human factor. A study into the knowledge standard of acquisition personnel of small UAVs would provide basis and conducting trials of these members using the tool with analysis of accuracy to risk would provide support to the claim of ease of use.

- **Expansion of Data:** This research presented five different models with a significant range of features and cost that may be weighed in consideration by a customer. Since the UAV market has many more options even within the single manufacturer DJI, future research would need to include more models to verify the uniqueness of risk scores to aid risk framework decision points.

- **Feedback of Data:** The true measure of validity for a cyber risk framework is its ability to predict attacks over time, in the face of prior historical data being a poor indicator of future cyber events [38]. The CVSS algorithms have been updated over time for IT systems based on seen changes for a shorter term prediction of severity [4]. To build resiliency similarly to CVSS, this tool calculates risk based on security principles that evolve at a slower pace but are correlated to fewer attacks [4]. Future work will be required to update the

weighting of sub-metrics and numerical values to continue to best calculate risk.

- **Hardware-in-the-Loop Simulation:** One avenue of extension to this research would be to create a simulation of current small UAV models to run against mission sets to evaluate the specifications to the risk. Due to the cyber-physical characteristics of UAVs, hardware would be required in the loop to best simulate the responses to stimulus. The first advantage to doing this simulation would be to verify the risks to certain specifications within this research other than through logic or operational testing. The second advantage would be to validate manufacturer specifications of hardware and software to their publicized specifications, especially when supply chain trust has been compromised.

- **Fully Quantitative Assessment:** The risk assessment proposed in this research places numerical values to qualitative characteristics, which naturally introduces variations based on perceived value. A quantitative measure of UAV characteristics would remove this bias and variation, though the exact characteristics to measure is still unknown. One method proposed and showing promise is through the collection of input / output signals to the system through which an attacker in limited. This method assumes a safe state prior to use, no inclusion of the ground controller and other connected vehicles to the closed system, and nearly none of the operational factors of importance to the URAF.

5.4 Final Words

This work demonstrated a viable new process to calculate the cyber risk of a small UAV. The cyber security of these airframes will need to continue to increase in proportion with the fielding of new fleets across military, commercial, and individual inventories. There has been found to be a gap in the current state of cyber security for

these devices, though cyber risk frameworks have been implemented amongst nearly all organizations today. The operational risk is covered well by the FAA's URAF, though cyber risks and the unique characteristics of small UAVs are excluded. Built from the well-respected CVSS model, this proposed new assessment will require tuning to better score risk and recognition by major organizations to hold any significance to individuals. Improvements to operational fleets' security will be realized when operational and cyber threats are accurately recognized and weighed. Since the manufacturers of small UAVs have not responded to this need, consumers must take appropriate actions including assessing the risk of their own fleets to protect their most valuable assets.

Bibliography

1. J. J. Winnefeld and F. Kendall, in *Unmanned Systems Integrated Roadmap: Fy2013-2038*. Collingdale, PA: DIANE Publishing Company, 2014.

2. R. Bojanc and B. Jerman-Blažič, "A Quantitative Model for Information-Security Risk Management," *EMJ - Engineering Management Journal*, vol. 25, pp. 25–37, 2013.

3. N. I. of Standards and Technology. (2016) Risk management framework: Quick start guides. Accessed September 2019. [Online]. Available: csrc.nist.gov/Projects/Risk-Management/Risk-Management-Framework-Quick-Start-Guides

4. FiRST. (2015) Common Vulnerability Scoring System V3. [Online]. Available: www.first.org/cvss/cvss-v30-specification-v1.8.pdf

5. P. Kopardekar, "(12) Patent Application Publication (10) Pub. No.: US 2016/0275801 A1," pp. 1–47, 2016.

6. National Highway Traffic Safety Administration. (2017) Purchasing with Safety in Mind: What to look for when buying a vehicle. [Online]. Available: www.NHTSA.gov/ratings.

7. P. G. Fahlstrom and T. J. Gleason, "History and overview," in *Introduction to UAV Systems*, 4th ed. West Sussex, United Kingdom: John Wiley Sons, Ltd, 2012, pp. 3–31.

8. T. J. Allen, "Design and Test of a UAV Swarm Architecture over a Mesh Ad-hoc Network," *Air Force Institute of Technology Thesis and Dissertations*, 2018.

9. J. Gray, "Design and Implementation of a Unified Command and Control Architecture for multiple Cooperative Command Unmanned Vehicles Utilizing Commercial-Off-The-Shelf Components, Thesis," *Air Force Institute of Technology Thesis and Dissertation*, pp. 1–159, 2015.

10. S. Kim, "Unmanned Aerial Vehicle (UAV) Operators' Workload Reduction: The Effect of 3D Audio on Operators' Workload and Performance during Multi-Aircraft Control," *Air Force Institute of Technology Thesis and Dissertation*, 2016.

11. K. Hartmann and K. Giles, "Uav exploitation: A new domain for cyber power," *International Conference on Cyber Conflict, CYCON*, vol. August, pp. 205–221, 2016.

12. M. Yampolskiy, P. Horvath, X. Koutsoukos, Y. Xue, and J. Sztipanovits, "Systematic analysis of cyber-attacks on cps-evaluating applicability of dfd-based approach," *Proceedings - 2012 5th International Symposium on Resilient Control Systems, ISRCS 2012*, pp. 55–62, 2012.

13. L. Kohnfelder and P. Garg, "The threats to our products," *Microsoft Blogs*, 2009. [Online]. Available: adam.shostack.org/microsoft/The-Threats-To-Our-Products

14. A. Kerns, D. Shepard, J. Bhatti, and T. Humphreys, "Unmanned Aircraft Capture and Control Via GPS Spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014.

15. D. P. Shepard, J. A. Bhatti, T. E. Humphreys, and A. A. Fansler, "Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks," *Ion Gnss 2012*, pp. 3591–3605, 2012.

16. A. Kim, B. Wampler, J. Goppert, I. Hwang, and H. Aldridge, "Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles," *Infotech at Aerospace 2012*, pp. 1–30, 2012.

17. H. Sedjelmaci, S. M. Senouci, and M. A. Messous, "How to Detect Cyber-attacks in Unmanned Aerial Vehicles Network?" *2016 IEEE Global Communications Conference, GLOBECOM 2016 Proceedings*, 2016.

18. T. Vuong, A. Filippoupolitis, G. Loukas, and D. Gan, "Physical Indicators of Cyber Attacks against a Rescue Robot," *2014 IEEE International Conference on Pervasive Computing and Communication Workshops*, pp. 338–343, 2014.

19. D. R. Kuhn, V. Hu, W. T. Polk, and S.-J. Chang, *NIST SP 800-32: Introduction to Public Key Technology and the Federal PKI Infrastructure.* National Institute of Standards and Technology, 2001.

20. F. Swiderski and W. Snyder, *Threat Modeling.* Microsoft Press, 2004.

21. N. Bar-Yosef. (2012) Examining threats facing public key infrastructure (pki) and secure socket layer (ssl). Accessed January 2020. [Online]. Available: securityweek.com/examining-threats-facing-public-key-infrastructure-pki-and-secure-socket-layer-ssl

22. T. Reed, J. Geis, and S. Dietrich, "SkyNET: a 3G-enabled Mobile Attack Drone and Stealth Botmaster," *Proceedings of the 5th USENIX conference on Offensive Technologies (WOOT11)*, pp. 1–4, 2011.

23. C. Gudla, S. Rana, and A. H. Sung, "Defense Techniques Against Cyber Attacks on Unmanned Aerial Vehicles," *International Conference of Embedded Systems, Cyber-physical Systems, Applications*, 2018.

24. S. Kriaa, M. Bouissou, and L. Pièvre-Cambacédès, "Modeling the Stuxnet attack with BDMP: Towards more formal risk assessments," in *7th International Conference on Risks and Security of Internet and Systems, CRiSIS 2012*, 2012.

25. K. Soo Hoo, "How much is enough? a risk-management approach to computer security," *Consortium for Research on Information Security and Policy (CRISP)*, 2000.

26. A. Pendleton, R. Dill, and D. Pettit, "Surveying the incorporation of iot devices into cybersecurity risk management frameworks," *SECUREWARE 2019 Proceedings*, 2019.

27. J. Rios, D. Mulfinger, and J. Homola, "NASA UAS Traffic Management National Campaign," *2016 IEEE/AIAA 35th Digital Avionics Systems Conference (DASC)*, pp. 1–6, 2016.

28. P. Kopardekar, "Enabling Civilian Low-Altitude Airspace and Unmanned Aerial System (UAS) Operations by Unmanned Aerial System Traffic Management (UTM)," *AUVSI Unmanned Systems 2014*, vol. 2, pp. 1678–1683, 2014.

29. L. Barr, R. Newman, E. Ancil, C. Belcastro, J. Foster, J. Evans, and D. Klyde, "Preliminary Risk Assessment Model for Small Unmanned Aerial Systems," in *17th AIAA Aviation Technology, Integration, and Operations Conference*, 2017.

30. E. Ancel, F. M. Capristan, J. V. Foster, and R. C. Condottax, "Real-time Risk Assessment Framework for Unmanned Aircraft System (UAS) Traffic Management (UTM)," *17th AIAA Aviation Technology, Integration, and Operations Conference, 2017*, pp. 1–17, 2017.

31. D. Diessner, H. Wynsma, L. Riegle, and P. Morrissey, "Civil aviation cybersecurity industry assessment recommendations, august 2019," *Aerospace Industries Association Civil Aviation Council*, pp. 1–36, 2019.

32. D. of Homeland Security Integrated Task Force, "Executive order 13636: Improving critical infrastructure cybersecurity department of homeland security integrated task force incentives study analytic report," pp. 1–69, 2013.

33. B. Brown. (2014) The ever-evolving nature of cyber coverage. Accessed: 2019-05-15. [Online]. Available: www.insurancejournal.com/magazines/mag-features/2014/09/22/340633

34. C. Stanley, "Cyber market estimate," 2017, interview: 2017-06-26.

35. L. Graham. (2017) Cybercrime costs the global economy $450 billion: Ceo. Accessed: 2019-05-14. [Online]. Available: www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo

36. InsuranceJournal.com. (2017) Cyber insurance premium volume grew 35% to $1.3 billion in 2016. Accessed: 2019-05-20. [Online]. Available: www.insurancejournal.com/news/national/2017/06/23/455508

37. J. Yin. (2015) Cyber insurance: Why is the market still largely untapped? Accessed: 2019-05-23. [Online]. Available: www.aei.org/publication/cyber-insurance-why-is-the-market-still-largely-untapped

38. S. Shetty, M. McShane, L. Zhang, J. P. Kesan, C. A. Kamhoua, K. Kwiat, and L. L. Njilla, "Reducing Informational Disadvantages to Improve Cyber Risk Management," *Geneva Papers on Risk and Insurance: Issues and Practice*, 2018.

39. J. Bolot and M. Lelarge, "Cyber Insurance as an Incentive for Internet Security," Tech. Rep.

40. A. Panou, C. Xenakis, and C. Ntantogian, "RiSKi: A Framework for Modeling Cyber Threats to Estimate Risk for Data Breach Insurance."

41. R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Computing Surveys*, vol. 46, no. 4, pp. 1–29, 2014.

42. A. J. Chaves, "Increasing Cyber Resiliency of Industrial Control Systems," *Thesis and Dissertations*, vol. 1563, 2017.

43. A. Matrosov, E. Rodionov, D. Harley, and J. Malcho, "Stuxnet under the microscope," *ESET*, 2010.

44. NIST, "Framework for improving critical infrastructure cybersecurity," *NIST Publications*, vol. 1, no. 1, pp. 1–48, 2018.

45. K. Huang, C. Zhou, Y. C. Tian, S. Yang, and Y. Qin, "Assessing the physical impact of cyberattacks on industrial cyber-physical systems," *IEEE Transactions on Industrial Electronics*, vol. 65, pp. 8153–8162, 2018.

46. Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber security risk assessment methods for scada systems," *Computers & security*, vol. 56, pp. 1–27, 2016.

47. J. Shin, H. Son, and G. Heo, "Cyber Security Risk Evaluation of a Nuclear I&C Using BN and ET," *Nuclear Engineering and Technology*, vol. 49, no. 3, pp. 517–524, 2017.

48. S. Haque, M. Keffeler, and T. Atkison, "An Evolutionary Approach of Attack Graphs and Attack Trees: A Survey of Attack Modeling," in *International Conference on Security and Management*, 2017, pp. 224–229.

49. K. Scarfone and P. Mell, "An analysis of CVSS version 2 vulnerability scoring," *2009 3rd International Symposium on Empirical Software Engineering and Measurement, ESEM 2009*, pp. 516–525, 2009.

50. I. Stine, "A cyber risk scoring system for medical devices," *Air Force Institute of Technology Thesis and Dissertations*, 2017.

51. DimensionalResearch, "Trends in security framework adoption: A survey of IT and security professionals," 2016. [Online]. Available: static.tenable.com/marketing/tenable-csf-report.pdf

52. M. Assante and R. Lee, "The industrial control system cyber kill chain," *SANS Institute InfoSec Reading Room*, 2015. [Online]. Available: www.sans.org/reading-room/whitepapers/ics/industrial-control-system-cyber-kill-chain-36297

53. K. Hartmann and C. Steup, "The vulnerability of UAVs to cyber attacks - an approach to the risk assessment," *International Conference on Cyber Conflict, CYCON*, 2013.

54. F. Corrigan. (2019) DJI Mavic 2 pro and zoom review includes features, specs with FAQs. Accessed November 2019. [Online]. Available: www.dronezon.com/drone-reviews/dji-mavic-2-pro-zoom-review-of-features-specifications-with-faqs/

55. DJI. (2019) Mavic 2 pro/zoom user guide, v2.0, 2019.04. Accessed November 2019. [Online]. Available: dl.djicdn.com/downloads/Mavic_2/Mavic_2_Pro_Zoom_User_Manual_V2.0_en.pdf

56. D. Sullivan. (2019) Drone security: Enhancing innovation and mitigating supply chain risks. Accessed December 2019. [Online]. Available: commerce.senate.gov/2019/6/drone-security-enhancing-innovation-and-mitigating-supply-chain-risks

57. Intel. (2015) Falcon 8+ system. Accessed November 2019. [Online]. Available: www.intel.com/content/www/us/en/products/drones/falcon-8

58. J. Feist. (2018) Intel's drone business explained – falcon 8+, shooting star and insight. Accessed November 2019. [Online]. Available: dronerush.com/intel-drone-business-12568/

59. Parrot. (2018) Anafi. Accessed November 2019. [Online]. Available: www.parrot.com/global/drones/anafi

60. G. Corfield. (2018) Eye in the sea skies: Insitu flies scaneagle 3 uav in first public demo. Accessed January 2020. [Online]. Available: theregister.co.uk/2018/05/18/insitu_scaneagle_3_first_public_demo

61. "1993 cfr title 22, chapter 1, subchapter m, part 121 - the united states munitions list," *Electronic Code of Federal Regulations*, 2020. [Online]. Available: ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=70e390c181ea17f847fa696c47e3140a&mc=true&r=PART&n=pt22.1.121

62. AFSOC. (2011) Scan eagle. Accessed January 2020. [Online]. Available: web.archive.org/web/20130710112005/http://www.af.mil/information/factsheets/factsheet.asp?id=10468

63. M. Golden. (2018) Insitu debuts scaneagle3 unmanned aerial system at xponential 2018. Accessed January 2020. [Online]. Available: insitu.com/press-releases/Insitu-Debuts-ScanEagle3-Unmanned-Aerial-System-at-Xponential2018

64. RockwellCollins. (2017) Athena 111m. Accessed January 2020. [Online]. Available: rockwellcollins.com/-/media/files/unsecure/products/product-brochures/controls/flight-controls/athena-111m/athena-111m-data-sheet

65. Insitu. (2020) Insitu's common open mission management command and control (icomc2). Accessed January 2020. [Online]. Available: insitu.com/information-delivery/command-and-control/icomc2

66. PX4_Dev_Team. (2019) Px4 v1.9.0 user guide. Accessed January 2020. [Online]. Available: docs.px4.io/v1.9.0/en/flight_controller/pixhawk4

67. E. Hermand, T. W. Nguyen, M. Hosseinzadeh, and E. Garone, "Constrained control of UAVs in geofencing applications," in *2018 26th Mediterranean Conference on Control and Automation (MED)*. IEEE, 2018, pp. 217–222.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From — To)*
26–03–2020	Master's Thesis	May 2018 — Mar 2020

4. TITLE AND SUBTITLE

Cyber Risk Assessment and Scoring Model for Small Unmanned Aerial Vehicles

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Pettit, Dillon M., Capt, USAF

5d. PROJECT NUMBER

20G327

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology
Graduate School of Engineering an Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT-ENG-MS-20-M-055

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory
2241 Avionics Circle
WPAFB OH 45433-7765
Attn: Steven Stokes
COMM 937-528-8035
Email: steven.stokes@us.af.mil

10. SPONSOR/MONITOR'S ACRONYM(S)

AFRL/RYWA

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

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A:
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Small Unmanned Aerial Vehicles (UAVs) present small radar cross sections, low heat signatures, and carry a variety of sensors and payloads. As with many new technologies, security seems secondary. Research indicates a growth in vulnerabilities applicable to small UAV systems, from individual UAV guidance and autopilot controls to the mobile ground station devices. Even if developers strive to improve the security of small UAVs, consumers are left without meaningful insight into the hardware and software protections installed when buying these systems. To date, there is no marketed or accredited risk index for small UAVs. Building from similar domains of aircraft operation and information technologies, a cyber risk assessment methodology tailored for small UAVs is proposed and presented in this research. Through case studies of popular models and mission-environment scenarios, the assessment is shown to meet the three objectives of ease-of-use, breadth, and readability. By allowing a cyber risk assessment before acquisition, organizations will be able to accurately compare and choose the best aircraft for their mission.

15. SUBJECT TERMS

Quantitative Assessment, Risk, Small UAV, Cybersecurity, Cyber-Physical

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Scott Graham, AFIT/ENG
U	U	U	UU	98	19b. TELEPHONE NUMBER *(include area code)* (937) 255-6565 x4581; scott.graham@afit.edu