Spring 5-20-2019

Malicious Digital Penetration of United States Weaponized Military Unmanned Aerial Vehicle Systems: A National Security Perspective Concerning the Complexity of Military UAVs and Hacking

Edwin Bell
La Salle University, nexus608@comcast.net

Malicious Digital Penetration of United States Weaponized Military Unmanned Aerial Vehicle Systems: A National Security Perspective Concerning the Complexity of Military UAVs and Hacking

A MASTER THESIS

Submitted to the faculty

of

LaSalle University

by

Edwin S. Bell

In Partial Fulfillment of the Requirement for the Degree

of

Master of Science

May 2019

LaSalle University

Philadelphia, Pennsylvania

DEDICATION

I dedicate this thesis to my wife whose support and encouragement was invaluable to me during the research and writing process.

ACKNOWLEDGEMENTS

I am thankful to the members of my committee for their assistance and guidance during this research. I wish to give special thanks to my specific thesis advisor, Professor Steven Hilkowitz for his teaching and instruction during my studies. I remain grateful for his support towards me in pursuing the highest analytical and writing standard. I also wish to thank Professor Margaret McCoey for her unfailing support whenever I required assistance. Her dedication to academic excellence, skills in evaluating digital networks, and leadership as department chair are unrivaled. She shall always be remembered fondly.

ABSTRACT OF THE THESIS

Malicious Digital Penetration of United States Weaponized Military Unmanned Aerial Vehicles Systems: A National Security Perspective Concerning the Complexity of Military UAVs and Hacking

A MASTER THESIS

Submitted to the faculty

of

LaSalle University

by

Edwin S. Bell

In Partial Fulfillment of the Requirement for the Degree

of

Master of Science

May 2019

LaSalle University

Philadelphia, Pennsylvania

Professor Steven Hilkowitz, Thesis Professor

Abstract

The United States' (US) military unmanned aerial vehicle (UAV) has seen increased usage under the post 9/11 military engagements in the Middle East, Afghanistan, and within American borders. However, the very digital networks controlling these aircrafts are now enduring malicious intrusions (hacking) by America's enemies.

The digital intrusions serve as a presage over the very digital networks the US relies upon to safeguard its national security and interests and domestic territory. The complexity surrounding the hacking of US military UAVs appears to be increasing, given the advancements in digital networks and the seemingly inauspicious nature of artificial intelligence and autonomous systems. Being most victimized by malicious digital intrusions, the US continues its military components towards growing dependence upon digital networks in advancing warfare and national security and interests. Thus, America's netcentric warfare perspectives may perpetuate a chaotic environment where the use of military force is the sole means of safeguarding its digital networks.

TABLE OF CONTENTS

CHAPTER

Introduction

In 2009 US Predator unmanned aerial vehicles (UAV) were employed in Iraq advancing US military operations. US military UAVs have operated within Iraq since the war began in 2003, as military proficiency in UAV intelligence gathering, reconnaissance, surveillance, and targeted killing increased (Scahill, 2016). However, US troops were frequently transmitting Predator drone video feeds over an unprotected network, which allowed enemy forces to intercept the video feeds and capture live full motion video through the Predator's camera sensors. US troops discovered the intercepted Predator video feeds on enemy computer laptops during later raids in Iraq. The information collected during the raids also showed that Iraqi forces were sharing the intercepted Predator feeds with enemy forces in Afghanistan and Pakistan (Villasenor, 2011; Gorman et al, 2009).

In 2011 a top-secret US UAV was captured by the Iranian military. The captured RQ-170 Sentinel has stealth capabilities and may have been flying in figure eight formations between Afghanistan and Iranian borders on surveillance missions. The apprehension method used by the Iranian military remains uncertain, but, the leading theory is that the RQ-170 Sentinel was captured by jamming its communication links, blocking its GPS coordinates, and spoofing its signals causing the RQ-170 to land in Iran. These malicious actions indicate that the Iranian military circumvented the Sentinel's encryption (Rogoway, 2016; Shashok, 2017; Loukas et al, 2017; Crampton, 2016; Hartman & Steup, 2013).

Lastly, in 2011 UAV ground stations located at Creech Air Force Base in Nevada became infected with a virus. The infection time period remains unknown to the public. The ground station operates Predator and Reaper UAVs employed within foreign battlespaces including Iraq. Military officials noted that initial attempts to remove the virus failed due to its persistent nature (Shachtman, 2011).

Moreover, US Army memorandums dated 8/2/17 and 5/23/18 terminated use of Dajiang Innovation (DJI) UAVs, all related DJI electrical components, and the use of all commercial off-the-shelf (COTS) UAVs, until their cyber vulnerabilities are resolved (Watson, 2017; Mortimer, 2017; Atherton, 2018). These memorandums were issued after DJI insisted that all UAVs not registered with their company will endure capability shortages in certain UAV functions. DJI is a Chinese company and controls much of the global commercial UAV market. US special forces have been using DJI UAVs in Syria and other battlespaces; and DJI's Phantom UAV has recently suffered GPS compromises by hackers (Watson & Tucker, 2017; Murphy, 2017).

The topic of this paper concerns various US military UAVs and the impact their vulnerabilities can have on US national security and interests. Specifically, this paper will address how malicious intrusions or hacking can influence the operation of US military UAV's during their domestic and international use. The complexity surrounding hacking military UAVs will also be addressed. As such, this paper will briefly consider Iraq, Afghanistan, and the United States as geographies where US military UAVs operate. The purpose of this research is to examine various ways to maliciously interfere with US military UAV's. This research will not consider all US military UAV or their systems, as their military use in general appears heterogenous and disjointed. In other words, each military branch has their own UAV program and does not operate under one single unified digital network (UNIDIR, 2017); and examination under those parameters exceed the intended length and scope of this research. Also, this research is not concerned with the ethical or legal issues regarding digital hacking, but views hacking from an objective lens.

Cross-pollination between commercial and military UAVs is done within this paper to further elucidate comprehension of the problem for the following reasons: Firstly, the interdependence/interrelationship existing between the civilian and military UAV markets; secondly, the US military's frequent use of commercial UAVs and thirdly, the theoretical extrapolation of commercial UAV hacking methods being applicable to military UAVS. Though this research notes some UAV types, its geographic scope will be limited mainly to Iraq, Afghanistan, and the US. This research assumes the examples of military UAVs presented serve as viable samples and accurate representation of the overall hacking picture concerning US military UAVs. As such, the researcher admits that drawing samples as representative of a larger relevant group has inherent flaws, but, given the military's use of commercial UAVs and the common network features, the researcher believes such inherent statistical flaws are minimized. Additionally, this research emphasizes the theoretical possibilities of hacking military UAVs, because the researcher is not a computer scientist; consequently, many technical hacking perspectives are within this paper are deemphasized.

The primary research question within this paper is how feasible is it to hack a US military UAV? Additional sub-questions concern:

1. How does hacking US military UAVs influence US national security and interests?
2. Why is the US military increasing its use of UAVs?
3. How are military UAVs being used within the military battlespace?
4. How does artificial intelligence factor in to military UAV hacking?
5. What countermeasures are the United States using to defend against malicious intrusions of their military unmanned aerial aircraft systems?

Moreover, this research binds UAV examination from the year 2001 to present. The significance of this research is paramount due to the continuing netcentric posture the US military is adopting, a posture aligned with the theoretical lens employed herein.

As such, this paper presents a unique perspective to the field and fills a perceived gap in the research because elements such as environment, motives, and interrelation respecting military UAV intrusions are analyzed. This approach appears scarce within the research. This paper will proceed with a literature review in section two. Section three will address the theoretical/methodology used within the paper, section four will concern findings/analysis, and section five will note general UAV/UAS environmental vulnerabilities. Section six will discuss motivations for hacking US military UAVs; section seven will discuss propositions. Section eight will briefly mention some national security and interest threats and section nine will state various emerging elements. Sections ten and eleven will discuss conclusions based upon the earlier presented material and recommendations respectively.

US military UAVs represent the standard for future weaponized aerial combat. For example, Navy Secretary Mabus stated that the F-35 will be the last manned war plane that the Air Force will produce, indicating that the UAV emphasis will supersede manned war planes in future aerial procurement (Whittle, 2015). This significant transition in air combat demonstrates the military's growing commitment to digital weaponized aerial platforms (GAO, 2018; Smith, 2016), which may assume an autonomous nature in the future and bring an unparalleled sophistication to a new generation of war planes. The complexity of modern and future warfare has yet to be fully understood, given the rapid rate of technological advances and the looming advent of autonomous applications to UAV platforms (UNIDIR weaponization, 2017).

As the US military transitions towards unmanned aircraft, the fluid nature of the battlespace will continue to challenge the most advanced military aerial fighters, due to uncertainties concerning digital networks. Despite the inherent vulnerabilities, wireless networks and UAVs are quickly becoming the backbone of modern warfare, as demonstrated by the controversial and popular use of the US UAVs on foreign battlefields in recent years.

US military UAV inherent vulnerabilities are receiving public attention, as hacking military and commercial UAVs have common weaknesses such as GPS systems, common data links, video data links, and human operators (Tippenhauer et al, 2011; Kwon et al, 2018). UAV vulnerabilities can be alarming due to the US military's reliance upon commercial networks in supplementing its bandwidth for UAV utilization (Kimball, 2015). Battlespaces in Iraq, Afghanistan, and Iran have already demonstrated the feasibility of hacking and capturing US military UAVs, demonstrating US enemy commitments to adapt to fluid battleground conditions dictated by American global technological and economic dominance.

Additionally, the US military's dependence upon UAVs is growing. Increasing digitization of advanced military weapons perpetuates complexity and weapon autonomy, which may introduce more vulnerability to US airpower and global dominance, despite the unparalleled sophistication advancing technology brings to future generation war planes. Therefore, the thesis within this paper is the US military's rapid conversion to, and the malicious intrusions of, military UAVs simultaneously presents the promise of continued global military dominance and inherent network vulnerabilities. This duality presents the US military unmanned aerial system on the edge of chaos (Fellman, 2010) and may lead to a compromise of US national security and interests.

Literature Review

The Department of Defense (DoD) is a complex bureaucracy (Niva, 2013) riddled with significant inadequacies concerning checks and balances on its advanced weapons systems. The DoD UAV programs are no exception. Government reports are seemingly constant in chastising the DoD for its shortfalls in properly managing UAV budgets, strengthening network vulnerabilities, and properly fielding UAV systems, while, simultaneously, recognizing the DoD's countermeasure efforts at such issues. However, since 2004, the DoD has not paid adequate attention to its UAV cyber security matters; and presently, it faces a growing challenge at keeping pace with the fluid nature of malicious intrusions attacking UAV platforms (GAO, 2004, 2018).

The DOD also faces security challenges regarding global proliferation of UAVs due to the potential dual nature of UAV technology/software applications (Fitzpatrick, 2014). Even the term "unmanned aerial vehicle" is ambiguous as it applies to various aerial platforms including cruise missiles (GAO, 2004, 2017). Though this research is not addressing cruise missiles, government reports clarify that the DoD is lagging in emphasizing cyber security for these instruments. Conversely, the DoD is making some efforts in securing the influx of counterfeit parts into its supply chain, which directly affects UAV operations. Their mitigation efforts are done through formal reporting by DoD employees and contractors, but supply chain complexities hinder adequate reporting, leaving the supply chain vulnerable (GAO, 2016; Edwards et al, 2015). Interoperability and bad weather are noted within government reports as partial points indicating the DoD's inability to utilize UAVs at their fullest capacity, this being noted after reports indicate the military has had significant success employing UAVs in foreign theaters (GAO, 2005; Fomichev et al, 2017).

The national airspace is emerging as the next great frontier for UAV operation, with the DoD on the vanguard of such employment (Jackson et al, 2008). Yet, challenges with UAVs in domestic airspace and national safety standards for UAV operations, regarding balancing citizen privacy, domestic security, and corporate endeavors remain obstacles for domestic UAV usage. These issues have warranted the Federal Aviation Agency (FAA), DoD, National Aeronautics and Space Agency (NASA), and other federal agencies' collaboration in domesticating UAVs (Elias, 2012; GAO, 2013; FAA Reauthorization Act, 2018; Electronic Frontier Foundation, 2012). UAVs are well established as the weapons platform most impacting change within the US military (GAO, 2006; NDAA, 2001, 2016), as its foreign and domestic use along US borders is increasing. These operations are also providing significant motivations for hacking military UAVs (GAO, 2010; Stepanovich, 2012; Jacobsen, 2015; Scahill, 2016; Coll, 2004, 2018). Budget constraints remain ominous in DoD planning. For example, the DoD was recently encouraged to increase investments in commercial satellite usage for its space systems, which aid UAV navigation, due to cheaper costs. However, the DoD has been challenged in technically knowing how to fully and safely implement its space and weapon platforms on commercial instruments (GAO, 2018).

Global threats to US national security and interests are present with the US military's future UAV ambitions. Potential threats may involve artificial intelligence and autonomous systems, as these driving forces may make the US economy more attuned to instability through the economics of warfare, decreasing UAV prices, and UAV technology proliferation.

However, the US military appears poised to meet resurfacing past and future threats through UAV utilization (Cunningham, 2015; Aspin, 1993), with the DoD's UAV budget increasing from approximately $1billion dollars in 2003 to $9 billion dollars in 2019 (Hartman & Steup, 2013; Gettinger, 2018; Bone & Bolkcom, 2003; Grose, 2016); but, the rapid pace of technological change is making cybersecurity a paramount issue. As DoD UAV procurement increases (Erwin, 2013), the network security surrounding these systems is increasingly raising alarm (Inspector General, 2018; Director Operational, 2016), especially given the Iranian capture of the US stealth UAV in 2011 and the current surge of Chinese and Russian cyber army/proxies units (Coates, 2017; Defense Intelligence, 2019; DoD Science Board, 2013; Shashok, 2017).

Lastly, other military UAV vulnerabilities are bad weather, human error, and electronic interferences. These issues have been leading problems with UAV functions since the early 2000s (Department of Defense, 2003; Thompson, 2005). Since that time, electronic warfare continues to take prime position in DoD attempts at mitigating UAV interferences (Marines Electronic, 2016; International Telecommunications, 2009). The DoD has planned a long-term strategy for UAV operation efficiency and network security as a partial response to malicious activity troubling unmanned aerial systems. The strategic plan extends to year 2042 and successful mitigation of UAV interoperability and human errors are key technical military objectives within the long-term plan (Unmanned Systems, 2017). The strategic plan regards the US military's global UAV operations. Other UAV vulnerabilities appear common within the literature, as general hacking techniques on commercial UAV can theoretically apply to military UAV platforms.

Thus, communication data links, video data links, navigational sensors aided by global satellite systems (GPS), and even encryption are all venues for attack by malicious intruders seeking to control and/or capture a UAV (Nassi et al, 2018; Davidson et al, 2016; Son et al, 2015). The literature appears abundant on various techniques used against these vulnerabilities regarding commercial UAVs, such as spoofing GPS sensors, password theft, man in the middle attacks (MITM), viruses, denial of service (DOS), deception of the UAVs neural network, sensor channel blocking, and injecting back doors (Tippenhauer et al, 2011; Hamsavahini et al, 2016; Rani et al, 2016; Rodday et al, 2016; Kwon et al, 2018; Li et al, 2013; Mozaffari et al, 2018; Suescun & Cardei, 2016; Gu et al, 2017; Nguyen et al, 2015; Loukas et al, 2017; Zhang, 2014). The DoD seeks to secure its UAV networks, as it also strives to advance swarm UAV network architecture under the belief that swarms provide more effective defensive and offensive measures during warfare. However, even UAV swarms possess vulnerabilities because they also rely on GPS or ground control stations, unless the swarm is autonomous. Autonomous platforms present another level of problems concerning hacking detection (Lachow, 2017; Yagdereli et al, 2015). Combating US military UAV vulnerabilities have been reduced to algorithmic warfare, as technology and the ominous nature of autonomous vehicles govern discussions concerning the US' utility of UAVs within a multi-domain dominance, including space (Crampton, 2015; Harris, 2018; Hall, 2006; United Nations, 2017).

Theoretical/Methodology

The theoretical framework employed within this research is complexity theory. Complexity theory emphasizes that a phenomenon is best comprehended as a living system in motion. As such, the phenomenon is viewed holistically (Bar-Yam, 1997; Stuart et al, 2015).

In viewing constructs holistically, complexity theory encourages analysis of phenomenon components as they relate to each other and their impact on their environment (Bar-Yam, 1997, 2018). Complexity presents systems as unstable and possessing tendencies existing on the edge of chaos; yet, the system maintains some degree of order through self-organization, giving the appearance of stability (Mason, 2009). Interdependence, interrelation, adaptation, exaptation, self-organization, and emergence are some elements observed under the theory, with successful application towards various fields of study, including the sciences, business management, mathematics and terror organizations (Bar-Yam, 1997; Fellman, n.d.; Anderson et al, 1999; McKelvey, 1999; Mason, 2009; Liang, 2013; Morrison, 2010; Mazzocchi, 2008; Kostlan, 1987).

Conversely, complexity theory does not encourage viewing a phenomenon by dissecting and analyzing its parts in attempts to gain understanding – reductionism. The reductionist approach is discouraged because the theory posits that system understanding is nullified when a system component is segregated and studied in a vacuum; in other words, the part does not equal the whole (Liang, 2013; Abraham, 2002). For example, the human body is a living organism consisting of vital organs, tissues, blood vessels, hair, neurons, and even smaller elements. Yet, present understanding and new discoveries of the human form, and its complexity, are continually generated by observing the body holistically, while considering its individual functions and their relation to each other and to their environment. Additionally, prediction is not encouraged under complexity theory due to system instability and environmental perturbations. In other words, it is unknown how a system will react or in what direction it will move when functioning within its surroundings; pattern behavior is unstable (Snowden & Stanbridge, 2004; Mason, 2009).

As such, this research views malicious intrusions of US military UAVs as a complex sub-system of the larger complex system respecting hacking commercial computer networks. This adjustment of scale will allow for greater understanding of the sub-system and its potential impact on US national security and interests. Lastly, the sub-system will be analyzed through four complex elements concerning, adaptation, resilience, interdependence/interrelation, and coherence (Snowden, 2011).

The methodology employed in this research is the qualitative explanatory case study. The qualitative method has favorable elements when used towards comprehending complex phenomenon. For example, the method allows generous degrees of subjectivity during examination, due in part to the method's embedded interpretative and explorative traits (Anderson & Pharm, 2010). This research posits that analytical generosity is necessitated by definitional and conceptual debates concerning malicious intrusions of US military UAVs. Moreover, the qualitative case study method provides amply examination liberty because the variable/case inequality can be significant (Hyett et al, 2014). For example, the variable/case inequality can influence the qualitative principles of transferability and validity, due to inadequate data on hacking US military UAVs, where U.S. government top secret classification plays a vital role. However, this research achieves transferability by relating US military UAV hacking to hacking commercial UAVs, thus, expanding the scale of the phenomenon; and validity (case falsification through other examples) is achieved by discussing more than one case, maintaining a logical movement through the paper, and theoretically defending causality between variables.

Validity is supported through the broad scope enveloping the data collection, as this research's data rests on government documents, some newspaper articles, international documents, military manuals, and books. Original sources were emphasized in the research, which furthered source evaluation through multiple data angles (triangulation). Themes and patterns were uncovered through triangulation, which presented independent variables respecting DoD, hacking, and the US. Dependent variables involve military digital networks, network vulnerabilities, weapons systems, UAVs, drone crashes, and the countries of Iraq, and Afghanistan. This research defines the qualitative case study as a spatially bound phenomenon analyzed through interpretative, historical, and/or descriptive perspectives under a given time period (Yin, 1981; Hyett et al, 2014). This definition is given to avoid the definitional problems inherent with the qualitative case study method, as some critics claim the method is not distinguishable from a simple narration, note-taking, being data disciplined under a strict timeline, or as simply being too vague (Yin, 1981; Jones, 2003; Lock & Seele, 2018; Harrison et al, 2017). Lastly, validity is also supported in the Analysis/Findings section of this research. This section commences with a formal problem statement concerning the phenomenon, which will guide the focus throughout the paper. The phenomenon's context will be discussed afterwards, which will concern past and current data before proceeding to four propositions evaluating the complex elements concerning hacking US military UAVs. This research will bind its examination to a time period between 2001 and present day to also aid the focus. Moreover, this research promotes transparency, reliability, and replication based upon the source listing, and it provides accessibility for increased evaluation through the material. An exact match of conclusions is not fully expected during replication attempts, but this research does contend that similarity will be achieved.

Analysis/Findings

Problem

Malicious intrusion of US military UAVs appears to be slowly emerging as a countermeasure used by US enemies in foreign battlespaces. Thus, the intrusions could serve as a template for further global and domestic anti UAV operations, particularly, as the domestic US airspace is rapidly moving towards integrating UAVs for commercial and law enforcement endeavors. Currently, the DoD is on the vanguard of standardizing UAV use within the US. However, successful hacking of military UAV platforms presents unprecedented danger to US troops, due to UAV weaponized payloads and the theft of sophisticated UAV technology through reverse engineering, which can promote unintended weaponized UAV global proliferation.

Context

Brief History of US Military UAVs: Elias (2012) traces US military UAV history to the early 1950s. During that time, flying drone experimentation was joined with aerial target simulations, which later led to the Hewitt-Sperry Automatic Airplane or the Curtiss-Sperry Flying Bomb, these projects served as protypes for future UAVs. However, these experimentations also initiated development in flying munitions, commencing the present ambiguity between unmanned aerial vehicles, unmanned aerial aircraft, and cruise missiles (Suescum et al, 2014). The 1960s and 1970s witnessed developing military UAV surveillance in Vietnam (Erwin,2013). Israeli UAV applications in the Middle East further stimulated American interests during the 1980s, as their capabilities influenced US federal agency creations dedicated to UAV management (Erwin, 2013). By the 1990s Gulf War, UAVs became a component of an aerial system providing high resolution surveillance in enemy territory, as this war showcased current practices of prosecuting war from space-based systems (Erwin, 2013; Elias, 2012).

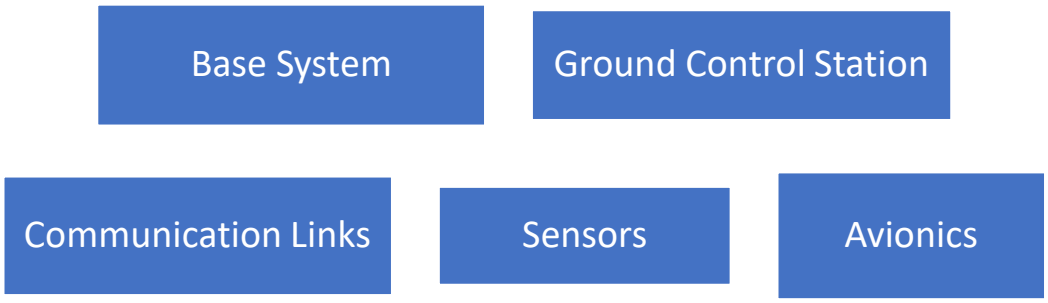
Future wars in the former Soviet Union continued UAV operations, as current Middle and Far East regions experience the most military UAV operations to date. The DoD aids the Federal Aviation Administration (FAA), Department of Homeland Security (DHS), National Aeronautics and Space Administration (NASA) and other federal agencies in normalizing UAV standards for US homeland use among corporations and law enforcement (GAO, 2012, 2013; DIA, 2019). Currently the Islamic State and Hezbollah are engaging cyber warfare and UAVs against the US in foreign battlefields (Carroll, 2008; Sly, 2018).

UAV Definition/General Types: The dynamically remotely operated navigation equipment (DRONE) is a term which inadequately reflects the present complexity of US military UAVs (Hamsavahini et al, 2016; Howard, 2013). Therefore, the ambiguity enveloping the term "drone" can represent unmanned aerial vehicles and/or munition functioning in US air, land, sea, and space battlegrounds. Also, the term "UAV" appears synonymous with unmanned aerial aircraft (UAA) and unmanned aerial system (UAS). The unmanned combat aerial vehicle (UCAV) symbolizes weaponized UAVs (O'Rourke, 2006). However, this research defines the UAV as aerial vehicles with autonomous potential, no human carrier, and abilities of remote or self-control. UAVs employ lift and can possess various sensor and weaponized capabilities (Bone, 2003; Shashok, 2017). UAVs can be grouped by altitude - (with extensive coverage, loitering, average 10-mile altitude features), and by type - rotary wing (hover, slow, reduced flight time), or fixed wing (small, fast, payload, hours in flight) (Mozaffari et al, 2018). There are currently four general types of UAVs: (1). Nano type: The smallest UAV which can vary in weight starting from 2 ounces and wing spans of a few inches or less. These models replicate insects and are developed by the Defense Advanced Research Projects Agency (DARPA).

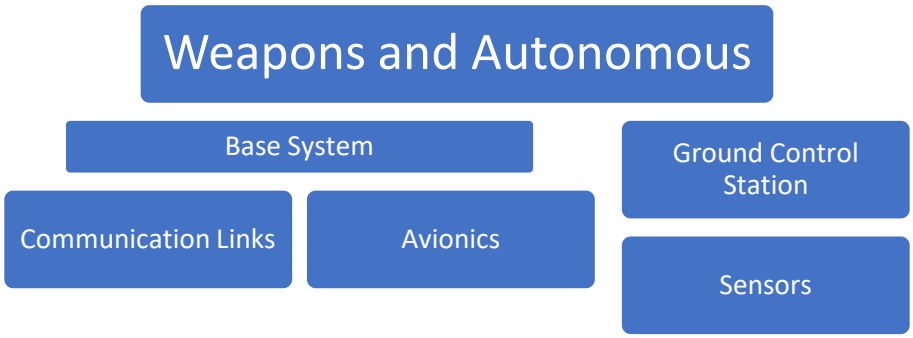
According to Jacobsen (2015), this type of UAV was spotted by war protesters in Washington D.C., as protestors were alarmed by three dragon fly like vehicles flying nearby, displaying a unified mechanical movement. Nanos are controlled through ground stations or possibly hand-held devices. (2). Micro-Air Vehicle (MAV): These are very small UAVs capable of video feeds through sensors while controlled through ground stations or remotes. Their autonomous behavior is possible. MAVs can reflect the sizes of various birds (Hamsavahini et al, 2016). The US Air Force's Wasp III Microdrone is an example weighing 14 pounds, with a ten-inch length, and operates at altitudes of approximately 1,000 feet (Air Force, 2007). (3). Man-Portable: A UAV operated mainly by ground forces. It is controlled through communication data links and a ground station. Man-portables possess an omnidirectional antenna and its control can be shared through handshake protocols. An example of a man-portable UAV is the RQ-16 Tarantula (Yochim, 2010). (4). Tactical UAV: The larger than man-portables class of UAV which show take-off by pneumatic catapult or by its own abilities. They require more intense ground station control and can land as manned aircraft. Tactical UAVs can use line of site communications (LOS) or beyond LOS. The Warrior Grey Eagle serves as an example flying at 29,000 feet (Yochim, 2010; General Atomics, n.d.).

US Military UAV Infrastructure: The UAV infrastructure is generally termed "unmanned aerial system" (UAS). It comprises a base station, ground control station, and communication systems. The base station unites the UAV with the ground control station (a form of pilot housing) through communication links. Pilots manage UAV mission and launch recovery issues within the ground station. Communication links provide data transmission, and UAV sensors gather environmental data. Avionics address UAVs flight capabilities, and GPS satellite systems aid UAV navigation when beyond line of site (LOS) is used (Kwon et al, 2018).

Basic Unmanned Aerial System



Advanced Unmanned Aerial System



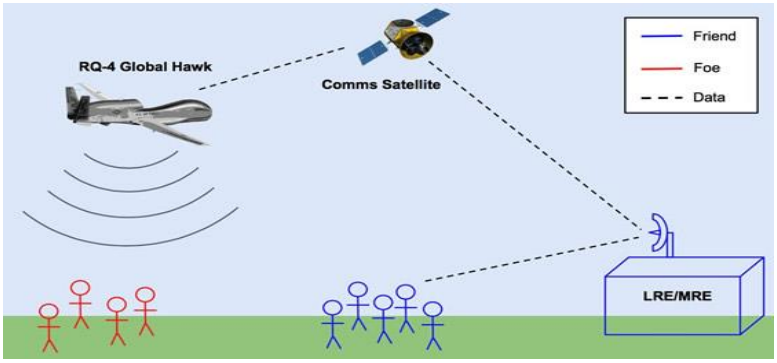
UAVs use omnidirectional antennas, which expands UAV command abilities, or directional antennas, which only grants communication in the direction towards the ground station (Hartman & Steup,2013; Yochim, 2010). UAV sensors relay data to the ground station. Internal sensors include the accelerometer, tilt functions, gyroscope, and inertial which address UAV stability and navigation. External sensors concern cameras and satellites (Cuadra et al, 2014; Suesun et al, 2014; Shashok, 2017; Winkler, 2016). However, the communication links and the GPS sensors will be further discussed due to their prominent vulnerabilities.

Data links are defined as channels though which components can communicate with each other and are essential to UAV operations. They provide battlespace data and image transmissions back to ground stations for analysis (Li et al, 2013). Common data link (CDL) was developed in the early 1990s for the US military. It normalizes wide-band LOS for the UAV system and has been a key venue for image and signals data (Li et al, 2013). Spin-offs of CDL are the Tactical Common Data Link (TCDL), which allows UAVs to send intricate data to the ground station (Hartman & Steup, 2013). TCDL was formed by the military and has a secure (encrypted) Ku band use during communications. It utilizes omnidirectional and directional antennas and has versatility in data transmission (Hartman & Steup, 2013). Link–11 is used by the North Atlantic Treaty Organization (NATO) and US naval forces. It has efficient data exchange between aerial, ship-based, and land-based vehicles. Link – 16 is the most popular link used by US aerial vehicles and employs the Joint Tactical Information Distribution System (JTIDSD) as its operation channel. This link is common with UAVs (Li et al, 2013; Zhang & Yang, 2014). Moreover, the Micro Air Vehicle link (MAVLink) is a header-based packet system which engages back and forth packet exchanges as its means of communication. MAVLink's common use concerns smaller UAVs controlled by the ground station and it does not employ encryption due to encryption protocols altering the header message, which confuses the MAVLink's packet header reading (Kwon et al, 2018). Other military data links are Situational Awareness Data Link and the Variable Message Format (VMF) (Trevithick & Rogoway, 2018). Military satellite communications utilize various frequencies.

They involve satellites dedicated to commercial activity, Extremely High Frequency (EHF), Ultra High Frequencies (UHF), and Super High Frequency (SHF). EHF and SHF have global reach and are secure. They cater to military and civilian entities**,** as EHF supports military management of troop activity. The global broadcast system is a subset of SHF. UAVs utilizing this frequency present one-way transmission (Naval Studies Board, 2005). Additionally, the Air Force employs its own satellite space system called the Advanced Extremely High Frequency System (AEHF) consisting of 5 satellites; 3 were launched in 2010 (McCaney, 2015). Lastly, the Milstar is a DoD system constituting 6 satellites, the last being launched in 2003. Satellite operations decay over time; therefore, the Wideband Global SATCOM system, with a data rate capability of 2.1 to 3.6 gigabytes per second, is due to replace Milstar soon, as its data rate abilities hover around 75 bits – 1.544 megabytes per second. Milstar has been operational since 1994 (Erwin, 2018; McCaney, 2015). The Defense Satellite Communications System III (DSCS) operates at approximately 200 megabites per second since 1982. Of its original 14 satellites, 8 remain operational since 2015 and the military engages this system frequently (McCaney, 2015). The DoD received additional satellites for its DSCS III in 2018, with a congressionally authorized $600 million for a Boeing contract. The DSCS is more efficient in data transmission and bandwidth use than previous satellite systems (Erwin, 2018). Today, approximately half of the US aerial munitions are GPS reliant (naval Studies Board, 2005); but the military is challenged with UAV bandwidth availability due to the high quantities necessary for UAV data exchanges with ground components (GAO, 2005; Naval Studies Board, 2005). Having discussed the UAV infrastructure, the UAV network will be briefly presented.

US Military UAV Transmission Networks: Wireless networks are designated as 802.11 and may use various transmissions rates.

This standard applies to both commercial and military Wi-Fi or WLAN communications. Wi-Fi (a, b, g, n) transmit between 2.4 GHz – 5.75 GHz. Higher transmission stems from the n medium, as it can use more than one antenna for transmissions. B and g mediums are free to use but are inefficient due to heavy usage (Hartman & Steup, 2013). UAVs operate by radio frequencies and require video data links and common data links to operate fully. WiFi and ZigBee are mainly used for data transmissions between the UAV and the ground station (Kwon et al, 2018; Hartman & Steup, 2013).



Source: Cunningham, 2015

Generally, military UAV communications are encrypted during transmission over the wireless network but applying encryption to UAV communications presents further expenses and complexity (Yagdereli et al, 2015) to the UAS. Military UAV bandwidth use is challenged by crowding airspace when attempting to transmit various data (Howard, 2013). Larger military UAVs have default systems which are engaged during technical problems. For example, pre-programming default commands within the UAV supplements interference countermeasures. Therefore, the UAV may hover, attempt ascertaining another data link to restore communication with the controller, return to base, or crash (Yagdereli Et al, 2015). The Industrial, Scientific, and Medical (ISM) 2.4 GHz band is the most common band used for UAV transmission.

It comprises a group of frequencies between 915Hz and 5.8GHz. Its utility is economical due to its abundant range, and no license requirements. Yet, there are concerns surrounding overuse of these frequencies (Electronic Code of Federal Regulations, 2019; Herman, 2010).

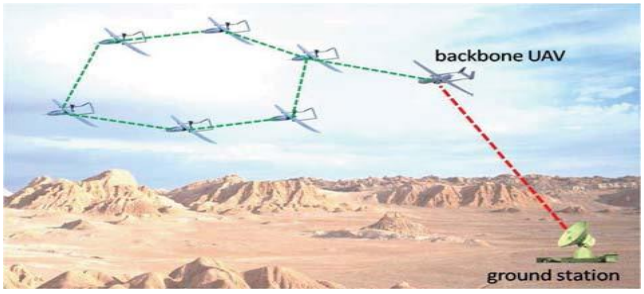
The swarm transmission network varies the basic UAV network arrangement. They can represent four basic formations. The first is a centralized network formation where the arrangement reflects all UAVs communicating with the ground station.

UAV Centralized Network

Source: Li et al, 2013

Second, the UAV ad hoc network comprises 1 UAV as the prime communicator between the ground station and the remaining UAVs. This network is suitable for UAV single formations.

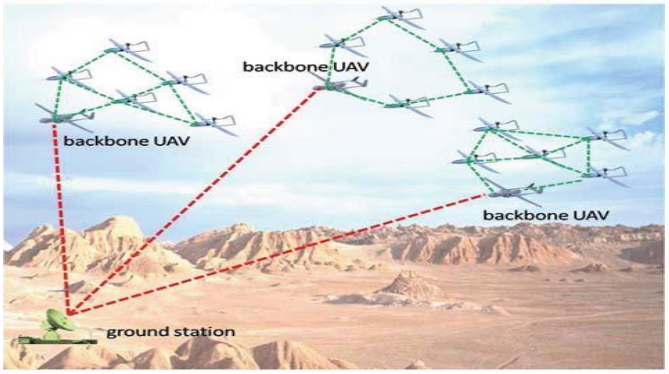
UAV Ad Hoc Network



Source: Li et al, 2013

Third, the UAV multi-group network utilizes more than one UAV to serve as communication hubs for the remaining UAV swarm members.

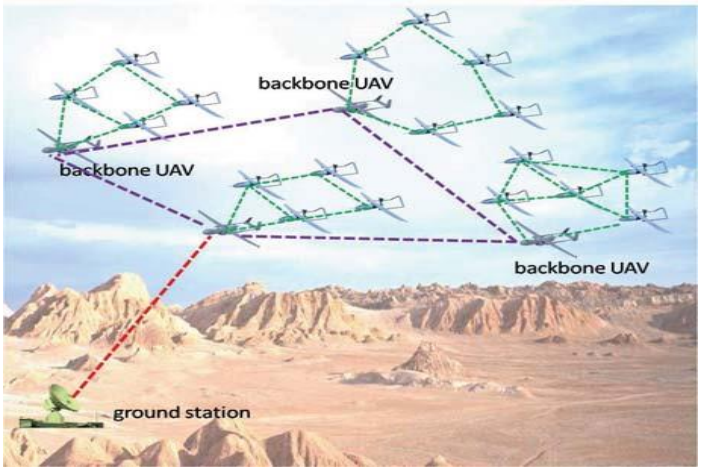
UAV Multi-Group Network



Source: Li et al, 2013

Fourth, the UAV multi-layer ad hoc network consists of more than one UAV serving as communication hubs, but only one UAV hub is communicating with the ground station (Li et al, 2013; Suescun et al, 2014).

UAV Multi-Layer Ad Hoc Network



Source: Li et al, 2013

Multi-group and multi-layer networks are suitable for UAVs swarms operating separately. Uni-point networks concern the UAV multi-layer ad hoc and the UAV ad hoc networks, which allow for greater operational efficiency than the other swarm network types.

However, multi-hop data relay capabilities are possible through decentralized networks, as the centralized UAV network presents some transmission inefficiency due to distance ratios between the ground station and the UAV (Li, et al, 2013). WiFi, ZigBee, GPS, Bluetooth, and infrared are wireless mediums frequently used in UAV networks. Military UAV swarms have proven formidable offensively during military simulations, as they were found indefensible (Lachow, 2017). A real-life example of a UAV swarm attack occurred in Syria in 2018, when a Russian military base was attacked by a swarm of miniature weaponized UAVs. The base suffered heavy damage before the UAVs were either manually shot down or were disengaged using electronic warfare. Russia suspects US involvement in the attack due to a US Poseidon reconnaissance vehicle hovering in the skies nearby during the conflict (Sly, 2018).

US Military Uses for UAVs: US military UAV ambitions increased significantly in 2001 (National Defense Authorization Act, 2001, 2006; GAO, 2005; Unmanned Systems, 2017) as the military's primary goal appears to create a hybrid military system using UAVs as compliments to traditional DoD battlefield and space elements. Thus, the DoD has worked towards making 1/3 of their aerial and ground vehicles unmanned since 2001 (National Defense Authorization Act, 2001; Defense Intelligence, 2019). The DoD's 2019 monetary request for drones and their supplemental architecture is approximately $9 billion. Naval and Army monetary requests for unmanned aerial systems have risen by 38% and 73% respectively; and DoD request for the MQ-9 Reaper UAV increased from $1.23 billion to $1.44 billion between fiscal years 2018-2019 (Gettinger, 2018). Naval UCAV programs gather intelligence, conducting surveillance, and reconnaissance missions. UCAV operations also entailed enemy aircraft countermeasures (O'Rouke, 2006).

UAVs do not have human needs, as sleep or hunger, and can hover for extended periods; they can also supplement ground forces by providing advanced visuals of enemy positions at great distances and provide intelligence necessary for war planes. Presently, military UAVs are conducting aerial surveillance and targeting killings in global battlespaces (GAO, 2005; Congressional Report Service, 2010).

Civilian Use for UAVs: Private companies have utilized UAVs for healthcare management and telecommunications. UAVs are also used for farm evaluations, traffic surveillance and commercial photography. Major corporations as Amazon and Google seek to implement UAVs within their daily operations; specifically, these companies seek to use UAVs for their delivery services which will increase the scale of their business functions (GAO, 2013; Villasenor, 2011; Rani, 2016). The Teal Group (2018) estimates the civilian UAV market to reach $89 billion in the next decade. Law enforcement use of UAVs appears the most controversial because many Americans perceive domestic law enforcement's UAV use as a potential increase in lethality towards the US population. However, federal law enforcement UAV operations for southern border security, surveillance, and as first responder complements are growing. Increased civilian desires to use UAVs within the US is necessitating a political, economic, and social infrastructure regulating safe UAV operations within the US airspace. As such, the DoD, Congress, FAA, and other federal agency partners are working to establish and fortify a UAV infrastructure within the US. This domestic UAV network continues to face implemental challenges due to its theoretical compatibility with traditional domestic airline industry (GAO, 2013; FAA Reauthorization Act, 2018).

Foreign Battlefield/Domestic Operations: US military UAV programs remain classified (Mazzetti, 2012). However, the UAV program has been known as the US' worst kept secret, as the program's global impact remains difficult to hide (Coll, 2004, 2018). For example, from 2009-2016 Somalia has had 32-39 drone strikes with 242-454 reported killed and 3-12 civilian deaths. In 2016, Pakistan had 3 drone strikes, with 11-12 reported kills, and1civilian death (Bureau of Investigative Journalism, 2017). In 2016, Yemen had 38 strikes with 147-203 reported killed and 0 civilian deaths. Moreover, between 2015 and 2016, Afghanistan had 1306-1307 UAV strikes, with 2371-3031 reported killed, and 125-182 reported injured (Bureau of Investigative Journalism, 2017). UAV statistics on Iraq are uncertain (Purkiss & Serle, 2017). The domestic U S airspace is currently an experimentation field for some military UAVs as Customs and Border Patrol are assisted by the DoD in UAV surveillance (Congressional Research, 2010; FAA Reauthorization Act, 2018). The Air Force and DARPA have conducted surveillance in Virginia Beach and California using the Scan Eagle and the Boeing A160 Hummingbird (Mazzetti, 2012). The Air Force has used the Reaper UAV in Nevada and Utah, which employs a UAV with a 9-camera array for capturing city-wide images, later to be analyzed by artificial intelligence. Also, the US Navy joined two federal agencies and local law enforcement in Maryland to use a UAV for surveillance of criminal activity (Mazzetti, 2012). UAVs are becoming a dominant instrument within the DoD's weapon systems portfolio (Smith, 2016). For example, the MQ-Reaper has seen a twofold increase in utilization by the Air Force between the years 2010 and 2015; moreover, the Air Force in the following year possessed 93 Reapers and 150 MQ-1 Predators among their 2016 weapons systems.

Not to be out done, the Army's 2016 weapons portfolio contained approximately 130 MQ-1C Grey Eagles UAVs, and other military branches have smaller non-weaponized UAVs totaling in the hundreds (Smith, 2016).

US Military UAV Crashes: US military UAVs crash frequently (Thompson et al, 2005; Bone, 2003). Often the crashes are due to technical failure such as lost communication links or insufficient fuel (Cuadra et al, 2014); and Yochim (2010) indicates that UAVs terminate flight 100 times more than manned aircrafts. UAV performance remains imperative to DoD military operations and applying proper remedies to operational challenges perpetuates intense UAV production evaluation (Department of Defense Unmanned, 2003). The US has initiated monetary rewards in Iraq and Afghanistan for the return of their crashed UAVs for fear of enemy forces learning the aerial technology (Yochim, 2010). Domestic UAV crashes have also occurred. For example, in 2006, Customs and Border Patrol in New Mexico lost an MQ-9 Predator UAV in a crash; and in 2012, Maryland witnessed a Navy RQ-4A Global Hawk crash. In 2014, Pennsylvania witnessed a RQ-7 Shadow crash. The Shadow weighs approximately 375 pounds with a wing span of nearly 16 feet (Elisa, 2012; NBC, 2014). Some UAVs are the size of small aircrafts and their demise presents significant danger to populations below (Elisa, 2012). Having considered some contextual elements for malicious intrusions of US military UAVs, a general view of UAV vulnerabilities is warranted.

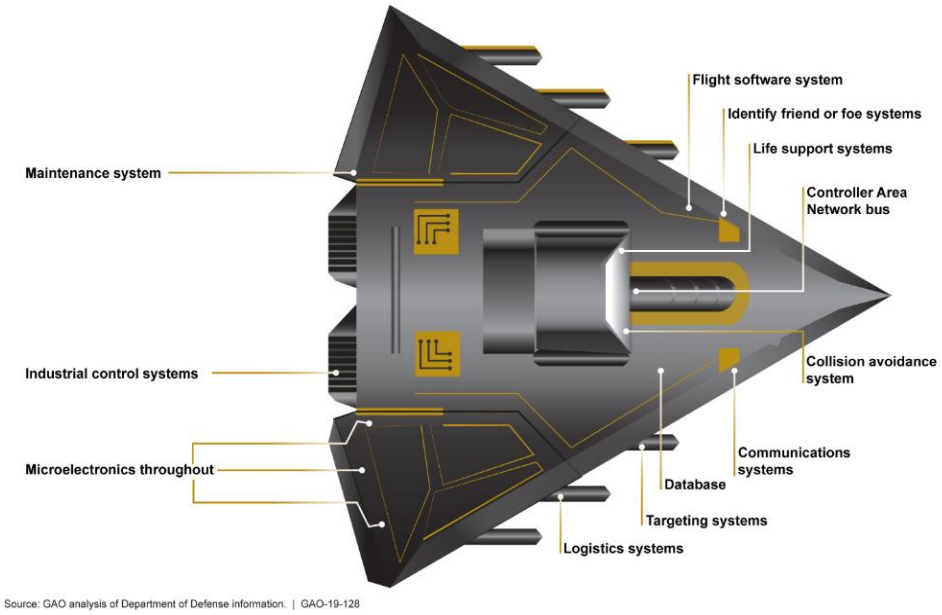
General US UAV/UAS Environmental Vulnerabilities

The US government remains high among countries victimized by digital malicious intrusions (Director Operational, 2016), and the military's UAV systems are not excluded. The Director of Operational Test and Evaluation Agency (2016) is responsible for significant cybersecurity testing for the DoD weapon systems.

In their recent report, it was noted that weapon systems under analysis proved inadequate in defensive measures against malicious intrusions and the agency was encountering additional system faults. Furthermore, inadequate DoD supply chain security presents opportunity for counterfeit parts (GAO, 2016) to inject back door intrusions into UAV technology (UNDIR Weapon, 2017). The DoD's policy requiring contractors to report counterfeit parts to the government remains without unified standards and has been wanting for years (GAO, 2004; GAO, 2016; Keller, 2018; Villasenor, 2011; Edwards et al, 2015). The growing complexity of related UAV parts also presents vulnerabilities due to the short life cycle inherent to many digital components (Edwards et al, 2015). The DoD's UAV infrastructure is significantly networked and can extend to other unsecured networks or electrical components, further extending network vulnerabilities (GAO, 2018; GAO, 2004). The GAO (2018) and the DOD Inspector General (2018) recently informed the DoD of their negligence towards cyber security regarding major weapon platforms, as it was discovered that some weapon systems testing demonstrated successful hacking of passwords and unencrypted data. The GAO's (2018) conclusions rests upon the fact that Military UAVs represent flying computerized platforms, just as their commercial counterparts (Rodday et al, 2016); as such, they face similar network vulnerabilities as laptops and cell phones under the proper circumstances (Defense Science Board, 2013; Director Operational, 2016). Artificial intelligence and autonomous applications to weapon platforms are not fully understood and are theorized to move too far ahead of human reasoning (UNIDIR, 2017; Allen & Chan, 2017).

Military UAV components and software stemming from commercial vendors remains suspect due to insufficient security protocols during production (Defense Science Board, 2013; UNIDIR, 2017). Congressional budget constraints are pushing the DoD towards creative measures in reducing costs during UAV production and procurement. Consequently, the DoD has become dependent upon commercial off the shelf (COST) UAVs and supplemental parts (GAO, 2018; Villasenor, 2011). Inadequate security protocols during commercial UAV production introduces more vulnerability to DOD aerial weapon systems (GAO, 2018; Brynes, 2014; Howard, 2015), and UAV interoperability and interconnectivity are problematic for DoD UAV/networks, because most UAV systems have hardware and software proprietary issues, presenting some corporate competition and legal barriers to defense contractors, DoD UAV procurement, and anti-hacking countermeasures (Unmanned Systems, 2017: GAO, 2018; Grose, 2016; Fomichev et al, 2017). Additionally, US military UAVs are increasing in technical and performance complexity, as their production regards systems of systems – abilities to add increased technical sophistication to current and/or new military UAVs in attempts to preserve US military technological superiority, while making enemy acquisition of the same technology economically unattainable (Jones, n.d.). This production approach rests on making competing algorithmic systems compatible in foreign and domestic arenas. The DoD's inability to achieve interoperability and interconnectivity furthers UAS vulnerabilities because it reflects the perpetuation of individual corporate proprietary challenges, along with a heterogenous UAV environment which can be more difficult to defend against cyberattacks (Unmanned, 2017; Coates, 2017; International Telecommunications, 2009).

Decreasing bandwidth, due to competing aerial applications, is infringing upon UAV domestic use (Hall, 2006); and contested battlefields present further military challenges because the DoD must control sections of foreign airspace in order to ensure UAV success in military operations (Harris, 2017; Crampton, 2016). Inadequate bandwidth challenges appear to encourage greater use of commercial satellite systems (GAO, 2018; Aspin, 2003), which generally are not encrypted. If bandwidth vulnerabilities continue, then military UAV beyond line of site (LOS) will be compromised. Thus, the commercial/military nexus regarding digital parts and networks is appearing interdependent. For example, some military technology makes its way back to the commercial market in altered forms, such as the Humvee vehicle, night vision, and the UAV itself as its very early use constituted a hot air balloon with munitions (Comen, 2017). Growing consumer/military interests in digital components, such as smart phones, laptops, and cameras are driving computer-oriented item prices down, while increasing their proliferation with continued interests in wireless communication protocols (GAO, 2018; Howard, 2015). Moreover, UAV loitering capabilities leave the UAV exposed to malicious intrusions due to its stationary position. The UAV at rest presents the attacker with time to exercise any chosen penetration method towards the network and UAV sensors. The loitering vulnerability is heightened when the drone is fully autonomous, due to nullification of human surveillance of the network, as autonomous features may choose various conclusions unknown and unrelated to human interests in seconds (UNIDIR, 2017; GAO, 2017). The average military UAV has a broad vulnerability spectrum if manipulated correctly (Son et al, 2015; Davidson et al, 2016; Nassi et al, 2018).



Potential threats to UAV system

Security Objectives	System Objective	Attack Method
	GCS	Virus
		Malware
Confidentiality		Keylogger
		Trojans
	UAV	Hijacking
	Communication link	Eavesdropping
		Man in the middle
-	-	-
Integrity	Communication link	Packet injection
		Replay attack
		Man in the middle
		Message deletion
-	-	-
	GCS	Denial of service
	UAV	Fuzzing
Availability	communication link	Flooding
		Jamming
		Buffer overflow

Source Kwon et al, 2018

However, a brief survey of the known general battlefield UAV vulnerabilities can establish motivations respecting why US enemies desire to maliciously intrude US UASs. Some motivations are listed below.

Motivations for Hacking US Military UAVs

US hegemonic attempts in foreign regions are unacceptable to countries targeted by US UAV operations (Fitzpatrick, 2014). Moreover, the accuracy of UAV target acquisition is questioned, as shown during Operation Haymaker in Afghanistan, where most targeted killings were inaccurate (not legitimate). In one example by Scahill (2016), only 40 legitimate killings occurred from a given 200 UAV targeted killings during the entire campaign. The US military's UAV international battlespaces are also controversial and produce many innocent civilian deaths (Purkiss & Serle, 2017). Additionally, US military UAV operations are occurring within countries where the US has not declared war (Niva, 2013), as the US has approximately 76 global active covert war fronts for counterterrorism operations (Costs of War, n.d.). The Obama administration's legal justification for targeted killings of Americans on foreign soil raised questions about the policy's domestic application (Office of the Attorney General, 2010; Scahill, 2016; Jackson et al, 2008). Furthermore, domestic commercial and law enforcement UAV use is increasingly raising concerns regarding privacy and individual rights. Militarization of local law enforcement- supplying police with UAVs and other military weapons, is creating concerns about the US becoming a police state; as the growing netcentric warfare construct, or a collection of information networks containing nodes linked electronically (Niva, 2013), appear to advance among local law enforcement (GAO, 2013; Stepanovich, 2012). Having discussed hacking motivations, the following propositions will briefly discuss the complexity surrounding malicious intrusions of military UAVs. The propositions are interrelated.

Proposition #1

The malicious intrusion of military UAVs is a sub-system of the overall hacking of commercial computer networks, including commercial UAVs. As such, malicious intrusions of military UAVs have an adaptative nature.

Adaptation is defined as phenomenological development of traits for a situation or purpose (Snowden, 2011). The data concerning how often commercial digital systems are hacked is disjointed and too voluminous for digestion. Information concerning malicious intrusions of US military UAVs is scarce or non-existent due to its classified and covert status. Nevertheless, it has been recently shown that modern commercial vehicles, such as cars, can be hacked based upon their digital vulnerabilities. (Loukas et al, 2018). For example, recently a Telsa Model S was successfully hacked through its key fob by using a cell phone and a computer, accessing the vehicle's network. Once the car's computer network is accessed, control of the brakes and engine were possible. In 2015, experimentation demonstrated hacking a Jeep Cherokee through a laptop from approximately ten miles away, while taking complete control of the vehicle (Greenberg, 2015). These actions were accomplished by accessing the car's network through the key fob, Bluetooth, or other associated wireless units (Blum, 2018; Yaghereli, et al, 2015). In principle, US military UAVs are no different (Leopold, 2014), as their wireless network or human error leaves the UAV vulnerable to cyberattacks. Some common hacking techniques used against commercial UAVs in the US homeland are spoofing, jamming, man-in-the-middle attacks, trojan horse viruses, distributed denial of service, and application of various hacking software designed specifically for aerial vehicles.

Advanced techniques concern exploiting UAV deep neural networks, zero-day exploits, and triggering flash events through back doors or accidentally through algorithm mergers/conflicts (GAO, 2012,2013; Zhang & Yang, 2014; Vakin, Shustov, and Dunwell, 2001; Gu et al, 2017; Nguyen et al, 2015; UNIDIR, 2017 weaponization; UNIDIR, 2017; Rani, 2016). These same techniques apply to US military UAVs.

The UAV satellite component within the UAS is vulnerable to spoofing. Spoofing satellites occur when the attacking signal recognizes and conforms to the legitimate GPS satellite signal conditions. However, the attacker's signal has falsified satellite coordinates, which are used to deceive the satellite (UNIDIR, 2017). Spoofing is more difficult to counter due to its conformity to legitimate satellite communication specifications (Shashok, 2017). Electronic jamming is a lesser type of malicious intrusion than spoofing, due to its incompatibility with the target satellite communications protocol (Shashok, 2017). However, they are related. Jamming is done by simply injecting noise at the target sufficiently to disrupt the target's communication abilities. Broadband, tone, and swept are the three basic types of jamming. Broad band jamming occurs across multiple frequencies. Tone jamming involves concentration against a single frequency, and swept jamming happens when a single target frequency and its immediate context frequencies are disrupted through noise (US Marines, 2016; Yochim, 2010). Jammers are easily purchased over the internet but remain difficult to use against military UAVs due to the UAV's constant motion; thus, the jammer and target must be in relative near proximity (Zhang & Yang, 2014). Jamming and spoofing techniques can be used jointly against a target (Vakin, Shustov, & Dunwell, 2001).

Man-in-the-middle-attacks (MITHM) occurs when the attacker interjects himself between two parties by exploiting their communication link (Easttom & Taylor, 2011), and Trojan Horse viruses disguise their identity from the target network in order to perform its intended malfeasance. For example, the virus infecting UAV ground control systems at the Creech Air Force Base was a keylogger virus. Thus, for an unknown period the computer keystrokes performed by UAV ground controllers were sent to the virus user. Distributed Denial of Services (DDOS) involves overwhelming a target network with data packets with the goal of rendering the target system unusable (Panko & Panko, 2015).

Popular computer software used for hacking UAVs involve Sky Jack and Sky Grabber. Sky Jack operates through a host UAV and is used to hunt other UAVs. It overcomes the proximity need during the UAV hacking process. Sky Jack can take complete control of the target drone by sending de-authentication data to the target and coerce the target into believing its true owner has disconnected use (Shashok, 2017). The program will then authorize the target UAV to allow attacker control. However, Sky Jack is only successful on limited small UAV models (Shashok, 2017). Sky Grabber was developed by Sky Software, a Russian company whose main aim was to intercept internet products. The company appeared surprised at the program's UAV application (Gorman et al, 2009). Some more advanced and theoretical measures in hacking military or commercial UAVs can be through zero-day and neural network exploits. Zero-day exploits regard manipulating the software operating system vulnerabilities. Zero-day exploits can rest undetected within target networks for years. The Stuxnet malware, which was used against an Iranian nuclear facility and resulted in physical destruction of its centrifuges, is a zero-day exploit.

The malware had to be injected into the proper network through human participation – disc or flash drive, to initiate its payload (UNIDIR weapon, 2017). Zero-day exploits could be initiated during UAV production cycles by American or foreign private companies, given the DoD supply chain vulnerabilities.

Exploiting a UAV's deep neural network involves deceiving the UAV's image dictionary by the target altering his image. For example, New York University demonstrated that if a traffic sign was slightly altered by placing a post-it note on the sign, then the roadside sign detector's neural network was unable to recognize the object as a road sign, despite its preprogramming (Gu et al, 2017; Nguyen et al, 2015). The university program also noted that backdoor injecting of neural deception can be achieved when software is temporarily managed by outside contractors (Gu et al, 2017; Nguyen et al, 2015). This research states that the New York study can apply to US military UAVs. For example, a target can slightly alter or disguise its image if it believes it is under military UAV surveillance. The image alteration, with changes in daily routine, may be adequate to deceive the UAV's neural network and complete the intended hack of the UAVs image pre-programming. Given the zero-day and neural network exploits, the opportunity for algorithms to conflict while systems are performing autonomously are significant. For example, a US military UAV swarm could have algorithm conflicts during autonomous operations because of inadequate interoperability protocols. The algorithm conflict could endanger the entire swarm and or cause one or more weaponized UAV to exhibit rogue behavior. Algorithm conflicts within UAVs can also be initiated during the UAV development life cycle by contractors or through UAV foreign electronic parts procurement. The resulting behavior (flash trigger event) is unknown and unpredictable.

The Predator UAV hack in Iraq in 2009 was discovered through ground raids conducted by American forces which found enemy laptops containing large amounts of Predator video feeds. The attack was conducted by intercepting the Predator's video data link, due to its occasional transmitting over unencrypted networks. The Predator UAV was also likely using an omnidirectional antenna during flights, because this antenna can be vulnerable to interference from any direction. Nevertheless, American forces also discovered that the computer software used to intercept the Predator video links was the Sky Grabber program, costing approximately $26.00 US dollars (Gorman et al, 2009). If the coincidental military raids had not occurred, then the Predator's video data link would have remained compromised for additional periods of time. The above listing of hacking measures shows that over time, hacking techniques of UAVs have remained fluid to adjust to environmental perturbations. As technology continues to change, it can be expected that UAV hacking techniques will continue its adaptative behavior.

Proposition # 2

Malicious intrusions of military UAVs have demonstrated resilience. As such, more sophisticated cyber-attacks on US military UAVs may be forthcoming.

The above proposition serves as partial support for this because computer malware, and subsequent military UAV hacking, did not emerge as one single act. Hacking techniques change in the process of time. As indicated above, the Iraqi military successfully hacked the US Predator UAV in 2009, but during the earlier Gulf War, Iranian forces were overwhelmed by more primitive forms of US electronic warfare. Artificial intelligence, autonomous weapons platforms, consumer demands for increasingly advanced digital objects, and corporate monetary ambitions are some drivers in the UAV environment aiding hacking resiliency because these issues further insecure digital networks and UAV components.

These drivers also continue to present challenges within the UAV environment because UAV cyber security measures still receive inadequate attention within the UAV production lifecycle (GAO, 2018). Moreover, Iran's capture of the US RQ-170 stealth UAV in 2011 was a paradigm shift in hacking resiliency for two reasons: First, a few years prior, Iran probably did not possess the knowledge to bypass US encryption and track US UAV stealth capabilities. Iran's ability to track US stealth technology was undoubtedly derived from the 1990s Balkans' conflict when a US stealth F-117 bomber was shot down by Yugoslavian forces. This data was unquestionably shared with other US military enemies; and secondly, Iran's capture of the RQ-170 Sentinel UAV certified Iran's cyber warfare capabilities as being formidable in the Middle Eastern region. Iran's use of spoofing and jamming GPS signals to capture the RQ-170 Sentinel UAV aided its current climb to cyber elite status, which has not occurred overnight. Additionally, it does not appear coincidental that hacking resiliency in Iran perpetuated through the year 2011, regarding the RQ-170, as approximately one-year prior Iran suffered the 2010 US Stuxnet cyber-attack. It is also possibly not coincidental that Tippenhauer et al (2011) published their research on successful GPS spoofing two months before Iran captured the US RQ-170 Sentinel UAV. Iran's 2011 malicious intrusion shows that hacking the US UAV infrastructure was a priority among the Iranian military. Thus, the malicious intrusion of US military UAV sub-system demonstrates adaptation and resilience when it combined its stealth tracking capabilities with spoofing and jamming GPS. Lastly, Iran's sharing the RQ-170 Sentinel technology with US enemies will further aid hacking resilience because all countries now possessing military UAVs are interested in UAV vulnerabilities. Resiliency is also supported by DoD and private corporate rewards programs paying hackers to use cyberattacks against their networks to expose systemic vulnerabilities.

Proposition # 3

Malicious intrusions of military UAVs and their countermeasures are interdependent/interrelated. Thus, malicious intrusions and their countermeasures appear inseparable.

This proposition is also partially supported by propositions 1 and 2, as the adaptative and resilient nature of hacking military UAVs results from the larger commercial hacking complex system. Understanding UAV vulnerabilities is partially derived from exercising the vulnerability against the UAV or UAV prototype. Also, as indicated above, the DoD is increasingly dependent upon commercial off the shelf UAV products (Watson & Tucker, 2017; Murphy, 2017) due to congressional budget constraints or challenges in retrofitting current systems with improved security protocols. Inadequate security measures during the production of commercial UAVs and US military UAS appear to encourage malicious intrusions, as UAV vulnerabilities are supplemented by political, social and legal motives (Fitzpatrick, 2014). Most hardware and software used for military UAVs is commercially originated. As indicated in the introduction, the US Army Inspector General directed the Army to discontinue its use of Da-Jiang Innovation (DJI) UAVs due to cybersecurity concerns. DJI is a Chinese company and monitors its customer UAV usage by requiring them to register their UAV with the company or suffer capability shortages (Watson & Tucker, 2017; Murphy, 2017). DJI's position here implies a form of reverse hacking upon its customers. Hence, the DoD Inspector General's decision to discontinue all DJI's and supplemental parts used in other DoD areas. However, Sullivan (2017) reported that hackers are dedicated to working around DJI restrictions through malicious means. US Special Forces' significant use of DJI UAVs appears based upon cost, as Special Forces were using thousands of them on the battlefield.

DJI products are competitively priced compared to US UAV domestic market prices (Bloomberg, 2018) but, DJI UAVs have recently had their GPS signals spoofed by hackers (Watson & Tucker, 2017; Murphy, 2017). The interdependent/interrelationship between hacking and its countermeasures is further demonstrated through a UCAV swarm. Theoretically, UCAVs can initiate default programming and move to smaller group formations, or move individually, and still pursue mission objectives if under network attack (Rogoway, 2016). Yet, Zhang and Yang, (2014) already demonstrated that they can successfully jam UAV swarms with their algorithm, which forces UAV swarms into a triangle formation of groups of three or less, allowing for more efficient network intrusion. Malicious intrusions and their countermeasures appear to always reach a degree of equilibrium with each other, despite the countermeasure introduced to the military system. In other words, as the United Nations (UNIDIR, 2017) noted, increasing defensive network measures will inevitably produce an equally determined malicious countermeasure.

Proposition #4

Malicious intrusions of military UAVs prompt coherence by instigating countermeasures. Thus, the intrusion/countermeasure relationship can be viewed as a feedback loop.

Coherence refers to something being consistent or of a logical nature (Snowden, 2011). Regarding malicious intrusions of US military UAVs, coherence respects whether the countermeasure is accurately and sufficiently addressing the attack and, if not, then coherence seeks to determine which countermeasures are leading in the right direction. Consequently, this research theoretically contends that the malicious intrusion of military UAV sub-system can be viewed as possibly a positive element in driving battlefield technological innovation. In other words, unstable systems have their benefits if properly managed.

For example, instability introduced into the DoD UAV development life cycle and fielding operations produced DoD cyber countermeasures regarding policy, as the DoD's 2014 effort replaced their Information Assurance policy with the (DODI 8500.01) Department of Defense Instruction Cybersecurity. Also, the DoD's (DODI 8510.01) Risk Management Framework for Information Technology replaced the Information Assurance Certification and Accreditation Process. In 2015, the DoD stated its Cyber Strategy and the Joint Capabilities Integration and Development System Manual was enhanced regarding expectations for UAV survivability in hostile environments. In 2017, the DoD included new cybersecurity elements within its (DODI 5000.02) Operations of the Defense Acquisition System, which emphasizes cybersecurity in the procurement process (GAO, 2018). The policy revisions illuminate cybersecurity measures throughout the military UAV development and operations. Additionally, the DoD created new agencies addressing cybersecurity among advanced weapon platforms. Hence, the Navy's creation of CyberSafe in 2015, the Air Force's creation of the Cyber Resiliency Office for Weapon Systems in 2017, and the Army's new Task Force Cyber Strong agency also created in 2017 (GAO, 2018).

Other DoD countermeasures involve research and development, as shown through DARPA's Tactical Targeting Network Technology, which pertains to an improved communications network compatible with Link-16, LOS, and ad hoc infrastructures (Li et al, 2013). The DoD is also employing defense contractor Boeing in developing a "hack-proof" aerial vehicle. DARPA is writing the code for this UAV helicopter test vehicle and will fully enclose the vehicle's data transmission computer, with hope that the vehicle will withstand malicious intrusions.

This appears to be part of an earlier secret DARPA research program called High Assurance Cyber Military Systems (HACMS) which began around 2012. HACMS is a computer code that DARPA claims to be un-hackable under testing. DARPA also believes HACMS can have civilian applications in protecting various digital systems relevant to the US critical infrastructure (Infosec, 2014). DARPA's project completion date was 2018. If the software proves successful, then its scale will extend to other DoD UAV platforms (Infosec, 2014). In 2017, DARPA commenced a new satellite system called Black Jack. Its purpose is to provide low earth satellite orbiting for weapon platforms (Erwin, 2018). Pursuit of this system may be to reduce reliance upon commercial satellite communications. Moreover, Boeing has recently secured the naval contract to build an autonomous midair refueling UAV. The contract calls for 72 MQ-25 UAVs at the price of $13 billion. The MQ-25 tanker's autonomous features may prove formidable against malicious intrusions. The above countermeasures are just some examples of DoD efforts at demonstrating coherence within the UAV platforms, and partially showing that if the malicious intrusion sub-system is made more visible (Bar-Yam, 2018), then coherence can lead to continued innovation, despite system instability. Coherence is not a principle that concerns a finalized solution but indicates whether the measures being taken are directing towards the correct path (Snowden, 2011).

National Security and Interests Vulnerabilities

US military UAV crashes threaten US national security and interests due to opportunities for enemy forces to reverse engineer captured advanced US technology and use it against US forces or the homeland. As indicated above, Yochim, (2010) indicated a US military UAV crash rate is 100 times greater than manned aerial vehicles.

Iran's successful capture of the US stealth RQ-170 Sentinel was later reverse engineered by Iran's military and shared with major US enemies. Reverse engineering US UAV technology also allows US enemies to develop sound countermeasures against future US systems. The vulnerability of US military UAVs to malicious intrusion can compromise military operations globally, which can impact US national security and interests by compromising strategic and tactical advantages that UAVs provide to US troops through intelligence gathering, surveillance, and reconnaissance measures during battlefield operations, especially given the DoD's growing dependence on UAV systems (GAO, 2018); the DoD's dependence upon UAVs is further threatened by DoD supply chain security weaknesses. The US' growing dependence upon commercial UAV platforms and related parts also jeopardizes US national security, due to the expanding UAV market, the potential impact on the US economy, and inadequate security protocols during the commercial UAV development life cycle. DJI's cyber threat profile raised concerns for DoD officials, initiating a ban on their UAV products (Watson & Tucker, 2017; Murphy, 2017). As DJI continues to dominate the global UAV commercial market, their registration requirements can serve as a global intelligence gathering net for the Chinese government. It remains unknown whether the US military's extensive use of DJI UAV/components managed to inject undetected exploits within US military systems. Lastly, malicious intrusions of military UAVs may perpetuate national security and interest threats because of its complex nature. As a sub-system, the intrusions may continually possess hidden and evolving elements that may not be fully understood. Inadequate sub-system comprehension may be minimized by embracing the inevitability of military UAVs being subverted and continuation of humans in the loop protocols within the UAV development and operational lifecycle.

Emerging Elements

Application of autonomous systems to malicious intrusion of military UAVs appears inevitable. Therefore, autonomous hacking methods towards military UAV systems (adaptation) could move beyond the realm of human reasoning and control. Thus, as autonomous military UAVs present beyond next generation functions, autonomous malicious intrusion capabilities are soon following. US autonomous UAV technology proliferating among US enemies may emerge more quickly than suspected, given the pace the technology is advancing. Domestically, military UAVs may present a significant bases for civil unrest against corporate and law enforcement UAV use, which can lead an autonomous military UAV to enact additional countermeasures addressing the protesting population. This, in turn, can enact stronger cyber violence by the protesting population (attack/countermeasure relationship). UAVs as loitering airborne warning and control systems (AWACS) and as aerial network stations, are likely to advance and change the domestic wireless network transmission infrastructure. In other words, loitering UAVS can replace cell towers. Also, countries targeted by US UAV strikes may view domestic civilian components, such as defense contractors, UAV pilots, NSA employees, US civilian satellites as justifiable targets as US enemies continue to use asymmetrical warfare to combat superior US forces.

Conclusions

The malicious intrusion of the US military UAV complex sub-system is likely to expand in scale, as the US continues its global military ambitions. The sub-system many also scale across the US homeland and possibly reach equilibrium as it merges with its commercial counterpart, which is also still evolving.

The possible merging of the malicious intrusions of military and civilian UAV sub-systems will likely not conflict but may emerge into one larger complex system, as UAV consumer demand, asymmetrical warfare, and the Internet of Things continues to drive UAV global proliferation. Therefore, distinctions between commercial and military UAVs may slowly diminish in time, as the DoD continues consulting and aiding UAV procurement for domestic US law enforcement regarding anti-crime, surveillance, and border patrol issues. Also, inspection of UAV algorithms by an official body ensuring their non-military use within domestic UAVs may not be forthcoming, due to proprietary and national security concerns (UNIDIR weapon, 2017). Proprietary algorithm conflicts may increase the DoD ‘s inability to achieve full interoperability among its UAV fleet, as interoperability remains a road block in military UAV efficiency in foreign lands and safe and secure UAV airspace domestically.

Recommendations

The DoD should incrementally broaden (open) its circumference of individuals evaluating and developing malicious intrusion countermeasures because this will further innovation respecting anti-UAV hacking applications**.** Moreover, all defense contractors not applying next generation cyber security measures at each stage of the UAV development life cycle, should be given a reasonable and limited probation period to conform to this standard. Applying advanced cybersecurity measures in the military UAV development life cycle is necessary due to the DoD’s inadequate application of cybersecurity measures practices in this area as noted by the GAO (2018). Contractors not conforming to the new cybersecurity development life cycle standard will lose money from their contract each day or month they fail to implement the new security protocols.

This measure will serve as positive motivation for defense contractors in making cyber security a greater priority during the military UAV production life cycle. Also, the DoD should consider reducing it procurement pace of UAVs, because this will allow defense contractors more time to embrace and apply increased security standards on UAV platforms. With a decreased pace in military UAV procurement, additional funding can be applied to increase funding of DoD research and development of malicious intrusion defenses for its UAVs for fiscal year 2020 and beyond. This budget increase will fortify the above suggestions and will demonstrate further DoD commitments toward changing their UAV cybersecurity mindset. The DoD should also slow its pace at achieving fully autonomous UAVs, until it can fully comply with the GAO's and DoD Inspector General's recommendations on UAV cyber security, because autonomous military UAVs will present beyond next generation functions, with autonomous malicious intrusion soon following. Moreover, the DoD should continue to pursue procurement of its own satellite systems for UAV operations. Despite reduced economics, commercial systems should be avoided due to insufficient or non-existent encryption protocols. As such, all UAV elements should have encryption and layers of defense around communication links and sensors.

Layers of defense should be emphasized during the UAV production lifecycle and retrofitting security measures on military UAVs should be avoided as much as possible due to cost and time. Implementing layers of defense within military UAV elements will increase military battlefield operation efficiency and aid in safeguarding against advanced US UAV technology inadvertently falling into US enemy possession.

References

Abraham, R.H. (2002). *The genesis of complexity*. Retrieved from http://www.philpaper,org

Allen, G., & Chan, T. (2017). *Artificial intelligence and national security*. Retrieved from http://www.belfercenter.org

Anderson, C. (2010). Presenting and evaluating qualitative research. *American Journal of Pharmaceutical Education, 74,* 1-7.

Anderson, P., Meyer, A., Eisenhardt, K., Carley, K., & Pettigrew, A. (1999). Introduction to the Special Issue: Applications of Complexity theory to organization science. *Organization Science, 10,* 233-236.

Aspin, L. (1993). *Report on the bottom-up review*. Retrieved from http://www.hsdl.org

Atherton, K. (2018). *Pentagon suspends commercial drone purchases and use*. Retrieved from http://www.c4isrnet.com

Bar-Yam, Yaneer. (1997). *Dynamics of complex systems*. Reading, Massachusetts: Perseus Books.

Bar-Yam, T., Lynch, O., & Bar-Yam, Y. (2018). The inherent instability of disordered systems. *arXiv, 1*, 1-24.

Bloomberg News: DJI drones score U.S. wins as trade war with China takes a tool. (2018). Retrieved from http://www.bloomberg.com

Blum, S. (2018). *Watch thieve steal a Tesla Model S with just a tablet and a phone*. Retrieved from http://www.bgr.com

Bureau of Investigative Journalism. Obama's covert drone war in numbers: Ten times more strikes than Bush. (2017). Retrieved from http://www.thebureauinvestigates.com

Cole, S. (2018). *Directorate S: The C.I.A. and America's secret wars in Afghanistan and Pakistan.* NY, NY: Penguin Press.

Cole, S. (2004). *Ghost Wars: The secret history of the CIA, Afghanistan, and Bin Laden, from the Soviet invasion to September 10, 2001*. NY, NY: Penguin Books.

Comen, E. (2017). *15 commercial products invented for the military*. Retrieved from http://www.247wallst.com

Costs of war: Summary of findings. (2019). Retrieved from http://www.watson.brown.edu

Crampton, J.W. (2016). Assemblage of the vertical: commercial drones and algorithmic life. *Geographica Helvetica, 71,* 137-146.

Cuadra, A., & Whitlock, C. (2014). *How drones are controlled*. Retrieved from http://www.washingtonpost.com

Cunningham, S. (2015). *UAVs in the military*. Retrieved from http://www.sites.tufts.edu

Davidson, D., Wu, H., Jellinek, R. (2016). *Controlling UAVs with sensor input spoofing attacks*. Retrieved from http://wwwusenix.org

Defense Intelligence Agency. Challenges to security in space. (2019) Retrieved from http://www.dia.mil

Department of Defense, Defense Science Board Task Force Reports: Resilient military systems and the advanced cyber threat. (2013). Retrieved from http://www.ocq.osd.mil

Department of Defense, Director, Operational Test and Evaluation Annual Report (2016). Retrieved from http://www.dote.osd.mil

Easttom, C. & Taylor, J. (2011). *Computer crime, investigation, and the law*. Boston, MA: Cengage.

Edwards, N.J., Kao, G., Hamlet, J.R., Liptak, S.F. (2015). *Supply chain decision analytics: Application and case study for critical infrastructure security*. Retrieved from http://www.osti.gov

Electronic Code of Federal Regulations. (2019). Retrieved from http://www.ecf.gov

Electronic Frontier Foundation: Newly released drone records reveal extensive military flights in US. (2012). Retrieved from http://www.eff.org

Erwin, S. (2017). *U.S. military gets taste of new satellite technology for unmanned aircraft*. Retrieved from http://www.spacenews.com

Erwin, S. (2018). *Boeing to accelerate production of WGS satellite.* Retrieved from http://www.spacenews.com

Ewin, S. (2018). *DARPA to begin new effort to build military constellations in low earth orbit*. Retrieved from http://www.spacenews.com

Federal Aviation Authority Reauthorization Act. 2018. Retrieved from http://www.faa.gov

Fellman. P.V. (2010). *The complexity of terrorist networks*. Retrieved from http://www.necsi.edu

Fitzpatrick, A. (2014). Drones for good: Technological innovations, social movements, and the state. *Journal of International Affairs, 68*, 19-36.

Fomichev, M., Alverez, F., Steinmetzer, D., Stephen, P., & Hollick, M. (2017). *aRxiv*, 1-35.

General Atomics: Grey Eagle UAS. (n.d.). Retrieved from http://www.ga-asi.com

Gettinger, D. (2018). *Summary of drone spending in the fiscal year 2019 Defense budget request*. Retrieved from http://www.dronecenter.bard.edu

Gorman, S., & Dreazen, V. J. (2009). *Insurgents hack U.S. drones*. Retrieved from http://www.wsj.com

Government Accountability Office. December 2017. *Naval unmanned aerial refueling system: Acquisition addresses validated requirements and reflects a knowledge-based approach.* http://wwwgao.gov (accessed December 15, 2018)

Government Accountability Office. March 2004. *Nonproliferation: Improvements needed for controls on exports of cruise missiles and unmanned aerial vehicle technology. Testimony before the Subcommittee on National Security, Emerging Threats and International Relations, Committee on Government Reform, House of Representatives. Statement of Joseph A. Christoff, Director International Affairs and Trade.* http://wwwgao.gov (accessed December 15, 2018).

Government Accountability Office. January 2004. *Nonproliferation: Improvements needed to better control technology exports for cruise missiles and unmanned aerial vehicles. Reports to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives*. (accessed December 5, 2018)

Government Accountability Office. March 2004. *Unmanned aerial vehicles: Major management issues facing DoD's development and fielding efforts. Testimony before the Subcommittee on Tactical Air and Land Forces, Committee on Armed Services, House of Representatives. Statement of Neal P. Curtin, Director of Defense Capabilities and Management and Paul L. Francis, Director Acquisition and Sourcing Management*. (accessed December 5, 2018).

Government Accountability Office. February 2016. *Counterfeit Parts: DoD needs to improve reporting and oversight to reduce supply chain risk*. (accessed December 5, 2018).

Government Accountability Office. February 2016. *Unmanned aerial vehicles: Improved strategic and Acquisition planning can help address emerging challenges.* (accessed December 5, 2018)

Government Accountability Office. October 2018. *Weapon systems cybersecurity: DoD just beginning to grapple with scale of vulnerabilities. Report to the Committee on Armed Services, U.S. Senate.* (accessed December 10, 2018).

Government Accountability Office. February 15, 2013. *Unmanned aircraft systems: Continued coordination, operational data, and performance standards needed to guide research and development. Testimony before the Subcommittee on Oversight, Committee on Science, Space, and Technology, House of Representatives. Statement of Gerald L. Dillingham, Ph.D. Director, Physical Infrastructure Issues.* (accessed December 5, 2015).

Greenberg, A. (2015). *Hackers remotely kill a jeep on the highway- with me in it*. Retrieved from http://www.wired.com

Greenemeier, L. (2017). *The Pentagon's-seek-and-destroy mission for counterfeit electronics.* Retrieved from http://www.scientificamerica.com

Grose, T.K. (2016). Flight Risk. *Asee Prism, 25*, 30-33.

Gu, T., Dolan-Gavin, B., Garg, S. (2017*). Badnets: Identifying vulnerabilities in the machine learning model supply chain. arXiv, 1*.

Hall, K.D. (2006). *Near space: Should Air Force Space Command take control of its shore?* Retrieved from http://www.hsdl.org

Hamsavahini, R., Rashmi, N., Varun, N., Swaroop, R.S., Praneeth, V., & Narayana, S. (2016). Development of light weight algorithm in a customized communication protocol for micro air vehicles. *International Journal of Latest Research in Engineering and Technology, 71-73*.

Harrison, H., Birks, M., & Mills, J. (2017). Case study research: Foundations and Methodological Orientations. *Forum: Qualitative Social Research, 18,*

Harris, A. (2018). Preparing for the multidomain warfare. *Air & Space Journal*, 45-79.

Hartmann, K. & Steup, C. (2013). *The vulnerability of UAVs to cyberattacks – An approach to the risk assessments*. Retrieved from http://researchgate.net

Hyett, N., Kenny, A., Dickson-Swift, V. (2014). Methodology or method? A critical review of qualitative case study reports. *International Journal of Qualitative Studies on Health and Well-being, 9,* 1-12.

Infosec Institute – Hack-proof drones possible with HACMS technology. (2014). Retrieved from http://www.infosecinstitute.com

Insinna, V. & Larter, D.B. (2018). *Us Navy selects builder for new MQ-25 Stingray aerial refueling drone.* Retrieved from http://www.defensenews.com

International Telecommunication Union: Characteristics of unmanned aircraft systems and spectrum requirements to support their safe operation in non-segregated airspace. (2009). Retrieved from http://www.itu.int

Jackson, B.A.; Frelinger, D.R., Lostumbo, M.J.; Button, R.W. (2008). *Evaluating novel threats to the homeland: Unmanned aerial vehicles and cruise missiles.* Retrieved from http://www.rand.org

Jacobsen, A. (2015). *The Pentagon's brain: An uncensored history of DARPA, America's top-secret military research agency*. NY, NY: Little, Brown, and Company.

Jones, J. (n.d.). *System of systems integration technology and experimentation (SoSITE).* Retrieved from http://www.darpa.mil

Jones-Lloyd, G. (2003). Design and control issues in qualitative case study research. *International Journal of Qualitative Methods, 2,* 33-41.

Kostlan, E. (1988). Complexity theory of numerical linear algebra. *Journal of Computational and Applied Mathematics, 22,* 219-230.

Kwon, Y., Yu, J., Cho, B., & Eun, Y. (2018). Empirical analysis of mavlink protocol vulnerability for attacking unmanned aerial vehicles. *IEEE Access, 6,* 2169-3536.

Lachow, I. (2017). The upside and downside of swarming drones. *Bulletin of the Atomic Scientists, 73,* 96-101.

Leopold, G. (2014). *New hacking scenario emerges: Wi-Fi signal- sniffing drones*. Retrieved from http://www.defensesystems.com

Liang, Y.T. (2013). Edge of emergence, relativistic complexity and the new leadership. *Human Systems Management, 32,* 3-15.

Lock, I., & Seele, P. (2018). Gauging the rigor of qualitative case studies in comparative lobbying research. A framework and guideline for research and analysis. *Journal of Public Affairs, 18,* 1-5.

Loukas, G., Vuong, T., Heartfield, R., Sakellari, G., Yoon, Y., & Gan, D. (2017). *Cloud-based cyber-physical intrusion detection for vehicles using deep learning.* Retrieved from http://www.researchgate.net

Mason, R.B. (2009). Management actions, attitudes to change and perceptions of the external environment: A complexity theory approach. *Journal of General Management, 34,* 37-53.

Mazzetti, M. (2012). *The drone zone.* Retrieved from http://www.nytimes.com

Mazzocchi, F. (2008). Complexity in biology. Exceeding the limits of reduction and determinism using complexity theory. *EMBO Reports, 1,* 10-14.

McKelvey, B. (1999). Avoiding complexity catastrophe in coevolutionary pockets: Strategies for rugged landscapes. *Organizational Science, 10,* 294-321.

Memorandum for Distribution. Subject: Audit of the DoD's Implementation of Cybersecurity Controls for unmanned aerial vehicle systems (project no. D2018-D000CR-0113.000). Retrieved from http://www.media.defense.gov

Mohammad, M., Saad, W., Bennis, M., Nam, Y., & Debbah, M. (2018). A tutorial on UAVs for wireless networks: Applications, challenges, and open problems. *arXiv, 1*

Morrison, K. (2010). Complexity theory, social leadership and management questions for theory and practice. *Educational, Management Administration & Leadership, 38,* 374-393.

Mortimer, G. (2017). *US Army calls for units to discontinue use of DJI equipment*. Retrieved from http://www.suasnews.com

Nassi, B., Netanel, R., Shamir, A., & Elovici, Y. (2018). Game of drones- Detecting streamed POI from encrypted FPV channel. *arXiv,* 1-11.

National Defense Authorization Act. (2001). Retrieved from http://www.congress.gov

National Defense Authorization Act. (2016). Retrieved from http://www.congress.gov

NBC News. (2014). *Military drone crashes near school*. Retrieved from http://www.nbcphiladelphia.com

Niva, S. (2013). Disappearing violence: JSOC and the Pentagon's new cartography of networked warfare. *Security Dialogue, 44,* 185-202.

Nguyen, A., Yosinki, J., & Clune, J. (2015). Deep neural networks are easily fooled: High confidence predictions for the unrecognizable images. *Computer Vision and Pattern Recognition, 4.*

Office of the Attorney General. Memorandum for the Attorney General re: Application of federal criminal laws and the Constitution to contemplate lethal operations against Shaykh Anwar al-Aulaqi. (2010). Retrieved from http://www.fas.org

Osborn, K. (2015). *Navy Secretary says future Navy fighter planes will be unmanned*. Retrieved from http://www.military.com

Panko, R. & Panko, J. A. (2015). *Business data networks and security.* NY, NY: Pearson

Rani, C., Modares, H., Sriram, R., Mikulski, D., Lewis, F.L. (2016). Security of unmanned aerial vehicle systems against cyber-physical attacks. *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, 13,* 331-342.

Rodday, N.M., Schmidt, R.O., & Pras, A. (2016). *Exploring security vulnerabilities of unmanned aerial vehicles*. Retrieved from http://www.ieeexplore.ieee.org

Scahill, J. (2016). *The assassination complex: Inside the us government's secret drone warfare programme.* NY, NY: Simon & Schuster.

Shachtman, N (2011). *Exclusive: Computer virus hits U.S. drone fleet*. Retrieved from http://www.wired.com

Shashok, N. (2017). *Analysis of vulnerabilities in modern unmanned aircraft systems*. Retrieved from http://www.pdfs.semanticscholar.org

Sly, L. (2018). *Who is attacking Russia's bases in Syria? A new mystery emerges in the war*. Retrieved from http://www.washingtonpost.com

Snowden, D. (2011). Naturalizing sensemaking. In Mosier, K.L. & Fischer, U.M. (Eds). *Informed by knowledge: Expert performance in complex systems.* NY, NY: Psychology Press.

Snowden, D. & Stanbridge, P. (2004). The landscape of management: Creating the context for understanding social complexity. *E:CO, 2*, 140-148.

Son, Y., Shin, H., Kim, D., Park, Y., Noh, J., Choi, K., Choi, J., & Kim, Y. (2015). *Rocking drones with intentional sound noise on gyroscopic sensors.* Retrieved from http://www.usenix.org

Statement for the record worldwide threat assessment of the US Intelligence Community Senate Select Committee on Intelligence. Daniel R. Coats, Director of National Intelligence May 11, 2017. Retrieved from http://www.dni.gov

Stepanovich, A. (2012). *Electronic Privacy information Center: Testimony and statement for the record of Amie Stepanovich. Hearing on "Using unmanned aerial systems within the homeland: Security game changer?" Before the Subcommittee on Oversight, Investigations, and Management of the U.S. of Representatives, Committee on Homeland Security.* Retrieved from http://www.epic.org

Sternstein, A. (2015). *Pentagon on path to launch hacker-proof Boeing drone by 2018*. Retrieved from http://www.nextgov.com

Suescun, C.A., Cardei, M. (2014). *Unmanned aerial vehicles networking protocols.* Retrieved from http://www.researchgate.net

Teal Group predicts worldwide civil drone production will soar over the next decade. (2018). Retrieved from http://www.tealgroup.com

Thompson, W.T., & Tvaryanas, A.P. (2005). *United States Air Force 311TH Human System Wing. U.S. military unmanned aerial vehicle mishaps: Assessments of the role of human factors using human factors analysis and classification system (HFACS).* Retrieved from http://wwwpdfs.semanticsscholar.org

Tippenhauer, N.O., Popper, C., Rasmussen, K.B., & Capkun, S. (2011). *On the requirements for successful GPS spoofing attacks*. Retrieved from http://wwwcs.ox.ac.uk/files

United Nations Institute for Disarmament Research: The weaponization of increasingly autonomous technologies-autonomous weapon systems and cyber operations. (2017). Retrieved from http://www.unidir.org

Unmanned aerial vehicle reliability study. (2003). Retrieve from http://www.defensedaily.com

Unmanned systems integrated roadmap. (2017-2042). Retrieved from http://wwwdefensedaily.com

U.S. Air Force – Wasp III. (2007). Retrieved from http://www.usairforce.com

U.S. Marines Corps: Electronic Warfare. Retrieved from http://www.marines.mil

U.S. Library of Congress. Congressional Research Service. 2013. *Intelligence, surveillance, and reconnaissance (ISR) acquisition: Issues for Congress*, by Marshall Curtis Erwin. CRS Report 7-5700. Washington, DC: Office of Congressional Information and Publishing, April, 6, 2013.

U.S. Library of Congress. Congressional Research Service. 2012. *Pilotless drones: Background and considerations for Congress regarding unmanned aircraft operations in the national airspace: Issues for Congress,* by Bart Elias. CRS Report 42718. Washington, D.C: Office of Congressional Information and Publishing, September 10, 2012.

U.S. Library of Congress. Congressional Research Service. 2012. *Homeland security: Unmanned aerial vehicles and border surveillance: Issues for Congress*. CRS Report 21698. Washington, D.C: Office of Congressional information and Publishing, July 8, 2010.

U.S. Library of Congress. Congressional Research Service. 2003. *Unmanned aerial vehicles: Background and issues for Congress, by Elizabeth Bone and Christopher Bolkcom*. CRS Report 31872. Washington, D. C: Office of Congressional Information and Publishing, April 25, 2003.

U.S. Library of Congress. Congressional Research Service. 2006. *Unmanned vehicles for U.S. naval forces: Background and issues for Congress,* by Ronald O'Rourke. Washington, D.C: Office of Congressional information and Publishing, October 25, 2006.

Villasenor, J. (2011). *Cyber-physical attacks and drones strikes: The next homeland security threat.* Retrieved from http://www.brookings.edu

Watson, B. (2017). *The US Army just ordered soldiers to stop using drones from China's DJI*. Retrieved From http://www.defenseone.com

Whittle, R. (2015). *Air Force begs to differ with Matbus: F-35 not last manned fighter*. Retrieved from http://www.breakingdefense.com

Yagderell, E., Gemci, C., & Aktas, A.Z. (2015). A study on cyber-security of autonomous and unmanned vehicles. *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, 12,*369-381.

Yin, R.K. (1981). The case study crisis: Some answers. *Administrative Science Quarterly, 26,*58-65.

Yin, R. K. (2009). *Case study research: Design and methods – the case study as a research strategy method*. Thousand Oaks, Ca: Sage Publishing.

Zhang, Y., & Yang, L. (2014). Triangle ad GA methods for UAVs jamming. *Mathematical Problems in Engineering, 1-8*