Zero Stars: Analysis of Cybersecurity Risk of Small COTS UAVs

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

Rich Dill
Dept of Computer Engineering
Air Force Institute of Technology
Dayton, Ohio, USA
email: Richard.Dill@afit.edu

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

***Abstract*—Commercial off the shelf small Unmanned Aerial Vehicle (UAV) market has grown immensely in popularity within the hobbyist and military inventories. The same core mission set from the hobbyists directly relates to global military strategy in the modern age, with priority on short range, low cost, real time aerial imaging and limited modular payloads. These small devices have the added perks of a small cross section, low heat signature, and a variety of transmitters to send real-time data over short distances. As with all new advances within the technological fields, security is a second-thought to reaching the market as soon as viable. New research is showing growing exploits and vulnerabilities, from individual small UAVs guidance and autopilot controls to the mobile ground station devices which may be as simple as a cellphone application. Research calls producers to fix and engineer the small UAVs to protect consumers, but consumers are left in the dark to the protections installed when buying new or used vehicles. At current date, there is no marketed or accredited risk index for small UAVs, but current research in similar realms of traditional Information Technologies, Cyber-Physical Systems, and Cyber Insurance give insight to significant factors required for future small UAV risk assessment and prioritize lessons learned. In this research, three fields of risk frameworks are analyzed to determine applicability to UAV security risk and key components that must be analyzed by a proper 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 index risks of UAVs.**

Keywords*—*UAV; cybersecurity; quantitative; risk assessment; COTS.

I. Introduction

Cybersecurity is the Herculean task to prevent all adversarial attacks over Information Technology (IT) devices and errors that release or lose information deemed valuable to an organization or individual. As computer devices have exploded in variety and distribution around the globe, the protection task has grown and absolute security has become accepted to be a myth, though due diligence has been seen to reduce and delay incidents. IT devices have diverged into a multitude of subcategories, including Cyber-Physical Systems (CPSs) and further subsection 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 effect how effective and important common techniques are to cybersecurity. One 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 market share. As new vulnerabilities and exploitations accumulate for sUAVs, the industry will find the consumer base increasing in desire for quick and equal rating to make purchasing decisions based on their planned mission set.

Unmanned Aerial Vehicles (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 [1]. UAVs are usually able to either maintain a hover or move completely via computer navigation, whereas RPVs require control instructions throughout flight and drones have limited mission and sophistication [1]. The first UAV is most likely to be considered a kite or balloon that could maintain flight when tied off and have some control input from the ground. Cameras were first attached to kites in 1887 by Douglas Archibald as a form of reconnaissance and William Eddy used the same contraption during the Spanish-American War for reconnaissance [1]. 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 exploits [2]. The market share of small UAVs is made up of 70% DJI brand, followed by 7% Parrot, 7% Yuneec [3], showing a strangle hold of Chinese controlled manufacturers for consumers to take note.

UAVs take a multitude of forms and designs based on mission and user base, from hand-held copters to jet-powered light aircraft. For sUAV, all follow the general component break out as seen in Figure 1, with four 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 coded by brand per vehicle and allows near real time control. The weapon component has been seen within military operations, though the vast majority of sUAVs are used for military or hobbyist reconnaissance with the sensor component. As defined for UAV, some form of autonomous control will be built into the vehicle's navigation. The ground station is split into the Operators component and Communication links, though, with sUAVs, these are typically contained within the same device, a tablet or laptop.

Copyright (c) IARIA, 2019. ISBN: 978-1-61208-746-7

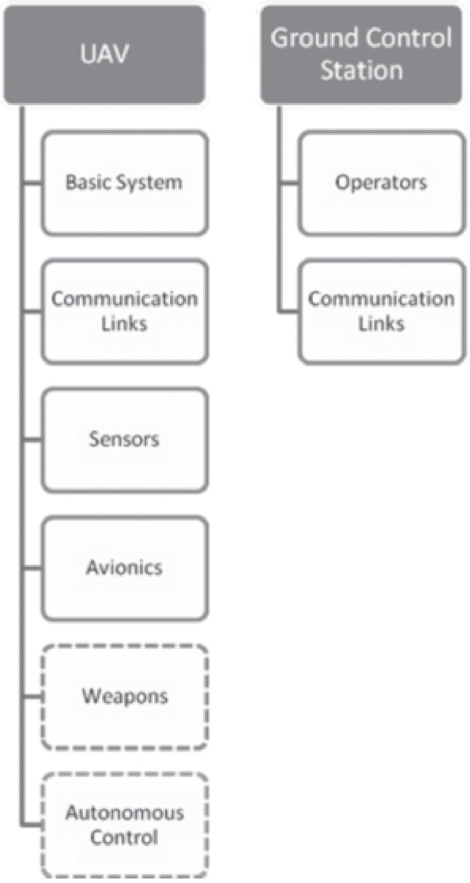

Fig. 1. Components of Typical UAV [4].

The exact definitions between sizing tiers have not been standardized between countries though, practically speaking, they 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 shorter in range, their size allows for access or angle of attack by altitude 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. 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 directly from the vehicle. Instead of a pilot and sensors, sUAVs are controlled by varying autonomy of their autopilot. Autopilots vary greatly by manufacturer, with the most common DJI autopilots closed-source and their specific rules hidden [2].

The rest of the paper is structured as follows. Section II explores current common rating systems for traditional IT, Supervisory Control and Data Collection (SCADA), and Insurance markets with a focus on aspects that do translate to the sUAV inventory. Section III builds out from the conglomeration of related rating indexes the important aspects that are required for a sUAV specific cybersecurity rating. Section IV analyzes each of the fields for their applicability to small UAVs risk assessment for potential adaptation. We conclude our work in Section V.

II. Related Work

No current physical or cyber security accreditation exists for UAVs. 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 meet the demand. 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 compare models. Adding to the issue, aerial vehicles were engineered for operational effectiveness first then marketed with minimal consideration for adversarial interference. Cyber incidents with and against UAVs have been limited with the most well-known consisting of the Iranian incident [4] and current research into hacking UAV controls. While the debate is still out on 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 use of exploitations on these devices is expected to also rise as effort to reward ratio grows. Research into the vulnerability of sUAVs has also increased with a multitude of research showing specific risk in areas of Denial of Service (DoS) [6], Global Positioning System (GPS) spoofing [7], and control hijacking [8]. No security specific components have been added to UAVs in response, other than patches and more secure software or additional navigational components for the autopilot to internally cross-check location.

A. Traditional Risk Assessment

UAVs are most simply flying computer systems. Traditional risk assessments have been around since the early 2000s [9] and have almost solely focused on business devices and networks. While Network Security Risk Model (NSRM) [10] and Information Security Risk Analysis Method (ISRAM) [9] are some of the oldest quantitative risk assessment models, Common Vulnerability Scoring System V3 (CVSSv3) is the most utilized today [11].

CVSSv3 is an "open framework for communicating the characteristics and severity of software vulnerabilities [12]." The score is based on three different metrics of a Base ranging from 0.0 to 10.0, tempered by Temporal and Environmental metrics. CVSSv3 is owned and managed by FIRST Inc. and is a heavy 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 [11]. CVSSv3 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 [13]. Built from CVSSv3, 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 trend across vendors of zero-days [14]. CVSSv3 is the starting point for determining known vulnerabilities present within a UAV, but the embedded nature of a component, the wide brand difference within a single UAV, and unique mission sets of UAVs mean CVSSv3 is not very likely to give a good perspective at actual risk.

B. Industrial CPS and 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 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 largely distributed networks. Physical sensors that used to require eyes to read, determine system state, and adjust actuators to keep processes within safety limits and manufacturing effectiveness, now are read by network adapters, ran through Programmable Logic Controller (PLC) that determine state, then send signals to actuators to finish the feedback loop. Human-Machine Interface (HMI) screens give real-time display of system state to allow minimum human interaction to keep our modern society running smoothly. SCADA systems are owned by corporations to produce or deliver their products to consumers, and therefore the networks are not the products directly as seen by 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 [16]. 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 or is valuable in itself, but industrial CPS exploitation usually requires exploitation to continue further to influence physical processes to either ruin or shut down systems [17]. This leads to attack sophistication differences between IT and SCADA risk, since physical process manipulation via PLCs require intense 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 with many known vulnerabilities. IT cybersecurity practices push for upgrade cycles on a regular basis to keep with manufactures' patching, however industrial systems do not upgrade nearly as often and require much larger investment capital to change out 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 [18]. Risk assessments building from this impetus and for more than just nuclear realm have been trying to grasp 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 [19]. Stuxnet introduced publicly the possibilities of cyber to physical exploitation while little is known of possible physical to cyber vectors. To cover the cyber to physical risk, the most common technique is through Bayesian networks with attach trees and Markov chains [20]. 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 CVSSv3, detection and vectors at the PLCs require expert weighting and most likely proprietary input [19]. This method for a rating has been worked out for the nuclear industry in the form of Cyber Security Risk Index (CSRI) where all the possible physical sensor states have been propagated and the penetration testing is impossible for other methods of rating risk [21]. 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 [16]. 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 open-source index, smaller scale, and shorter lifespan of systems reduce direct applicability to sUAVs.

C. 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 [22]. Insurance companies function on a strategy of taking premiums upfront to cover the risk of failure in the

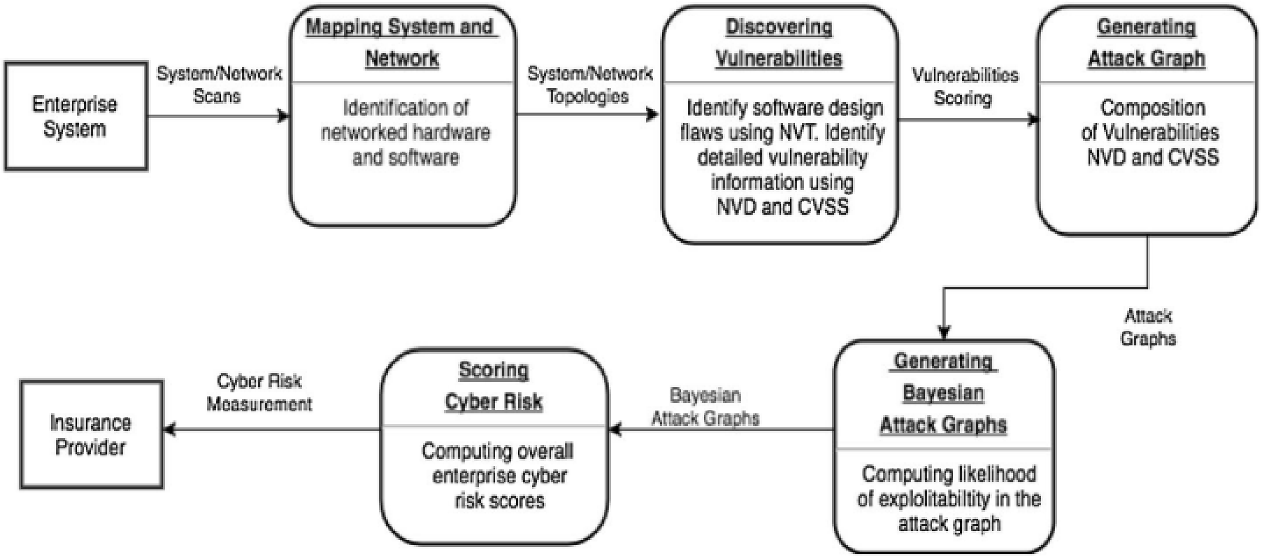
Enterprise System
System/Network Scans
Mapping System and Network
Identification of networked hardware and software
System/Network Topologies
Discovering Vulnerabilities
Identify software design flaws using NVT. Identify detailed vulnerability information using NVD and CVSS
Vulnerabilities Scoring
Generating Attack Graph
Composition of Vulnerabilities NVD and CVSS
Attack Graphs
Generating Bayesian Attack Graphs
Computing likelihood of explolitabiltity in the attack graph
Bayesian Attack Graphs
Scoring Cyber Risk
Computing overall enterprise cyber risk scores
Cyber Risk Measurement
Insurance Provider

Fig. 2. Five phases of the Cyber Risk Scoring and Mitigation (CRISM) tool [15].

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 market estimated at $3 to 3.5 billion in 2017 [23], with cyber crimes costing the global economy an estimated $450 billion in 2016 [24]. The companies that issued the total cyber insurance premiums totaling $1.35 billion in 2016 [25] 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 [26]. 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 [15], 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 and fewer have published methods of quantitative risk indexes. Cyber insurance is possible and good for security as long as the premiums imposed are tied directly to self-protection strategies employed by the organization [27]. 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 [28].

The most promising methods to grasp the state of a network are presented by the Cyber Risk Scoring and Mitigation tool (CRISM) which operates as a specially designed IDS [15]. This method used in cyber insurance is designed for IT networks where the CVSSv3 and NVD provide comprehensive insight to network vulnerabilities and usage probabilities, though was inspired by driver insurance programs where users installed a device to provide additional information to the insurance company for lower premiums. The ability to add an IDS to a Commercial Off The Shelf (COTS) UAV is most likely impossible due to size or tampering with warranty, therefore CRISM can not be directly applied to UAV risk indexing. However, their analytic model is very promising in its flexibility to include varying components. As shown in Figure 2, CRISM has five phases.

1) Mapping: The first step is static analysis of the 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 CVSSv3 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. CVSSv3 does present a usable index for consumers and manufactures, however, it is a vulnerability severity assessment and not a direct correlation to risk indexing.

III. Methodology

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-to-understand results [29]. Of these, usability will be further examined by traits of required expertise, flexibility to modifications, and coverage of device and network risk, which compose specific UAV risk components. These criteria should provide a more detailed view into the described fields before determining applicability.

Each of the fields specifically utilize their designated risk assessments simply for the reason that they work for their devices. These tools meet an understood baseline that they are effective, but fall short when sUAVs are the subject. Any assessment that meets, but does not have the potential to exceed this baseline, is rated “Yellow” per category. Within categories, it is possible for the field’s tool to fall below this baseline and miss key components for a sUAV risk assessment tool, which would then be rated “Red”. In the opposite manner, some fields that properly account for sUAV characteristics and calculate risk indices on par with with that field’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.

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. With swarm research as a far end of 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. The environment aspect is made of the inherit radio waves that may or may not interfere with communications and control of the UAV. 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. Table I shows analyzed applicability of each cybersecurity field to sUAV characteristics, if directly applied.

TABLE I
Index Applicability to Small UAVs.

	Expertise	Flexibility	Coverage	Cost	Readability
Traditional	Yellow	Red	Yellow	Yellow	Green
ICS	Yellow	Red	Green	Yellow	Red
Insurance	Yellow	Green	Yellow	Red	Green

CVSSv3 is built for traditional IT systems, especially for common computer components and software that the community can test and submit vulnerabilities. The sUAV field uses more embedded systems that either run on proprietary hardware or software, and the devices operate much more frequently on ad hoc networks where a simple modifier for environment and temporal scores is imprecise and lacking. Industrial Control System (ICS) and SCADA vulnerability tests take into account the physical aspects influenced by and can effect cyber devices as seen in sUAV, however the static and unique natures of SCADA systems show an underestimation for new exploits and most quantitative indices are close held by organizations selling services. Additionally, the unique fluidity of networking and device modification would require near continuous recalculation of risk or initial calculation for every configuration. The insurance-spawned CRISM shows theoretical promise, especially within its analytic approach, though the IDS portion needs adaptation to the UAV field before the tool would be truely useful. Since the market share is dominated by proprietary minded brands, the IDS in question may need to be network only, which will reduce its effectiveness but still provide live insight into the inherit risk. Many of the holes of CVSSv3 also carry over to the insurance field since the tool borrows heavily from the same IT databases for vulnerability assessment. While CVSSv3 and SCADA indices have more operational data backing approaches, CRISM requires additional research, data comparison, and marketing before being viable main-stream, which is where a sUAV risk index will be of greatest use to the consumers.

V. Conclusion and Future Work

Small UAVs do not have a quantitative risk assessment that meets the baseline of accuracy for their unique characteristics. Current risk assessments focus on either the standard desktop configurations of hardware and software as with the traditional CVSSv3 or the network with ICS and insurance’s CRISM. Of the three fields, the CRISM tool shows promise for attaining fidelity on sUAVs, but would need significant work to adapt to the ad hoc wireless networking and UAV specific protocols. Connected, CVSSv3 requires significant addition of UAV vulnerability signatures to be useful.

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. Analytical scoring of a sampling of UAVs then would provide validity to the assessment. It is unknown at this time if an analytic only scoring would provide the best results by providing ease of use in light of highly proprietary brands defining the market. A CRISM-like adaptation needs validation through either live testing on single and networked UAVs or at least hardware in the loop simulation. Hardware in the loop is vital to simulation with UAVs due to the physical responses of the system to cyber effects. Without considering the physical response, many of the detection methods of cyber to cyber and cyber to physical attacks are lost.

Scoring, at this point, is more for internal comparison, but the future expectation is to provide a medium for the manufacture or market to convey the risks inherent in different hardware and software configurations to consumers. By providing a single metric based on mission, the buyer may be better informed based on their individual level of risk acceptance, which may be then offset by insurance premiums. Until a risk assessment becomes accredited, consumers will be reliant on manufacturer advertisement and personal expertise to compare the risk being introduced to their mission sets.

ACKNOWLEDGMENT

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-2019-2852.

REFERENCES

[1] 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.

[2] 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: http://arxiv.org/abs/1804.08649

[3] 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: http://www.dronesglobe. com/news/drone-market-share-analysis-predictions-2018

[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: http://atwonline.com/government-affairs/congress-hold-uav-safety-hearing-oct-7

[6] 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.

[7] 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.

[8] 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.

[9] B. Karabacak and I. Sogukpina, "Isram: Information security risk analysis method," *Computers Security*, vol. 24.2, pp. 147–159, 2005.

[10] 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.

[11] 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.

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

[13] 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.

[14] 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.

[15] 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.

[16] 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.

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

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

[19] 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.

[20] 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.

[21] 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.

[22] B. Brown, "The ever-evolving nature of cyber coverage," 2014, [Retrieved: September 2019]. [Online]. Available: https://www.insurancejournal.com/magazines/mag-features/2014/09/22/340633.htm

[23] C. Stanley, "Cyber market estimate," 2017, interview: 2017-06-26.

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

[25] InsuranceJournal.com, "Cyber insurance premium volume grew 35% to $1.3 billion in 2016," 2017, [Retrieved: September 2019]. [Online]. Available: https://www.insurancejournal.com/news/national/2017/06/23/455508.htm

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

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

[28] 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.

[29] 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: https://doi.org/10.1016/j.ijcip.2017.04.001