Searching for Stars
Analyzing and Defining UAV Cyber Risk Assessments

Dillon Pettit
Graduate Cyber Operations
Air Force Institute of Technology
Dayton, Ohio, USA
Email: Dillon.Pettit@afit.edu

Scott Graham
Dept of Computer Engineering
Air Force Institute of Technology
Dayton, Ohio, USA
Email: Scott.Graham@afit.edu

Patrick Sweeney
Dept of Computer Engineering
Air Force Institute of Technology
Dayton, Ohio, USA
Email: Patrick.Sweeney@afit.edu

***Abstract*—The small Unmanned Aerial Vehicle market, commonly called UAVs, has grown immensely in popularity in hobbyist and military inventories. The same core mission set from the hobbyists directly relates to modern global military strategy, with priority on short range, low cost, real time aerial imaging and limited modular payloads. These small devices have the added benefits of small cross sections, low heat signatures, and a variety of transmitters to send real-time data over short distances. As with many new technologies, security seems secondary to the goal of reaching the market as soon as viable. Research indicates a growth in exploits and vulnerabilities, from individual UAV guidance and autopilot controls to the mobile ground station devices that may be as simple as a cellphone application. Even if developers heed calls to improve the security of small UAVs to protect them, consumers are left without meaningful insight into the protections installed when buying new or used UAVs. To date, there is no marketed or accredited risk index for small UAVs, but similar realms of traditional Aircraft operation, Information Technologies, Cyber-Physical Systems, and Cyber Insurance give insight to significant factors required for future small UAV risk assessment. In this research, four fields of risk frameworks are analyzed to determine their applicability to UAV security risk and key components that must be analyzed by a formal UAV framework. This analysis demonstrates that no adjoining field's framework can be directly applied without significant loss of fidelity and that further research is required to score the cyber risks of UAVs, along with potential objectives and avenues for then creation of a new framework.**

***Keywords*—Cyber-physical; Cybersecurity; COTS; Quantitative assessment; Risk; UAV.**

I. Introduction

Cybersecurity is the Herculean task to prevent all adversarial attacks over Information Technology (IT) devices with the potential to release information or control deemed valuable to an organization or individual. As computing devices have increased in variety and distribution around the globe, the protection task has grown immensely, with absolute security now accepted as a myth. However, due diligence has been seen to reduce and slow incidents. IT devices have diverged into a multitude of subcategories, including Cyber-Physical Systems (CPSs) and a further subsection of Small Unmanned Aerial Vehicles (sUAVs). While many techniques used to map and defend IT may be extended to sUAVs, CPSs in general have significant differences in internal architecture, external networking, and overall mission sets that influence the effectiveness of common cybersecurity techniques. An important aspect of cybersecurity is risk categorization of individual devices and the conglomeration on a network, which relies on common rating measures for comparison. IT devices still struggle with communication of security characteristics, though certain brands have made strides to separate themselves from the competition. This paper is an extension of the "Zero Stars" paper [1] to define the requirements for a simple rating system for consumers to effectively manage small Unmanned Aerial Vehicle (UAV) risk. The addition of traditional aircraft risk management provides new insights to the current risks facing UAVs that are not being managed by manufactures or consumers.

UAVs have been historically built for military applications and continued by hobbyist enthusiasm. By definition, UAV includes any device that can sustain flight autonomously, which separates it from similar sub-cultures of Remotely Piloted Vehicles (RPVs) and drones [2]. UAVs are usually able to either maintain a hover or move autonomously via computer navigation, whereas RPVs require continuous control instructions throughout flight and drones have even more limited mission and sophistication [2]. Arguably, the first UAV could be considered cameras attached to kites in 1887 by Douglas Archibald as a form of reconnaissance and which William Eddy used the same configuration during the Spanish-American War for reconnaissance [2]. As UAV operations and innovations continued through the Vietnam War, Desert Storm, and especially the Global War on Terror, the size, mission, and shape of UAVs have evolved to support military needs. Criminal uses have also grown with UAV prevalence with ingenious modifications matching latest military exploits [3].

UAVs take a multitude of forms and designs based on mission and user base, from hand-held copters to jet-powered light aircraft. Small UAVs follow the general component break out shown in Figure 1, 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. Commu-

nication Links are most commonly wireless Radio Frequency (RF) bands of 2.4 and 5 GHz. 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 logically separated from the Basic System but usually physically combined.

The ground station is split 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 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 secure 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 physical 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 Internet differently.

The exact definitions of size tiers have not been standardized between countries though they generally consist in some format of very small, small, medium, and large. Very small UAVs exist at a miniaturization of aerodynamics that result in very low Reynolds numbers, meaning the wing interacts with the air more similarly to a fin through water due to viscosity, 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 range is limited, their size allows for access or angle of attack at altitudes 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. Instead of a pilot and sensors, sUAVs are controlled by an autopilot, with varying degrees of autonomy. Autopilots vary greatly by manufacturer, with the most common DJI autopilots closed-source and their specific rules sets proprietary [3].

The rest of the paper is structured as follows. Section II explores current common rating systems for Traditional Aircraft, IT, Critical Infrastructure, and Insurance markets with a focus on the aspects of each that do translate to the sUAV inventory. Section III builds out from the conglomeration of related rating assessments the important objectives that are required for a sUAV specific cybersecurity rating. Section IV analyzes each of the fields for their applicability to a small UAV risk assessment for potential adaptation. We conclude our work in Section V with future work.

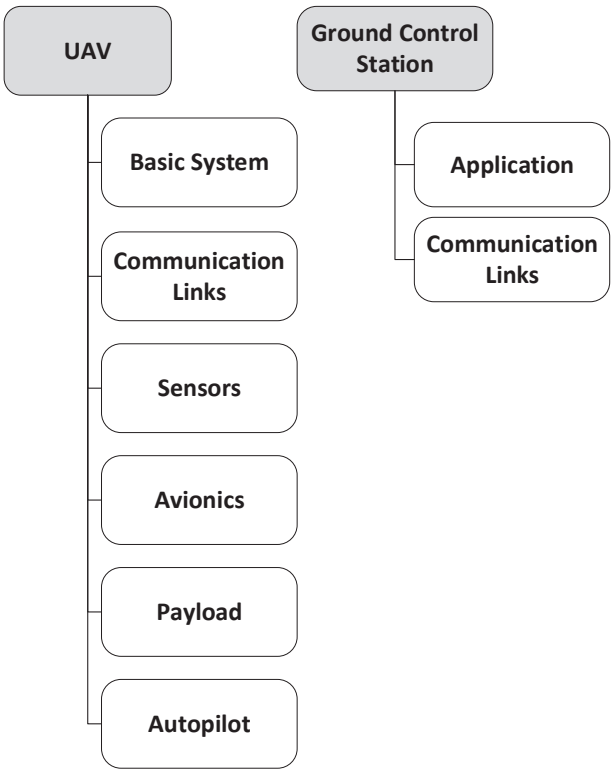

Fig. 1. Components of Typical UAV.

II. Related Work

No current physical or cyber security accreditation exists for UAVs. Since no current process exists to calculate risk, quantitative or qualitative, for sUAVs, there are no star ratings present on the market to be assigned to any sUAV, much less to compare models. Confounding the issue, aerial vehicles were engineered for operational effectiveness first, then marketed with minimal consideration for adversarial interference. Publicized cyber incidents with and against UAVs have been limited with the most well-known consisting of the Iranian incident in 2015 [4]. Whether the United States RQ-170 was captured by Electronic Warfare (EW) or cyber means [4], the incident highlights the vulnerability of UAVs in a combat zone and the need for security in future models to maintain integrity for mission success. With 15,000 UAVs being sold in the United States every month as of 2015 [5], the availability and exploitation of these devices is expected to also rise as the reward to effort ratio grows. The market share of small UAVs

manufacturers is as follows: 70% DJI, 7% Parrot, 7% Yuneec [6], with the remaining 14% comprised of all others. DJI and Yuneec are Chinese controlled manufacturers. This domination by China presents yet another avenue of supply chain risk that many organizations and countries with competing interests may want to be wary. Research into the vulnerability of sUAVs has also increased with a multitude of research showing specific risk in areas of Denial of Service (DoS) [7], GPS spoofing [8], and control hijacking [9].

A. Traditional Aircraft Assessment

The invention and market for UAVs stemmed from the traditional aircraft field. Regular aircraft have always been larger to accommodate the weight and thrust requirements needed for carrying pilots. In contrast, unmanned technologies have allowed for the creation of smaller vehicles. With nearly all on-board components being seen on both vehicles, a cyber risk assessment for traditional 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 aircraft industry does not currently have any cyber assessments for risk [10]. While industry standards for the design of aircraft information systems exist that incorporate defence 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 [10]. 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 [10]. As one of the key priorities of the report, the AIA subcommittee published that the industry needs "a risk managed approach...to architect future secure systems" and "better global visibility...to address aviation ecosystem threats and risks" [10].

Since the manufacturers have strict operational regulations but do not have any cyber assessments for aircraft, the Federal Avionics Administration (FAA) has had to incorporate a real-time operational risk assessment to the Aircraft Traffic Management (ATM) system which all traditional aircraft and all larger UAVs connect to for deconfliction of real-time flight plans [11]. Recognizing the need for including smaller UAVs, the FAA has granted funds to the National Aeronautics and Space Administration (NASA) to build and test a new ATM to manage the National Airspace System (NAS) as of 2014 [11]. Building from the ATM risk framework, NASA published the Unmanned Aerial Vehicle Traffic Management Risk Assessment Framework (URAF) which calculates a numerical risk value to correspond to the expected real-time risk associated with collisions per vehicle [12], which is calculated in Figure 2 at the "Conflict?" step. Using Bayesian networks fully defined for every potential component failure based upon the Unmanned Aerial System Traffic Management (UTM)'s

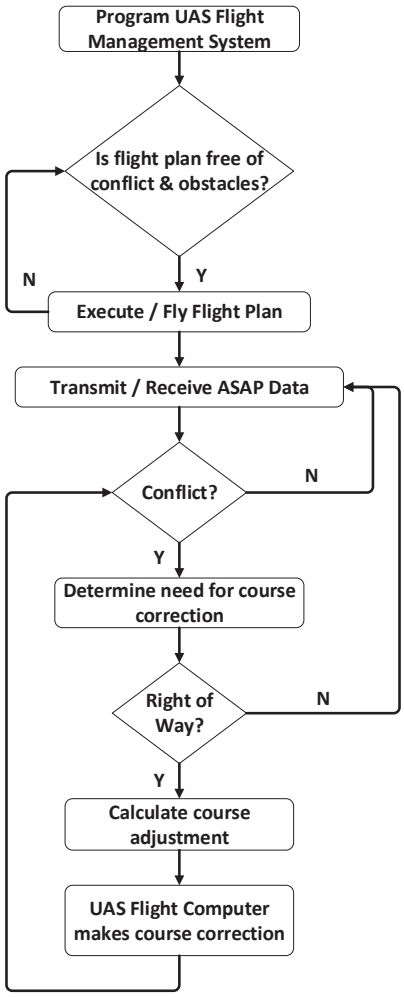

Fig. 2. FAA's UTM Control Flow for UAS [11].

input of vehicle and ground sensors, the URAF determines the probability of a collision with another aircraft, a structure, or a human being based on density maps of the United States (US) [12]. The flowchart shown is part of the patent for the system and is nearly a step-by-step reproduction from the current NAS framework, which fails to capture the differences between vehicles and only the operational risk. The small UAV sensor inputs are defined in the patent for the UTM as the required 14 communication protocols, none of which are currently required on small UAVs [13]. Initial tests of the UTM including the URAF was conducted in 2016 at seven FAA testing sites with 17 unique vehicles, though its success was marred with 32.5% non-conforming operations [14]. Non-conforming operations were defined by any position during a vehicle's mission that broke the operational risk threshold for collision, whether or not collisions actually occurred. The Bayesian network utilized in this testing captured the risk associated through one component failure and calculated from only five sensors [15]. NASA set the goal of initial operation by 2019, which was reached in the form of beta expansion

to the Low Altitude Authorization and Notification Capability (LAANC) in May of 2019 [16] at over 600 airports, and full operation for massive density operations by 2035 [11]. This beta is not the full UTM design, but a parallel authorization and tracking system of small UAVs. The URAF and the ATM risk framework are both device agnostic, except in terms of size and value [13]. There is no input of vehicle design, securities, or abilities to maneuver, all of which are a factor of cyber risks to aircraft. Due to the increasing automation and computation of aircraft, future risk assessments must individually consider each vehicle.

B. Traditional IT Assessment

UAVs can also be viewed as simply flying computer systems. Traditional IT risk assessments have been around since the early 2000s [17] and have almost solely focused on business devices and networks. While Network Security Risk Model (NSRM) [18] and Information Security Risk Analysis Method (ISRAM) [17] are some of the oldest quantitative risk assessment models, Common Vulnerability Scoring System (CVSS) is the most utilized today [19].

CVSS version 3.1 is an "open framework for communicating the characteristics and severity of software vulnerabilities" [20]. The score is based on three different metrics of a Base ranging from 0.0 to 10.0, tempered by Temporal and Environmental metrics. CVSS is owned and managed by Forum of Incident Response and Security Teams (FiRST) and is a significant information provider to the National Vulnerability Database (NVD). CVSS first gained large-scale usage under their Version 2 score which determined only a base score through metrics for Access Vector, Access Complexity, Authentication, Confidentiality Impact, Integrity Impact, and Availability Impact. Each metric was given a rating from up to three varying responses of severity. CVSSv2 was criticized heavily for vulnerability scoring diversity compared to experimental, lack of interdependence scoring of networks, and lack of correlation between proposed mitigations and actual score improvements [19]. CVSS version 3.0 added mandatory components for Privileges Required, User interaction, and Scope, plus the temporal and environmental metrics to influence the overall score. The current version has grown in use for vulnerability scoring, but still struggles with high false positive rates, poor predictability of future incidents, high sensitivity in regards to Availability Impact compared to all other impacts, and is heavily influenced by software type [21]. Built from CVSS, NVD has been found to lack in predicting mean time to next vulnerability due to the Common Vulnerability and Exploitations (CVEs) recording poor and inconsistent data by vendor and an increasing discovery, across vendors, of zero-day vulnerabilities [22]. The most recent version 3.1 of CVSS, summarized in Figure 3, also updated CVSS's mission from a simple risk severity to more limited vulnerability severity. The Base Metrics are split into three sub-categories due to commonalities in rating or how they are utilized in the underlying algorithms. The same grouping is applied to the Environmental Metrics, where the Modified Base sub-metrics are a repeat of the Base Metrics but updated for a network's individually unique security configuration. Each sub-metric is not equal, but are weighted numerically to best represent the severity that sub-metric conveys to the overall severity. In general practice, the Base Metrics, representing the severity of the attack, are the most heavily weighted as they can singularly push the severity to the extremes of an overall score of 0 or 10. Due to the change of scoring severity over risk and their consistent updating of algorithms, CVSS is a good starting point for known vulnerabilities present within a UAV, but the unique embedded nature of components, the normally informal and ad hoc networks used by UAVs, and unique mission and environment sets mean CVSS is not very likely to give a good perspective of actual vulnerabilities present and therefore directly assess risk.

C. Industrial CPS and Supervisory Control and Data Collection (SCADA)

At the other end of the spectrum for security indexing, sUAVs could be related to larger CPSs which have recently seen a surge in research and regulations to secure their unique networks. Industrial 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. These sensors are now directly digitized by network adapters, delivered to Programmable Logic Controllers (PLCs) that determine state, compute new controls, and send signals to actuators to finish the feedback loop. Human-Machine Interface (HMI) screens give a real-time display of the system state with minimal human interaction while smoothly running our critical infrastructure. SCADA systems are owned by corporations that produce or deliver their products to consumers; therefore the networks are not the product themselves, in contrast to home computers or even work stations which are most commonly modelled by IT networks. 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 [23]. The first two categories define differences in attack vectors for cyber-to-cyber or cyber-to-physical exploitation. 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 [24]. This leads to attack sophistication differences between IT and SCADA risk, since physical process manipulation via PLCs require detailed understanding of systems that are only present in the operational world. While the attack vectors require unique background, the computer systems monitoring and running the physical processes are commonly characterized by legacy equipment

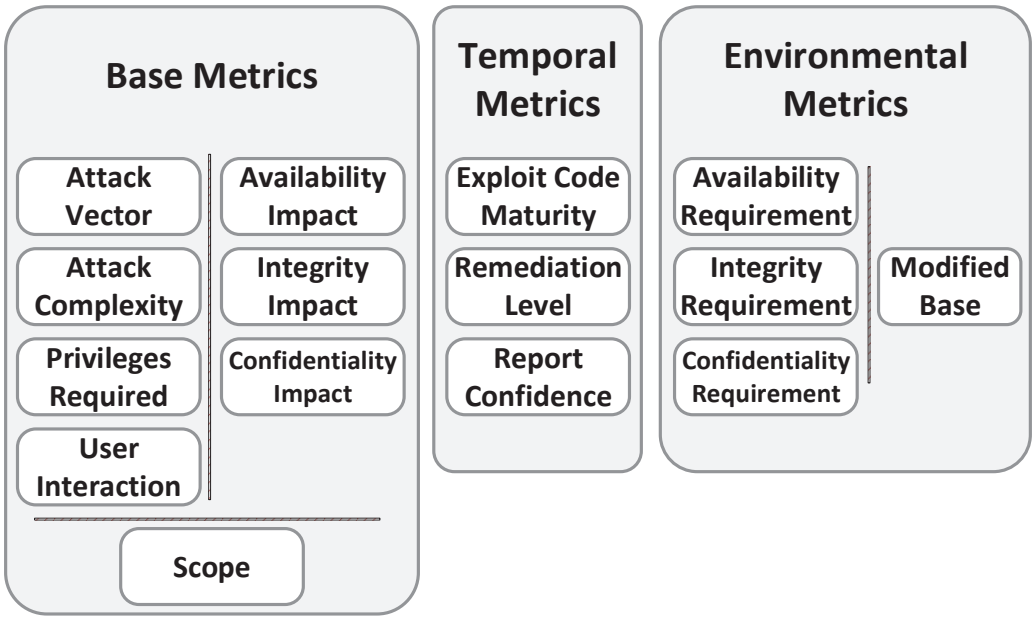

Fig. 3. Metric and Sub-metric breakout of CVSS [20].

with many known vulnerabilities. IT cybersecurity practices push for upgrade cycles on a regular basis to keep pace with manufactures' patching, however industrial systems are unable to upgrade nearly as often and require much larger investment capital to replace legacy systems that are considered permanent fixtures. 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 [25].

Risk assessments building from this impetus, and focusing on more than just nuclear, have attempted to predict the new methods to exploit processes. Most standardized methods merely cover the cyber-to-cyber and physical-to-physical exploitation, which arguably cover the easiest and most common historical attacks [26]. Stuxnet introduced publicly the possibilities of cyber-to-physical exploitation while little is known of possible physical-to-cyber vectors. At the direction of Department of Homeland Security (DHS), National Institute of Standards and Technology (NIST) published the Cybersecurity Framework (CSF) to directly define a risk framework for critical infrastructure in the US [27]. The core of the framework is the process of Identify, Protect, Detect, Respond, and Recover [27]. The framework's first push is to fully define the network currently in operation down to individual sensors with definitions of all system states. The next step is simple cybersecurity fundamentals such as segregation and locking down unnecessary protocols. Once at this steady operational state, the framework directs the effort to setup methods of detection, response, and recovery from attacks. 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 [26]. Even within unique critical infrastructure systems, it is useful to supervising organizations and protection agencies to compare system risks to more effectively protect nation-wide assets.

TABLE I. 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

Attempting to cover the lack of assessment of critical infrastructure systems' cyber risk, Cyber Security Risk Index (CSRI) is a proposed and beta risk assessment specifically using Bayesian Networks since systems should be defined through CSF. 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. [28]. 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 PLCs follow well-documented methods and means through NVD or CVSS, detection and vectors at the PLCs require expert weighting and most likely proprietary input [26]. 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 [29]. Detection before shut down is limited within industrial CPS to IT Intrusion Detection Systems (IDSs) that are built to overcome the unique aspects within industrial networks [23]. 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, the smaller scale of systems, and the shorter lifespan of systems reduce direct applicability to sUAVs.

D. Cybersecurity Insurance

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 [30]. 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 [31], with cyber crimes costing the global economy an estimated $450 billion in 2016 [32]. The companies that issued cyber insurance premiums totaling $1.35 billion in 2016 [33] 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 [34]. The most common and simple equation for insurance is based on the historical average of cost per incident times the probability of incident in the near future [35], 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 feasible and a positive for security, as long as the premiums charged are tied directly to self-protection strategies employed by the organization [36]. 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 [37].

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 [35]. CRISM is designed for IT networks where CVSS and NVD provide comprehensive insight to network vulnerabilities and usage. Inspired by automotive driver insurance programs, users voluntarily install a small device to provide additional operational information to the insurance company for the promise of lower premiums. As shown in Figure 4, CRISM has five phases.

1) Mapping: The first step of CRISM is static analysis of the targeted system to determine all components and links with all currently reported vulnerabilities. This mapping phase consists of determining the data and control links (if different) at a physical and protocol layer, operating system of both ground station and UAV, avionic and embedded systems controlling the UAV, and environment that the UAV lives in for connections and external (not necessarily adversary) radio waves.

2) Vulnerabilities: With all of the mapping laid out statically, the vulnerabilities that are known across all components are then expounded. At the communication links, vulnerabilities can consist of protocol flaws, susceptibility to jamming, and leakage of information. At the OS component, vulnerabilities are better laid out via CVSS and NVD such that the software and hardware vulnerabilities are better reported. The navigation vulnerabilities are based on the probability of false signals being accepted and the combination of sensors relied on reduces risk. Sensors such as Inertial Navigational System (INS) that are much more difficult to spoof than GPS reduce the cyber risk of system, but only if properly checked by the autopilot and the programmed failure state.

3) Attack Vectors: With the mapping and tabulation of known vulnerabilities, attack vectors can be determined by common methods through the entire system and the probability of attacks can be estimated. Attack vectors can be initialized only at input ports, whether on ground station or UAV. Vectors are trimmed by forward progress and ability to cause an effect on the mission.

4) Bayesian Network (BN) Graphs: Bayesian networks are then utilized to build out each vector across nodes to determine probability of forward progress and exploitation probability either through probabilities chosen by the organization or experts in the field.

5) Scoring: Lastly, scoring is completed by tabulating the probabilities of exploitation and its effect to the mission. CVSS does present a usable index for consumers and manufactures, however, it is a vulnerability severity assessment and not a direct correlation to risk indexing.

The ability to add an IDS to a Commercial Off The Shelf (COTS) UAV network is non-trivial due to size-weight constraints, mobile ad hoc network transients, and warranty issues arising from user “tampering”. Due to the light and mobile nature of UAV networks, this device or application

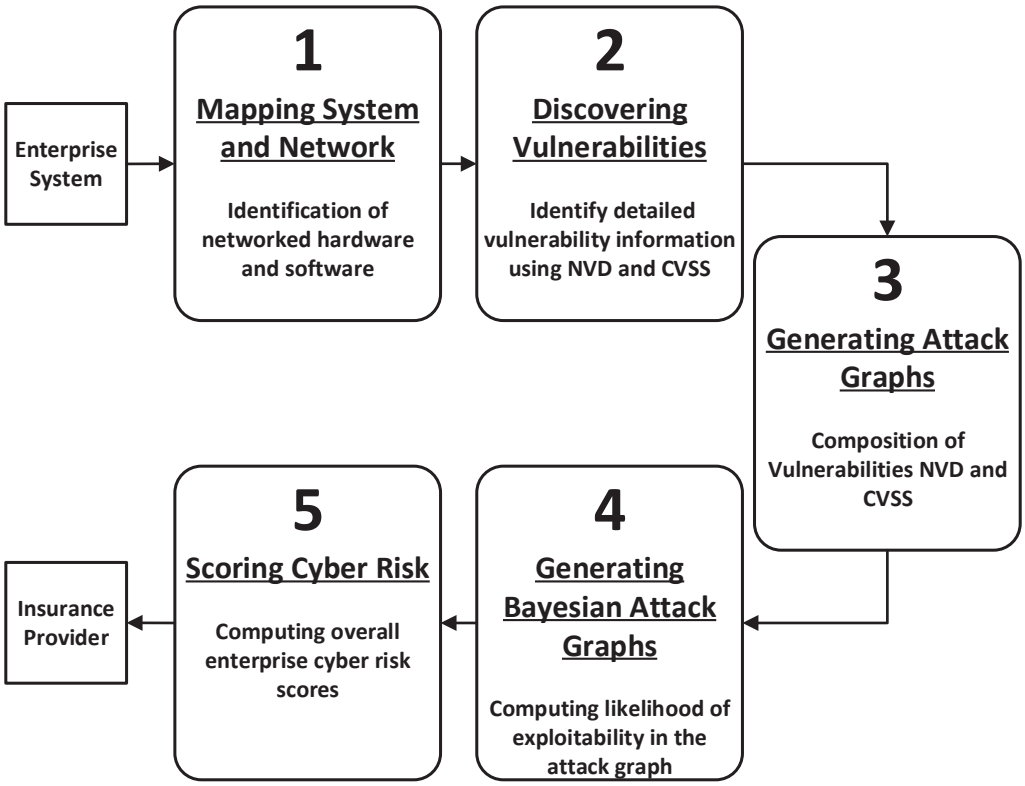

Fig. 4. Five phases of the Cyber Risk Scoring and Mitigation (CRISM) tool [35].

can not be stationary or the network will leave the protected area. Due to the proprietary nature of the majority of UAV manufacturers, tampering or augmenting the device will have secondary consequences that users may be unwilling to accept. Though most UAVs are unable to have an IDS attached or installed, an IDS application installed via hardware or software to the ground controller is a possibility. While CRISM can not be directly applied to UAV risk scoring without the IDS component (which currently does not exist and may not be feasible), their analytic model is very promising in its flexibility to include varying components.

III. Methodology

A difficult problem of risk assessment analysis is determining tool accuracy without historical use data to support it, of interest in this effort because not one of the presented risk assessments cover UAVs. Though accuracy may be the prime measurement, there are other measurements of value to consider which may aid in the process of determining an initial tool deployment until historical data can be realized. Three areas of comparison between these fields of risk assessment that are generally recognized as core to determining viability are as follows: usability, cost, and ease-of-understanding [38]. Unlike accuracy, it is important to note that these measures are qualitative and more prone to variability between observers, but not without value since differences can still be observed and compared.

The first measure, usability, is the measure of how well tailored a tool is to the value it measures. For these risk assessments, this means more specifically how well does the tool measure the risk of small UAVs. To break this down further, usability will be represented by traits of required expertise, flexibility to modifications, and network/device risk coverage. All risk assessments require the user to have some knowledge of the system being measured; however, if the tool uses information on the system that is more abstract or easier to access, then more users in the life-cycle would be able to use the tool. This measure is key if a risk assessment is to be used before operational employment, since not all operational details may be determined. Also the lower the required expertise needed to run the risk assessment, the more likely and more often the tool can be utilized as high expertise users are likely to be rare within any size organization. The second of the three sub-metrics of usability is flexibility. As with almost all computers, components are commonly rearranged and upgraded over time, which changes the cybersecurity risk of the system. Flexibility of the risk assessment to changes in the system and the ability to incorporate non-standard configurations is crucial to properly measuring the risk. The last of the usability sub-metrics is coverage, meaning the ability to measure the entire system for risk. A common saying is that “a chain is only as strong as the weakest link”, and this holds true for computer networks where attackers are smart and rewarded for utilizing the path of least resistance to

their target. While it may seem obvious that a risk assessment covers the entire system, history with risk tools has shown that smaller devices or components are commonly ignored even though they present a valuable node in the network [39].

Cost, the second metric, is the measure of how expensive (time and money) the tool is to run. Time is particularly important to smaller and more mobile devices like UAVs since the value of the measurement only lasts until something changes in the system. The monetary cost is also important since it determines the likelihood of an organization actually completing the test and the rate of re-assessing. Monetary cost can be incurred in a variety of methods, the most common being through additional devices to complete the measure and the level of expertise required to assess the measurements.

The last metric to be considered in this paper is that of readability or ease-of-understanding. Outside all of the prior metrics, the assessment needs to be easily communicated afterward to invested parties, such as supervising and regulating entities. Complication of readability can take the form of being too complex where it is impossible to compare systems or too simple where every system appears to have the same value. Users are better able to ingest a rating if it follows a form that they have seen before, such as a star rating or a percent value. Accreditation similar to the European and American automobile safety assessments, which use a number of stars to describe and compare the intrinsic safety quality for the vehicle, would be desirable. All of these criteria should provide a more detailed view into the described domains before determining applicability.

Each of the previously described operational domains use their designated risk assessments simply because they work, to some measure, for their devices. These tools meet an understood baseline that they are effective for their networks, but fall short when sUAVs are the subject. Any assessment that could be applied to sUAVs, but does not have the potential to properly rate the risk for these devices, is rated "Yellow" per category. It is possible for a tool to fall below this "Yellow" baseline and miss key components for a sUAV risk assessment tool, which would then be rated "Red". This "Red" rating means that significant changes are required to even initialize this tool to rate the risk of sUAVs. In the opposite manner, assessments that properly account for sUAV characteristics and calculate its system's risk on par with that domain's specific devices are to be labelled "Green". A "Green" rating is not to insinuate that all sUAV risk is completely accounted for, but that the tool reaches its own performance baseline with UAVs also. From Section II, it is expected that no assessment will reach "Green" across all or even most metrics since each showed significant failures in applicability to sUAVs.

IV. Analysis

As seen from the build out of other markets' rating systems, the validity of the rating is based on how holistic the system is examined. The layout of components and a cybersecurity risk index for sUAVs requires additional consideration for adjacent devices and networks plus the environment that the device is operating in since sUAVs are mobile. The environment for UAVs is defined as the system mission and the operational terrain, unlike traditional IT where environment is only the aspects that affect the digital access to a system such as the boundary design. The data link itself may be secure, but consideration for the country, locale, or altitude may change collision rate or noise on the channel and thus effect security. With swarm research as a far end of inter-connectivity of a sUAV, these flying computers use wireless communications that broadcast over the open air to connect to their ground station and to other UAVs. A rating needs to include some factor of the security of these other devices and the connection protocol that allows communications, especially if another ground station or UAV can gain operational control.

Table II shows analyzed applicability of each cybersecurity field to sUAV characteristics, if directly applied as described.

TABLE II. Assessment Applicability to Small UAVs.

	Expertise	**Flexibility**	**Coverage**	**Cost**	**Readability**
URAF	Green	Red	Red	Yellow	Yellow
CVSS	Yellow	Red	Yellow	Yellow	Green
CSRI	Yellow	Red	Green	Yellow	Red
CRISM	Yellow	Yellow	Yellow	Red	Green

NASA's URAF shows promise to applicability to sUAVs in terms of expertise required to complete the assessment, given that the Bayesian networks and density maps are prepopulated. Given the working UTM integrating with sUAVs, a real-time assessment of the operational risk should be calculable without much human involvement. However, it is an operational risk assessment that is "device agnostic" so its flexibility and coverage are particularly lacking in assessing cyber risk. Its implementation is expensive since it requires a multitude of ground sensors and manufactures to upgrade models, but this is a requirement of all aircraft so it is not worse applying it to sUAVs. In terms of readability, URAF uses a probability of accident as its score, which may be somewhat easy to use, but communicating the cyber risk is more difficult to tease out.

FiRST's CVSS provides a scoring system that has been tested and refined for a decade, but fails to assess the key aspects of risk and sUAVs. The tool's assessment of IT vulnerability severity has been a boon at the enterprise level to prioritize defenses and plan for future improvements. To be applied to sUAV networks, the tool would need to be updated to reflect first the characteristics and market of sUAVs, such as modifications and time in use. In addition, CVSS has explicitly defined themselves away from risk assessment for their own reasons, so the tool would also need to be updated from just severity, or the cost variable of risk, to risk in general. Incorporating likelihood is not easy. However, without it, risk frameworks are unable to compare risk and direct appropriate action.

The proposed risk assessment to CSF, the CSRI, generally misses the goal of a sUAV risk assessment more than the

other fields due to its focus on critical infrastructure. While the intent to include CSRI was to observe its ability to incorporate cyber-physical systems and wide area networks of smaller devices, the field of critical infrastructure is inflexible and very slow to change. Nuclear power plants, as the design impetus to CSRI, measure their lifespans in decades and require extreme bureaucratic processes to update networks for fear of network failure or compromise. The ability to fully map out all components and sensors to all system states, cyber and physical, is possible and most likely beneficial, but time and expertise consuming beyond the average user. Corporations may have the expertise and the desire to define their risk minutely, but development and acquisition move too fast for these businesses to stay competitive. To be molded as a sUAV risk assessment, CSRI would require direction to the most important components and provide accurate statistics for the Bayesian networks. A method of rectifying this may be to keep a living document accessible to the public, containing the Bayesian networks for common modifications to configuration and payload.

Lastly and also from the research community, CRISM presented an approach to correct for CSRI's last mentioned failure, adaptation to modifications. By inserting an IDS into a network, a real-time calculation similar to NASA's UTM can be attempted for risk, and unlike UTM, specifically to cyber risk. CRISM suffers from the same restrictions with its Bayesian networks as CSRI, in that likelihood statistics are currently lacking and would need to be provided to the consumer, whether at the acquisition or operational stage. While covering for the flexibility to modifications by tracking live traffic, CRISM lacks the coverage that UTM is building by attaching to the NAS. Without national coverage by regulation, individuals would need to insert the IDS into the sUAV network, which can be difficult due to the mobile and ad hoc nature of sUAVs. While corporations or governments may be willing to cover the additional cost to reduce risk via insurance, it is unlikely individuals will as insurance has not been made viable yet.

V. Conclusion and Future Work

No assessment properly calculated the cyber risk present within a sUAV and all related domains presented in this paper require significant working to be used. Of all of the related domains, CVSS by FiRST appears to have the closest ties to sUAV cyber risk through its presentation of an operational scoring system used by cyber professionals. Though CVSS is no longer defined as a risk assessment, the system was built as one and continues to provide the significant input of severity to the risk imposed by the system on the network. It is conceivable that by updating the definitions of the sub-metrics of CVSS version 3.1 to define sUAV networks over IT components, a new standalone cyber risk assessment may be possible and presented to consumers to more intentionally purchase sUAVs in accordance with their risk frameworks.

This is not to presume that the other assessments in this paper are incapable of adaptation, as described in their analysis. NASA's UTM currently treats sUAVs as indistinguishable from a cyber perspective, which is simply incorrect seeing the wide differences in manufacturers, components, and payloads. Adjusting for cyber-related sensor measurements may be simple enough, however the regulation process will require decades until adoption. Critical infrastructure's CSRI has the most adaptation required as the process to apply to unique sUAVs is significant and the Bayesian statistics required are mostly unknown or unproven. Lastly, the insurance industry's CRISM follows NASA's model with a focus on cyber risk over operational risk, but does not have the backing, funding, or maturity that UTM currently has in the field. National coverage in calculating cyber risk per vehicle would provide unique insights and feedback to corporations to use in their risk framework, but misses the opportunity to provide these inputs at development and acquisition life-cycle phases where they can provide the most effective change.

Future work in the field of sUAV risk assessment requires the building of a quantitative equation for the flying devices or the adaptation from a parallel assessment, as discussed at length in this research. The strongest potential seems to be qualitative characteristics given numerical value and weight, as seen with CVSS and meeting the initial objectives of usability, cost, and ease-of-understanding. Analytical scoring of a sampling of UAVs when paired with missions and environments then would provide validity to the assessment. It is unknown at this time if an analytical-only scoring would provide the best results in light of highly proprietary brands dominating the market and focusing risk assessment at the earliest stages of a system's life-cycle. To focus at the operational stage, a CRISM-like adaptation may be better suited, though the model needs adaptation followed by validation through live testing on hardware in the loop simulation and then networked UAVs. Hardware in the loop is vital to simulations with UAVs due to the physical responses of the system to cyber effects, without which many of the detection methods of cyber-to-cyber and cyber-to-physical attacks are lost. Even with an IDS for UAVs, the Bayesian models would still need to be created for UAVs over the traditional networks and validated to historical data.

Scoring, at this point, is more for internal comparison, but the future expectation is to provide a medium for consumers to easily compare similar sUAVs and influence the manufacturers with their purchases. By providing a single metric per model, mission, and expected environment, the buyer may be better informed based on their individual level of risk acceptance or risk framework, which may be still further offset by insurance premiums. However, until a risk assessment becomes accredited, consumers will be reliant on manufacturer's advertisements and limited personal expertise to compare the risk being introduced to their mission sets. While this trust may be enough for lesser priority missions, the major countries of manufacturing for sUAVs have shown repeated violation of trust and security, and consuming organizations still lack a

formal method to utilize their own cyber risk frameworks with sUAV inventories.

Disclaimer: The views expressed in this paper are those of the authors and do not necessarily reflect the official policy or position of the Air Force, the Department of Defense, or the U.S. Government. PA Case Number: 88ABW-2020-0189.

REFERENCES

[1] D. Pettit, S. Graham, and R. Dill, "Zero Stars: Analysis of Cybersecurity Risk of Small COTS UAVs," *International Conference on Emerging Security Information, Systems and Technologies, Conference Proceedings*, 2019.

[2] 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.

[3] A. Roder, K.-K. R. Choo, and N.-A. Le-Khac, "Unmanned Aerial Vehicle Forensic Investigation Process: DJI Phantom 3 Drone As A Case Study," *Digital Investigations*, pp. 1–14, 2018. [Online]. Available: arxiv.org/abs/1804.08649

[4] K. Hartmann and K. Giles, "UAV exploitation: A new domain for cyber power," *International Conference on Cyber Conflict, CYCON*, vol. 2016-Augus, pp. 205–221, 2016.

[5] A. Karp, "Congress to hold UAV safety hearing Oct. 7," 2015, [Retrieved: September 2019]. [Online]. Available: atwonline.com/government-affairs/congress-hold-uav-safety-hearing-oct-7

[6] Z. Valentak, "Drone Market Share Analysis Predictions for 2018: DJI Dominates, Parrot and Yuneec Slowly Catching Up," *Drones Globe*, 2017, [Retrieved September 2019]. [Online]. Available: www.dronesglobe.com/news/drone-market-share-analysis-predictions-2018

[7] 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.

[8] 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.

[9] 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)*, p. 4, 2011.

[10] D. Diessner, H. Wynsma, L. Riegle, and P. Morrissey, "Civil Aviation Cybersecurity Industry Assessment & Recommendations, August 2019, Report to the AIA Civil Aviation Council , Civil Aviation Regulatory & Safety Committee AIA Civil Aviation Cybersecurity Subcommittee," 2019.

[11] P. Kopardekar, "Enabling Civilian Low-altitude Airspace and Unmanned Aerial System Operations by Unmanned Aerial System Traffic Management," *AUVSI Unmanned Systems 2014*, pp. 1678 – 1683, 2014.

[12] E. Ancel, F. Capristan, J. Foster, and R. Condotta, "Real-time Risk Assessment Framework for Unmanned Aircraft System (UAS) Taffic Management (UTM)," *17th AIAA Aviation Technology, Integration, and Operations Conference*, pp. 1–17, 2017.

[13] P. Kopardekar, "(12) Patent Application Publication (10) Pub. No.: US 2016/0275801 A1," *United States Patent Applications*, pp. 1–47, 2016.

[14] J. Rios and P. Venkatesan, "NASA UAS Traffic Management National Campaign," *2016 IEEE/AIAA 35th Digital Avionics Systems Conference*, pp. 1–6, 2016.

[15] L. Barr, R. Newman, E. Ancel, C. Belcastro, J. Foster, J. Evans, and D. Klyde, "Preliminary Risk Assessment Model for Small Unmanned Aerial Systems," *17th AIAA Aviation Technology, Integration, and Operations Conference*, pp. 1–57, 2017.

[16] F. A. Administration, "Air Traffic Facilities Participating in LAANC," 2019, accessed December 2019. [Online]. Available: www.faa.gov/uas/programs-partnerships/data-exchange/laanc-facilities

[17] B. Karabacak and I. Sogukpina, "ISRAM: Information Security Risk Analysis Method," *Computers Security*, vol. 24.2, pp. 147–159, 2005.

[18] M. H. Henry and Y. Y. Haimes., "Comprehensive Network Security Risk Model for Process Control Networks," *Risk Analysis: An International Journal*, vol. 29.2, pp. 223–248, 2009.

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

[20] FiRST, "Common Vulnerability Scoring System V3," 2015, [Retrieved: September 2019]. [Online]. Available: www.first.org/cvss/cvss-v30-specification-v1.8.pdf

[21] A. A. Younis and Y. K. Malaiya, "Comparing and Evaluating CVSS Base Metrics and Microsoft Rating System," in *Proceedings - 2015 IEEE International Conference on Software Quality, Reliability and Security, QRS 2015*. Institute of Electrical and Electronics Engineers Inc., 2015, pp. 252–261.

[22] S. Zhang, X. Ou, and D. Caragea, "Predicting Cyber Risks through National Vulnerability Database," *Information Security Journal*, vol. 24, no. 4-6, pp. 194–206, 2015.

[23] 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.

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

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

[26] 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, no. 10, pp. 8153–8162, 2018.

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

[28] 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.

[29] 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.

[30] B. Brown, "The Ever-Evolving Nature of Cyber Coverage," 2014, [Retrieved: September 2019]. [Online]. Available: www.insurancejournal.com/magazines/magfeatures/2014/09/22/340633.htm

[31] C. Stanley, "Cyber Market Estimate," 2017, interview: 2017-06-26.

[32] L. Graham, "Cybercrime costs the global economy $450 billion: CEO," 2017, [Retrieved: September 2019]. [Online]. Available: www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html

[33] InsuranceJournal.com, "Cyber Insurance Premium Volume Grew 35% to $1.3 Billion in 2016," 2017, [Retrieved: September 2019]. [Online]. Available: www.insurancejournal.com/news/national/2017/06/23/455508.htm

[34] J. Yin, "Cyber insurance: Why is the market still largely untapped?" 2015, [Retrieved: September 2019]. [Online]. Available: www.aei.org/publication/cyber-insurance-why-is-the-market-still-largely-untapped

[35] 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.

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

[37] A. Panou, C. Xenakis, and C. Ntantogian, "RiSKi: A Framework for Modeling Cyber Threats to Estimate Risk for Data Breach Insurance," *Association for Computing Machinery*, 2017.

[38] I. Stine, M. Rice, S. Dunlap, and J. Pecarina, "A cyber risk scoring system for medical devices," *International Journal of Critical Infrastructure Protection*, vol. 19, pp. 32–46, 2017. [Online]. Available: doi.org/10.1016/j.ijcip.2017.04.001

[39] A. Pendleton, R. Dill, and D. Pettit, "Surveying the Incorporation of IOT Devices into Cybersecurity Risk Management Frameworks," *SECUREWARE 2019 Proceedings*, 2019.