Abstract

The use of Unmanned Aircraft Systems (UAS) for military, law enforcement, and private applications has increased significantly in recent years, and this increase will only continue both by the United States (U.S.) and by other nation states and private organizations. This proliferation comes with an increased risk of a cyber attack against an unmanned aircraft itself, its ground station(s), and the computer or sensor networks that enable its use. This study examined ways in which UAS are employed, ways in which they are vulnerable to cyber attack, and ways these risks can be mitigated. The risk of cyber attack is analyzed by considering vulnerability, impact, likelihood, and countermeasures. The study found that the risk of cyber attack varies significantly between the high, fast flying UAS and the lower altitude, slower UAS likely to be employed in domestic airspace by law enforcement and other organizations. The study also found that every attack that can be executed abroad can also occur over the U.S., with perhaps more significant consequences. Also, sophisticated and multi-stage and insider threat attacks are an underreported risk. Lastly, the study found that every UAS attack capability the U.S. and its allies have employed will eventually be used against us by nation state and non-state adversaries as their own UAS capabilities mature in the coming years. The study concluded with recommendations for future areas of research, including improved "sense and avoid" technology, cloud-based command and control, and an international legal framework for the use of UAS in sovereign nations' airspace.

AN ANALYSIS OF THE VULNERABILITY OF UNMANNED AIRCRAFT SYSTEMS TO CYBER ATTACK

by

Daniel W. Brodsky

A Capstone Project Submitted to the Faculty of

Utica College

May 2012

In Partial Fulfillment of the Requirements for the Degree

Master of Science

Table of Contents

List of Illustrative Figures

Acknowledgment

This paper marks the completion of a very challenging graduate program, one that I could not have completed without the advice and support of my friends and family. First, I would like to thank my parents, Bruce and Mary Ann Brodsky, for raising me to value education and hard work.

I would like to thank my capstone project advisor, Prof. Daniel Draz, for providing encouragement and guidance even when I didn't want to listen to him. I would also like to thank my second reader, Mr. Robert Parry, a bottomless well of information on drones (and a great many other things), for reading the numerous drafts of this paper and graciously lending his expertise.

Lastly, I would especially like to thank my wife, Megan, and my children, Jack and Isabella. It was them that bore the brunt of the sacrifice as I squirreled myself away in front of the computer for countless hours over the last 20 months. It is to them that I dedicate any good fortune that may smile down upon us as a result of earning this degree.

An Analysis of the Vulnerability of Unmanned Aircraft Systems to Cyber Attack

The use of Unmanned Aircraft Systems (UAS), also known as Unmanned Aerial Vehicles (UAVs), Remotely Piloted Aircraft (RPAs), or Drones, has increased dramatically in recent years. UAS airstrikes in Pakistan increased from five in 2007 to 117 in 2010, and led to the deaths of 1,550 members of the Taliban, Al Qaeda, and other affiliated extremist groups (Roggio & Mayer, 2011). The General Atomics MQ-1 Predator aircraft (Predator) was used extensively in the last months of Moammar Gadhafi's regime in Libya; from mid-April to mid-October 2011, the Predator launched 145 airstrikes (Ackerman, Libya: The Real U.S. Drone War, 2011). Predator use for surveillance dates back to the North Atlantic Treaty Organization's (NATO) use of them in 1995 in Bosnia and Herzegovina (Airforce-Technology.com, n.d.). The United States (U.S.) has deployed UAS along the U.S.-Mexico border for years to conduct reconnaissance, looking for illegal immigrants and reporting back to border patrol officials, and has recently performed flights over Mexico for counternarcotic missions (Sheridan, 2011). Law enforcement agencies have also begun to use non-military UAS to spot criminal activity, where Federal Aviation Administration (FAA) rules have allowed (Seidman, 2011). These new uses for UAS highlight the need to protect both the aircraft and the network that enables them from cyber attack.

The purpose of this study was to examine the uses of UAS in civil, law enforcement, and military applications, to explore the ways in which they are vulnerable to cyber attack, and to suggest countermeasures that can lower the risk of a cyber attack. The focus was on descriptive research, with the goal of summarizing the state of the art when it comes to UAS cyber vulnerabilities and mitigation strategies. Data was collected

primarily from open sources and includes capabilities of commodity hardware, firmware, and software, publicly released UAS activity in law enforcement and military operations, and an exploration of the emerging do-it-yourself drone community. Previously disclosed cyber attacks were examined in detail, and potential attack vectors that have not yet been implemented were considered.

Applications of Unmanned Aircraft Systems

Perhaps the most well-known use of UAS has been for surveillance and attack missions in the Middle East. Drone use under President Obama has grown every year since he took office, and there is speculation that there are now dozens of facilities supporting UAS missions, including operational bases, virtual U.S. Air Force cockpits, and clandestine bases in at least six countries (Miller, 2011). For every unmanned aircraft that flies, there is a support infrastructure around it, including its connections to satellite- and ground-based Command and Control (C2) systems, relay stations needed to pass signals long distances and account for the curvature of the Earth, bandwidth used to feed video or other sensor data back to a ground station, and the classified networks used to manage UAS missions. Each of these discrete infrastructure elements comes with its own vulnerabilities, and those weak points were explored.

Comprehensive research into UAS vulnerabilities must not be limited to just the medium- and long-range military weaponized and surveillance platforms such as the Predator, the General Atomics MQ-9 Reaper (Reaper), and the Northrop Grumman RQ-4 Global Hawk (Global Hawk) aircraft. Drones are becoming smaller, quieter, and more affordable, and their applications are becoming more diverse. The Wasp III microdrone weighs less than a pound and is under a foot long, yet it can carry two cameras and a

Global Positioning System (GPS) receiver and can fly at an altitude of 1,000 feet Above Ground Level (AGL) (Villasenor, 2011). These small drones are not strictly the provenance of nation states, either. There is a do-it-yourself drone movement that seeks to empower ordinary citizens who want to launch UAS. One example is the ArduPlane, which is a set of hardware components and software programs capable of converting a remote control (R/C) plane to a fully autonomous drone, with GPS waypoints, scriptable missions, and one-click software loading complete with mission planning tools (Anderson, 2010). At the 2012 ShmooCon security conference, a researcher presented plans for a disposable sensor package that could be flown into place by a small UAS. This low-cost technology could be used to build an ad-hoc airborne sensor network that even a hobbyist could afford (Greenburg, 2012). These systems often use off-the-shelf hardware and amateur software programs downloaded from the Internet, and are likely more vulnerable to attacks than the hardened military systems.

Law enforcement is another important use of UAS. Two examples of UAS in use by police today are the T-Hawk, a micro air vehicle that can carry 20 pounds of equipment and capture 24 minutes of high-quality video, and the Draganflyer X6, which is a remotely operated miniature helicopter designed to carry wireless video, still cameras and light thermal imaging equipment (Cuadra & Downs, 2011).

The last category of UAS explored was one that was itself capable of conducting a cyber attack. At the 2011 DEFCON security conference, researchers demonstrated a small UAS that was capable of attacking IEEE 802.11 (Wi-Fi), Bluetooth, and Global System for Mobile Communications (GSM) cellular networks. It can record packets being transmitted on wireless networks, and capture GSM phone information that can

later be used to make outgoing calls or spoof cellular towers. The system can also connect to unsecured Wi-Fi networks and use them as a gateway for launching computer network attacks (The Economic Times, 2011). These aircraft can be used by government officials, law enforcement agencies, citizens, or criminals for airborne surveillance on individuals, so it is important to understand their capabilities and weaknesses.

Research Questions

This research sought to provide answers to the following questions:

- What are ways each component of a UAS is vulnerable to cyber attack? This includes aircraft hardware, aircraft software, air-ground communication, and supporting computer networks. This is not limited to UAS use in foreign theaters of operation; civilian and military UAS that fly in the domestic airspace may also be susceptible to attack.
- What is the impact of an attack on each component of the UAS infrastructure? How would an attack affect military, law enforcement, or other operations?
- What is the likelihood of a cyber attack? What technologies and what level of access would an adversary require to disrupt UAS operations? This includes an attempt to separate media hype about cyber attacks from the true probability that an attack could be successful.
- What countermeasures can be employed to reduce the likelihood or impact of a cyber attack? This includes a cost-benefit discussion, since UAS have two fundamental limits that affect how they are used: weight and bandwidth. If a countermeasure is too heavy, or requires too much bandwidth, it may be not considered worthwhile given the likelihood of an attack.

- What are the implications of constructing a drone whose purpose is to prosecute a cyber attack? How can such an aircraft be countered, in light of the vulnerabilities explored as part of this research?

Research Methodology

As mentioned earlier, the focus was on descriptive research, on looking at all available data and making empirical generalizations to satisfy the research questions. The data was analyzed in the context of risk: What are the risks of using UAS? How can these risks be mitigated? What are the risks of attempting to disrupt UAS operations? The components of risk in this context were the vulnerabilities of a system, the impact of an attack on the system, the likelihood of an attack, and the countermeasures that could be deployed to reduce the magnitude of vulnerabilities, impacts, or likelihood. These components of risk were different for different applications of UAS. Military weaponized UAS that rely on classified networks are inherently more resistant to attack than a hobbyist's side project. The nature of the UAS application was considered when weighing risks associated with operating them.

Sources of data included scholarly journals, essays and articles by experts in the field, and information provided by vendors of UAS components. Given the relative newness of UAS proliferation, there is not a substantial body of scholarly research specific to UAS cyber attacks. That said, many of the attack vectors have an electronic warfare (EW) or Electronic Countermeasures (ECM) component to them, and there is ample research on EW and ECM techniques.

After surveying the scholarly literature and presenting findings, the research concluded with recommendations for further areas of research. In addition to known

cyber attacks, there is speculation on what future attack vectors may look like, and research recommendations were made with these forward-thinking attacks in mind.

Importance of Research

Research into this area was important, because as Hennigan (2011) notes, "the Pentagon is looking to cheaper, smaller weapons to wage war in the 21st century", and is looking to small unmanned aircraft to drop "smart bombs" and to conduct surveillance on enemy targets. The U.S. government is also looking at UAS for fleet reconnaissance, forest fire identification, chemical and biological agent detection and dispersal, search and rescue, weather and satellite research, and missile defense (Parry, 2012). As these systems proliferate, they become a more significant target for attackers. The Department of Defense (DoD) has already seen malicious code infecting Microsoft Windows computers in its Predator and Reaper Ground Control Stations (Carr, 2011). This comes two years after the U.S. discovered that insurgents in Iraq were intercepting an unencrypted UAS video feed using widely available satellite dishes and software programs (Shachtman, 2009). Most recently, there is speculation that Iran used a cyber attack to take down a U.S. surveillance drone (West, 2011).

Research into cyber attack mitigation is especially important to the DoD, whose spending on UAS has increased every year of the past decade, from $284 million in Fiscal Year (FY) 2000 to $3.3 billion in FY 2010. Unmanned aircraft now make up 31% of the DoD aircraft inventory, up from 5% in 2005. Both DoD and civilian organizations are working with the FAA to allow unmanned aircraft in the National Airspace System (NAS), highlighting the need to understand how these systems are vulnerable and how to assess risk since they'll be flying over populated areas in the U.S. (Gertler, 2012)

Deficiencies in Current Research

Research into UAS cyber vulnerabilities has yet to represent the threat in its entirety. Puchaty & DeLaurentis (2011) discuss ways to model the performance of UAS networks using a system of systems approach, showing how local cyber attacks such as Distributed Denial of Service (DDoS) attacks can disrupt UAS operations. Kotenko (2005) performed additional modeling and simulation work on cyber attacks, and gave a visual representation of those attacks. The Defense Advanced Research Projects Agency (DARPA) has funded research on "high assurance" systems to prevent infection with malicious code, and in November 2011 conducted its first-ever Cyber Colloquium with the goal of identifying how to protect UAS from cyber attacks (Ackerman, Darpa Looks to Protect Drones From Hack Attacks, 2011). DARPA is also funding research into secure, mission-oriented resilient cloud computing platforms that could be used by UAS (Montalbano, 2011).

Much of the research on UAS has been focused on the most well-known usage of them; their use by the U.S. military in foreign countries. Less attention has been paid to domestic use of UAS by local, state, and federal law enforcement agencies. There has also been less attention paid to amateur or criminal use of UAS. Assessing the cyber attack risk these less expensive and smaller drones face fills an important gap in understanding the effects of using UAS for civilian and law enforcement applications.

There has been some research done on novel ways to network UAS, to provide ad-hoc wireless communications between them, and to allow them to operate in formation to avoid collisions. Elston, Frew & Argrow (2006) describe a Wi-Fi network using Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) to create

an ad-hoc Wi-Fi network for UAS to communicate. The Center for Unmanned Aircraft Systems (C-UAS) has funded research into advanced autonomy, UAS-based communications networks, and multi-agent UAS (C-UAS, n.d.). Each of these uses comes with their own vulnerabilities that were explored.

Audiences for this Research

Research in this area is useful to several audiences. Engineers creating UAS systems can build resiliency and countermeasures into their designs, creating more secure networks and systems (keeping in mind cost, weight, and measurable threat and likelihood of an attack). UAS customers will be prepared for potential denial or disruption of their operations. Those wishing to deny or degrade UAS operations will know which points in the systems' infrastructure are most vulnerable. Researchers finding new ways to network UAS and to fly them autonomously, particularly in the NAS, will be aware of ways in which their networks can become compromised. Researchers looking to compromise adversarial UAS networks will have a recent survey of the latest attack vectors. Lastly, an understanding of UAS vulnerabilities will be useful for offensive operations as well as defensive, since the U.S. may soon face adversaries with UAS capabilities comparable to our own (Shane, 2011).

UAS will continue to grow in the future, and the output of this research aids UAS stakeholders in understanding the threat posed by cyber attacks, the likelihood of successful attacks, and how to mitigate those attacks.

Literature Review

UAS usage has only recently captured the attention of the public, but there has been scholarly research on the uses and vulnerabilities of these systems for a number of

years. In this section, the author discusses how previous scholarly research can provide background information, support for or against, or alternative theories about the topics being addressed in this study.

The research reviewed in this section is summarized and analyzed in the context of the previously defined research questions:

- What are the ways each component of a UAS is vulnerable to cyber attack?
- What is the impact of a successful cyber attack?
- What is the likelihood of a cyber attack being successful?
- What countermeasures can be employed to mitigate the risk of attack?
- What are the implications of creating offensive cyber UAS capabilities?

Use of Unmanned Aircraft Systems by the United States

Before an analysis of cyber vulnerabilities can take place, it is pertinent to review how UAS are being used by the U.S. today.

Department of Defense. The most recent review of DoD use of UAS comes from the Congressional Research Service. Gertler (2012) reviews the history of UAS use by the U.S. military, provides up-to-date numbers of aircraft strength and program funding, and discusses future use of UAS.

According to Gertler, the U.S. military has researched and employed unmanned aircraft since 1917. UAS experimentation during wartime dates back to World War I, although it was not until the Vietnam War that the U.S. first used a UAS, the AQM-34 Frisbee, in a combat role. Drone aircraft have since played roles of increasing importance in Kosovo, Bosnia and Herzegovina, Afghanistan (and the broader terrorist pursuits in neighboring nation states), Iraq (Operations Desert Storm and Iraqi Freedom), and Libya.

Gertler writes that "UAS are thought to offer two main advantages over manned aircraft: they eliminate the risk to a pilot's life, and their aeronautical capabilities, such as endurance, are not bound by human limitations" (Gertler, 2012). This history is valuable because it supports the idea that UAS are assets of national significance, and the U.S. government is relying on their use more than ever. This makes UAS a greater target to our adversaries, and also increases the impact of a successful attack.

The two primary uses of UAS within DoD are Intelligence, Surveillance, and Reconnaissance (ISR), and Strike. Intelligence gathering is the traditional use of UAS, but they are also being used for Explosive Ordinance Disposal (EOD), Battle Damage Assessment (BDA), and Force Protection. Future applications of UAS that DoD is exploring include: resupplying Navy ships, Combat Search and Rescue (CSAR), aerial refueling, and air-to-air combat. Gertler's report shows that while systems like the Predator might be more well-known, the largest quantities of UAS are small, hand-launched systems, as shown below.

Table 1

DoD UAS with the Most Number of Aircraft in Inventory

Name	Aircraft	Ground Stations	Capability
RQ-11 Raven	5,346	3,291	ISR, Target Acquisition
Wasp	916	323	ISR, Target Acquisition
gMAV / T-Hawk	377	194	ISR, Target Acquisition, EOD
RQ-7 Shadow	364	262	ISR, Target Acquisition, BDA
MQ-1 Predator	161	61	ISR, Strike, Force Protection

Smaller UAS that fly closer to the ground could be more susceptible to cyber attack, because they're easier to jam with lower power equipment, and because they're designed to be more expendable, they're not equipped with as many redundant systems as their more expensive, higher altitude counterparts.

Lastly, Gertler discusses the origins of the term "Unmanned Aircraft Systems", indicating that the "system" is comprised of one or more RPAs, ground control stations, and data links. According to the DoD, unmanned aircraft "can fly autonomously or be piloted remotely, can be expendable or recoverable, and can carry a lethal or nonlethal payload" (Gertler, 2012). The author has adopted the use of the acronym UAS throughout this document (as opposed to UAV, RPA, etc.) to reflect the whole-system approach to identifying and mitigating cyber attack risks.

Law enforcement and federal agencies. One of the largest potential growth areas for UAS is their use by law enforcement. Stanley & Crump (2011) recently published a report for the American Civil Liberties Union (ACLU) on the privacy concerns raised by law enforcement and government use of UAS in the U.S. The topic of civil liberties is a paper in its own right, but the ACLU's report does provide a good synopsis of the current uses of UAS in the NAS.

Customs and Border Protection (CBP) has been using seven Predator drones along the U.S. border with Mexico since 2005. They hope to expand that program in the coming years. CBP UAS patrol the entire length of the Mexican border. In December 2011, the Los Angeles Times reported that CBP has made their Predators available for use by local police departments and federal agencies such as the Federal Bureau of Investigation (FBI) and the Drug Enforcement Administration (DEA) (Stanley &

Crump). Police departments that have received permission to fly drones (generally, smaller ones) include: Mesa County, Colorado; Miami, Florida; Houston, Texas; Arlington, Texas; Ogden, Utah; and the State of Hawaii.

Use of drones in the U.S. is limited by FAA rules regarding unmanned aircraft in the NAS, and by 18 U.S.C. § 1385, the Posse Comitatus Act (Posse Comitatus) of 1878. As Stanley & Crump report, the FAA has thus far been cautious in allowing unmanned aircraft in the NAS, and has attached strict conditions to their approval. These restrictions apply to military as much as civilian users of UAS; the 174th Fighter Wing in Syracuse, NY that operates the Reaper aircraft is not yet allowed to take off from or land at the airport in Syracuse, but must rather use the Wheeler-Sack airfield 65 miles north at Fort Drum. Lawmakers, lobby groups, law enforcement agencies, and DoD have been working with the FAA to loosen their rules surrounding use of drones in the NAS (Stanley & Crump, 2011).

The other limiting factor to domestic drone use is Posse Comitatus. The purpose of Posse Comitatus is to limit the conditions under which the U.S. military could be used in a civilian law enforcement role. Posse Comitatus prohibits, for instance, the use of military drones for domestic law enforcement surveillance missions. This restriction does not prevent law enforcement from purchasing their own drones, but it is cost prohibitive for local police departments to acquire the top-of-the-line UAS technology, which can cost millions of dollars per aircraft.

What this means from a cyber risk perspective is that civilian federal or law enforcement agencies will likely be purchasing smaller, less expensive aircraft, that lack the sophistication and redundant systems of their military counterparts. Local police

departments are also less likely to treat UAS as an attrition-tolerant platform, since they don't have the procurement dollars the DoD has for buying replacements for crashed or compromised aircraft.

Hobbyists and private citizens. UAS development by hobbyists and other private citizens can be thought of as the next evolution of the R/C aircraft community. There are online communities for people interested in building their own UAS, the most well-known being DIY Drones. From this site, it is possible to find off-the-shelf hardware and free software to build drones capable of performing acrobatics (loops and barrel rolls), with wireless C2 and telemetry, mission planning software, short-term autonomous flight, and mounts for cameras, sonar, and other equipment (DIY Drones, n.d.). Dronepedia, a sort of Wikipedia for UAS, is another site that amateur drone operators (and those aspiring to join them) can go to learn the basics about heavier-than-air flight, telemetry, wireless networks, and aerial photography (Dronepedia, n.d.).

Even the author has been exposed to amateur UAS. One of the author's co-workers has a quadcopter, and in addition to flying it around the office, co-workers have discovered that it is trivial to perform a packet capture on the drone's Internet Protocol (IP) traffic back and forth to the tablet computer that is controlling it over a Wi-Fi wireless network. All that is required is another computer with a wireless network card to listen on the same channel as the drone traffic (there are only a small number of frequencies allocated for Wi-Fi networks).

Hobbyist use of UAS is relevant for several reasons. The first is that they broaden the attack surface; the more types of UAS there are, the more it will draw those wishing to launch a cyber attack against them. They also offer an inexpensive test bed for people

wishing to learn how to attack commercial UAS platforms. Fully autonomous UAS can be had for less than a thousand dollars (much less if the person is willing to build some components themselves). Amateur drones can also be attack vehicles in their own right, and can be used as a modern day civil protest against law enforcement or military use of more sophisticated UAS.

UAS Design Considerations

Now that the current and near-future uses of UAS have been reviewed, an overview of the factors that affect how these systems are designed and implemented will lay the groundwork for understanding how to compromise those systems.

First, it is important to note that the intent of UAS is to be a cost effective alternative to manned aircraft and a way to prevent loss of a pilot's life (Yochim, 2010). Thus, cost is one of the overarching factors that go into UAS design considerations. The simplest of drones can be constructed for under $1,000, and even the military platforms cost less per aircraft than their manned counterparts. Another major consideration is weight. The more an aircraft weighs, the more lift is required to keep it in the air, and the more fuel is needed to propel it. An aircraft's empty weight relates to its wingspan, engine size, how much fuel it needs to be capable of carrying, and how much extra room is left for payload, which may include cameras or other sensors, communications equipment, and armament. This is of particular concern for man-portable UAS, which have to be light enough even at takeoff weight (empty weight, fuel, and payload) to be launched by a person. Even the larger UAS tend to be very lightweight; the Predator has an empty weight of only 1,130 pounds (U.S. Air Force, 2012), as opposed to a Hyundai Accent, a compact car with a curb weight of almost 2,400 pounds (Hyundai, n.d.).

Unmanned aircraft tend to be made of very lightweight materials, and are not built for crash resistance or surviving a surface-to-air or air-to-air attack.

That being said, unmanned aircraft are more than just glorified R/C planes. In addition to the remote piloting capability, the more sophisticated aircraft are capable of fully autonomous flight, typically along a preplanned route. Aircraft like the Predator carry a solid-state avionics suite, multi-mode radar, signal collection capability, and can be outfitted with Hellfire missiles (General Atomics, MQ-1 Predator, n.d.).

Every unmanned aircraft uses wireless communications technology for transmitting and receiving both its C2 and its sensor data. Smaller UAS have used Wi-Fi, or the 33-centimeter (900 MHz) band that is also used by some cordless phones, and industrial and scientific equipment (Tassey & Perkins, 2011). Larger aircraft designed for longer range use may employ satellite communications. For example, the Predator operates in the C-Band for line-of-sight communications, and the Ku-Band satellite communications for longer distances (General Atomics, MQ-1 Predator, n.d.). Communications may be encrypted, although smaller aircraft, particularly the hobbyist models, generally transmit their C2 and sensor data unencrypted. There was a well-publicized incident where insurgents in Iraq were able to monitor a UAS video feed using off-the-shelf hardware and software components, because the feed was being sent unencrypted (Shachtman, 2009). This may seem surprising given the sensitive nature of the mission, but encrypting full-motion video does add hardware and bandwidth requirements, and discovery of the unencrypted feed may have been deemed worth the risk to get the system deployed sooner. In addition, decrypting the video may require hardware and cryptologic keys that are of a higher classification than the ground

personnel using the video hold; the author notes that access to communications security (COMSEC) information is often restricted to a minimal of personnel who have "need to know" privileges.

Keeping COMSEC equipment onboard is also a risk if the aircraft crashes, because that sensitive cryptologic hardware could end up in the hands of an adversary. Nearly all U.S. military aircraft radios use a counter-ECM system called HAVE QUICK. These radios have a complex frequency hopping scheme that relies on two seed values: the time of day (TOD), usually from a GPS receiver, and a word of the day (WOD). These two seeds, together with a network number, are fed into a pseudo-random number generator that controls frequency changes (Crypto Museum, n.d.). Tight controls on the WOD make it unlikely that an attacker would be able to predict the frequency hops, and it's why the TOD and WOD must change if hardware that has already been keyed becomes compromised during mission execution.

Given UAS dependence on data links for C2 information, some of the more sophisticated aircraft have so-called "lost link" procedures built in to them. For instance, the RQ-11 Raven will execute a self-recovery program and return to a preprogrammed recovery point. The RQ-7 Shadow may be determined by its operators to be rogue, and they will command it to launch a recovery parachute, both as an evasion procedure and also to keep it from becoming an obstacle to other local aircraft. Even with these features, communications failure was still the primary cause of 11 percent of Predator accidents, according to a September 2009 report (Yochim, 2010).

UAS come in many different sizes, and their maximum payload, altitude, and range/time on target are affected by the size of the aircraft. The U.S. Air Force Scientific

Advisory Board (2011) categorized UAS into five groups, based on their maximum payload and flight range.

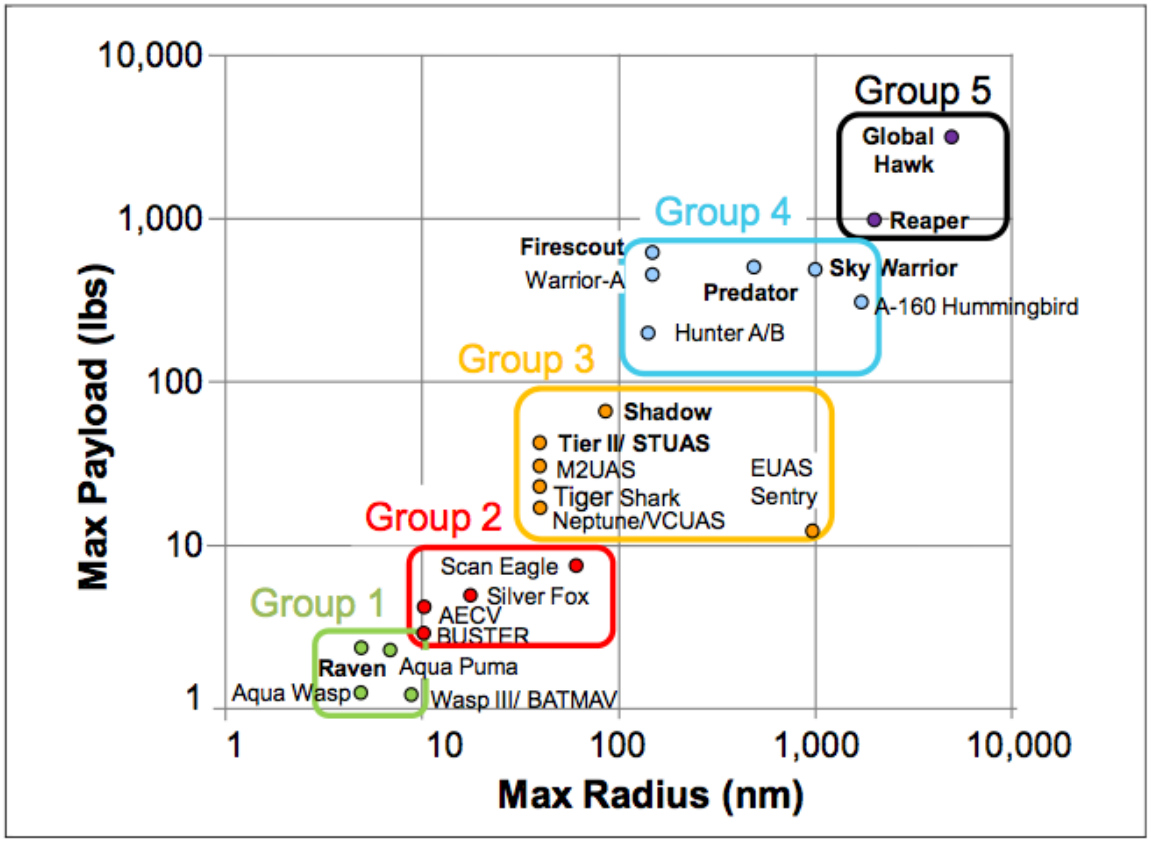

Figure 1: UAS Groupings Based on Maximum Payload and Flight Radius, from "U.S. Air Force Scientific Advisory Board Report on Operating Next-Generation Remotely Piloted Aircraft for Irregular Warfare", p. 3.

Although the chart focuses on payload and radius, the different groups also represent orders of magnitude of cost per aircraft. Groups 4 and 5 are most likely to contain sophisticated communications and intelligence collection capabilities, and are more suitable to weaponization. Thus, Groups 4 and 5 are also more costly to lose, and are not as attrition tolerant as some of the more easily mass produced systems in Groups 1-3. The design decisions made in each of the UAS Groups reflects their cost to replace,

their intended usage, and a tolerance of the risk of loss due to cyber attack or other means.

UAS design limitations generally focus around cost and weight. For medium- and long-range drones, the ability to carry sufficient quantities of fuel is of principal concern, since aerial refueling of unmanned aircraft is not yet possible. Also, because all UAS use wireless communications, they all share common concerns about bandwidth, communications range, jamming, and electromagnetic interference (EMI). The level of concern about these problems, and thus the amount of risk mitigation that needs to be designed into the systems, varies based on how high the aircraft fly and what their mission is, amongst other factors.

Cyber Attacks on Unmanned Aerial Systems

Having reviewed the design considerations for UAS large and small, different types of cyber attacks will now be explored. The first step is to define what exactly is meant by the term "cyber attack". Lin (2010) makes a useful delineation between cyber attack and cyberexploitation. Whereas cyberexploitation is non-destructive and limited to stealing information or other types of unauthorized access to a computer system that a user may never notice, cyber attack

> refers to the use of deliberate actions and operations – perhaps over an extended period of time – to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and (or) programs resident in or transiting these systems or networks (Lin, 2010).

Lin notes that the computer or network being attacked needn't be owned or operated by an adversary, but that it could merely be used to support it. Thus, to call

something a cyber attack would require virtual destruction or degradation of computing or network resources.

Lin goes on to define the necessary conditions of a cyber attack. Cyber attacks require a vulnerability, access to that vulnerability, and a payload to be executed. For example, if a user wanted to infect a ground control station with malicious code that feeds false commands to an unmanned aircraft, they would need to (a) discover an exploitable software bug in the control software, (b) gain physical or remote access to the computer that control software is running on, and (c) inject the malicious code into the control software, either directly into the application or via a lower level exploit (operating system, BIOS, hypervisor, firmware, etc.) These are not easy conditions to achieve, particularly in the classified, encrypted networks that support DoD UAS.

Lastly, Lin describes some of the potential objectives a cyber attacker may be interested in achieving. These include destroying data on a network or a system connected to the network, being an active member of the network and generating bogus traffic, clandestinely altering the data in a database or other data store, or degrading or denying the service on a network (Lin, 2010).

With a good definition of cyber attack, an understanding of the necessary components of a successful attack, and an idea of the outcomes attackers are interested in, detailed examination of proven or potential attack vectors can now be explored.

Cyber attacks on unmanned aircraft. The "cyber" portion of an unmanned aircraft refers to the onboard computer systems; the sensor package and wireless communications equipment. One attack that made the news in 2011 is a GPS spoofing

attack. There is speculation that Iran used GPS spoofing to take over and land a Lockheed Martin RQ-170 Sentinel (Sentinel) in December 2011 (West, 2011).

Tippenhauer, Pöpper, Rasmussen & Čapkun (2011) researched the feasibility of a successful GPS attack of this nature. Their research focused on sending the correct spoofing signals with the right timing, and getting a victim that is already synchronized to the legitimate GPS service to lock onto the attacker's spoofing signal. Several techniques were researched. One was to use a satellite simulator mounted to a truck to attack a target receiver; this approach required an antenna to be in close enough proximity to the victim and thus wouldn't be feasible for higher altitude targets. Another was to capture legitimate GPS signals, time-shift them, then broadcast them with more power than the original signals. The latter approach is the one that will work for authenticated military GPS signals, since an attacker would likely be unable to generate their own spoofing signal that the receiving aircraft would accept. The authors concluded that a successful attack of a high-altitude aircraft is possible, but it requires the attacker to know their location relative to the victim within 22.5 meters (less than 100 feet), which is essentially impossible for high altitude aircraft, or aircraft using military GPS.

Another category of EW attack on aircraft is jamming. Jamming can occur on an aircraft's navigation, telemetry, and C2 signals, or on a sensor data feed that the aircraft is attempting to transmit. Of particular concern is an aerial jammer; an unmanned aircraft would eventually fly out of range of a static jammer, but would have difficulty with a jammer that could follow it at altitude and airspeed. Bhattacharya & Başar (2010) define jamming as "a malicious attack whose objective is to disrupt the communication of the victim network intentionally causing interference or collision at the receiver side". In

their scenario, an aerial jammer intrudes on the communications channel for a multiple UAS formation, although they could also jam the communications between a single UAS and its control station. Their research focused on computing strategies for spatial reconfiguration in the presence of an aerial jammer. Their simulations concluded that unmanned aircraft can take evasive maneuvers to escape the aerial jammer. However, for this to work operationally, the game theoretic software would need to be loaded onto the aircraft and the aircraft itself would have to initiate its maneuvers. For aircraft flying over contentious airspace, this may not be feasible.

Jamming and sensor spoofing were the two cyber threats to unmanned aircraft that had the most scholarly research associated with them. Any system that uses wireless communications has the potential to be jammed, although systems that use frequency hopping and other anti-jamming techniques will be more resistant to jamming than one that operates over Wi-Fi or cellular networks. Trying to perform just-in-time flight path computations to evade airborne jammers is not a feasible option due to unknown airspace conditions in the vicinity of the UAS. Some other countermeasures for jamming will be discussed later in this section. The feasibility of sensor spoofing depends largely on the type of sensor and the defensive capabilities built in to the UAS; any system that encrypts its communications is going to be much more difficult to spoof. Nevertheless, the ability to successfully deny, degrade, or deceive sensor equipment on UAS can negate some of the advantages of using unmanned aircraft.

Cyber attacks on ground stations and networks. As mentioned earlier, a UAS is more than just the aircraft in flight. There are typically one or more ground control stations where pilots control the aircraft, and a network of relays, satellites, and other

infrastructure that ensures the aircraft stays in constant communication with its controlling pilot or computer system. In this section, the vulnerabilities to cyber attack of these system components are explored.

First, the ground control stations will be examined. For medium- and long-range UAS in use by the U.S. military, one or more ground stations are staffed with rated unmanned aircraft pilots. For smaller drones or less sophisticated aircraft, the ground control station might be a personal computer, a mobile device, or a simple remote control. Earlier, the author referenced Carr's (2011) article regarding malicious code that infected a ground control station at Creech Air Force Base (AFB). The U.S. Air Force has maintained that the malware was limited to a Microsoft Windows computer in the ground station that was not connected to the UAS control systems. At the time of this writing, there are no published reports of an external actor breaking into the network that controls UAS such as the Predator and Reaper.

An external attack is not the only one to be concerned with. The 2010 Cyber Security Watch Survey conducted by CSO magazine, in cooperation with the U.S Secret Service, the Software Engineering Institute Computer Emergency Response Team (CERT), and Deloitte, attributes 26% of the cyber security events in 2009 to insiders (CSO Magazine, 2010). Insider manipulation of the classified control networks for military UAS is a potential attack vector, even if it has not yet been realized.

Udoeyop (2010) reviews several cases of insiders abusing their access privileges to exfiltrate data, corrupt information systems, and conduct denial of service attacks. For example, software developer Chris Harn was responsible for network monitoring and maintenance of servers that automated day-to-day betting at Autotone Systems. In 2002,

he altered bets placed by his friends and was able to funnel more than $3 million in illicit earnings to them. In 2008, Marie Lupe Cooley, an administrative assistant at Steven E. Hutchins Architects, deleted architectural drawings valued at $2.5 million from her employer's servers after she suspected she was going to be fired. In 2003, William Shae, a programming manager at Bay Area Credit Services, Inc., planted "time bomb" code on his corporate network after being placed on a performance improvement plan. Two weeks after his termination, the malicious code executed and deleted or modified 50,000 financial records, resulting in a total financial loss of over $100,000.

Each of these insider attacks were perpetrated by people with access to the information systems. The 2010 case of Bradley Manning, the intelligence analyst for the U.S. Army accused of downloading hundreds of thousands of classified and sensitive documents from the DoD's Secret Internet Protocol Router Network (SIPRNet) and sending them to the authors of the WikiLeaks web site while he was deployed in support of Operation Iraqi Freedom, is a reminder than even classified networks can be vulnerable to insider attack (Pilkington, 2012). In light of access restrictions to military UAS C2 networks, the author believes insider threat to be the attack vector with the greatest chance of success in perpetrating a cyber attack against a military UAS ground control station.

Multi-stage cyber attacks. The attack vectors explored thus far have been primary attacks; that is to say, the attacker directly targeted the UAS component and launched an attack on it. However, it is possible that an attack on the UAS could actually be the last in a multi-stage cyber attack. UAS procured by military or law enforcement customers are typically designed and developed by the private sector. It is worth

considering the threat of an attack that originates in a corporation that designs UAS. Two types of these attacks are considered: an intentional or unintentional software backdoor, and a cyber attack on the manufacturer by an external entity.

In software parlance, a backdoor is a method of accessing a software program while it is running that intentionally bypasses normal program authentication or other control mechanisms (The Jargon File, n.d.). Sometimes these backdoors are left by unscrupulous programmers to gain later entry into the system, sometimes they are left by accident (i.e., the backdoor was created for testing purposes, and mistakenly left in the code). A more recognized type of backdoor is a vendor-supplied password, which is essentially a backdoor that a hardware/software vendor acknowledges putting into the system to allow access to it later, perhaps to maintain the system or to reset it if there is an unexpected system failure. As Todd (2003) reports, many of these passwords have been discovered either intentionally or unintentionally by users, opening up security holes in their systems. These backdoors are not always publicized, and it is not likely that the government procurement process includes a thorough review of all source code (software and firmware) that goes into a UAS.

The other type of attack that could leave UAS indirectly vulnerable is a cyber attack on a corporation that designs UAS and that results in exfiltration of sensitive design data or cryptologic key information. In March 2011, the SecurID two-factor authentication system developed by security company RSA was compromised when an attacker exfiltrated information from RSA's internal network (Coviello, n.d.). It is widely believed that this information was used in subsequent cyber attacks against Lockheed Martin and Northrop Grumman (Hypponen, 2011). Security experts speculate that what

was stolen from RSA were "seed values" used to generate token codes normally generated by SecurID authenticators, and that the attackers used this information to clone SecurID tokens and gain access to the Lockheed network (Kaplan, 2011). The attack against RSA was very sophisticated, and involved a mix of phishing (tricking users into trusting an individual or software program), multiple zero-day exploits (software vulnerabilities that have not yet been publicly discovered or disclosed), rapidly deployed malicious code, and an intimate knowledge of the RSA corporate network topology. This type of multi-stage, multi-target attack could be directed towards UAS capabilities in the future. Corporations supplying mission critical technologies such as UAS should not underestimate foreign intelligence agencies' desire to access their information.

On the Likelihood of a Successful Cyber Attack

In aviation, there is a concept known as Operational Risk Management (ORM). One of the assumptions of ORM is that there will be risks inherent in any activity, and that it is necessary to think about the potential risks ahead of time, to define risk mitigation strategies where appropriate, but also to be prepared to acknowledge that a risk is being accepted, either based on the importance of the mission, the likelihood of the risk coming to fruition, or the relative impact of the risk if it does occur (FAA, 2000). UAS usage carries risks, and one of those risks is the potential to fall victim to a cyber attack. The author has already noted that UAS are deployed with varying degrees of attrition tolerance (an acceptance that some aircraft will be lost), and that cost and weight are primary design considerations for the aircraft. With those factors in mind, this section addresses the likelihood of a successful cyber attack, which will lay the groundwork for the section that follows on mitigating the risks of attack.

Existing force protection capabilities. Although the precise configuration and defenses of military UAS are not available publicly, there are some things about their capabilities that can be gleaned from public sources. For example, the Reaper has a triple-redundant flight control system, redundant flight control surfaces, the ability to fly fully autonomous, and operates in the C-Band and Ku-Band frequency ranges for C2 (General Atomics, MQ-9 Reaper/Predator B, n.d.). From the perspective of cyber attack prevention, the key takeaways are that the system can fly fully autonomous (in the absence of a human piloting it remotely), that the system has redundant flight control systems (requiring a potential attacker to attack all three simultaneously for a truly effective attack), and that the system has line-of-sight and satellite communications capabilities, which allow it to resist jamming of one or the other. The Reaper can also operate at an altitude of up to 50,000 feet, and can fly over 200 knots. The operating altitude and airspeed alone make the aircraft itself resistant to ground-based cyber attack.

Not every UAS used by the DoD has such robust defenses. The less expensive, man-portable RQ-11 Raven UAS has an operating altitude of 500 feet AGL, with a range of up to 10 kilometers, and can only be airborne for up to 110 minutes (Yochim, 2010). This leaves the Raven much more vulnerable to the attacks described above. Its low altitude allows for ground-based jamming and sensor disruption attacks, which could be easier to execute than a kinetic attack (e.g., rocket-propelled grenade). Ravens are inexpensive enough such that losing some isn't as costly as losing one of the larger, higher altitude UAS, but if an adversary is able to launch consistent, simple EW attacks against it, it's advantage on the battlefield is greatly reduced.

Returning to the UAS groupings in Figure 1, the author concludes that the aircraft in the lower groupings are at a greater risk of cyber attack. This is not a surprising conclusion, given the differences in cost, sensor capabilities, ability to weaponize, and operating limitations (namely altitude, airspeed, and time on target) of the aircraft.

Difficulty of accessing the UAS network. Simple jamming and other denial techniques have their place, but an attack vector that is potentially more lucrative is one in which the attacker is able to get inside the network, and try to pass off bogus network traffic as legitimate. This would allow an attacker to take control of an unmanned aircraft from its rightful ground controllers. However, to execute this kind of attack requires accessing the network. For military UAS that are controlled on classified, closed loop systems, this is all but impossible. Even the spoofing attacks discussed earlier would be only a temporary victory if the ground station is able to detect when it is no longer remotely piloting the aircraft (e.g., after failing to receive acknowledgment messages, or just by watching what the onboard camera is displaying). Short of an insider attack, the author could not find any technology today that would allow an attacker to break into those secure systems.

However, only the most sophisticated UAS use such tightly controlled systems, and infiltrating networks of less secure UAS is possible. Elston, Frew & Argrow (2006) described their work creating a Wi-Fi network to support multiple UAS in a small geographic region. A Wi-Fi network is easy to detect and connect to using inexpensive off-the-shelf hardware available today, and the SkyNET network penetration techniques described later in this paper could also be used to gain access.

Being able to access the network is also a function of how large the network is. There are entire classes of locally controlled UAS that would be easier to access and still be valuable for an attacker. Some law enforcement agencies have begun to use drones such as the Draganflyer family of RPAs. The controllers for these systems can be purchased commercially, as can the receivers for off-boarded video and other sensor data (Draganfly, n.d.). From the perspective of a criminal enterprise, countering these less expensive drones, or reducing their advantage, forces law enforcement to spend more money on more sophisticated equipment.

Mitigation of Cyber Attack Vectors

Having discussed a variety of cyber attacks on unmanned aircraft and their ground stations, the next question that should be addressed is what to do to mitigate the risks posed by these attacks.

Making the aircraft more autonomous. As discussed earlier, some of the higher end UAS already contain lost link procedures they will follow in the event of a loss of communications with a ground station. A potential risk mitigation strategy to consider is to build retaliatory defenses into the aircraft themselves. Price & Lamont (2006) discuss a self-organized search and attack swarm comprised of multiple unmanned aircraft. They define self-organization (SO) as a principle used by biological entities such as ants, bees, and birds. SO models predict that many agents acting at a low level can produce a system-wide effect that is greater than what can be achieved by purely individual actions. It is nature's implementation of the adage "greater than the sum of its parts". The SO swarm attack scenarios involved several UAS with onboard software that were able to determine how the UAS should behave based on sensor data, and possibly

communications with other local UAS. This type of research would likely be limited to the smaller, less expensive UAS that can be deployed in sufficient quantities to swarm attackers.

In a similar vein, Niland (2006) ran simulations on the ability of UAS to autonomously cooperate in teams to achieve suppression of enemy air defenses (SEAD). His research used MultiUAV, a simulation tool developed by the Air Force Research Laboratory (AFRL). This research was interesting because it linked MultiUAV with the Flexible Analysis Modeling and Exercise System (FLAMES), a framework for developing constructive simulations and to connect other constructive, virtual, or live simulations together. This allows future researchers to build high-fidelity simulations that can test theoretical cooperation of UAS performing complex battlefield tasks.

Improving the durability of the network. There are a number of research thrusts that have to do with making wireless communications networks more resistant to tampering by adversaries. Čagalj, Čapkun, & Hubaux (2007) discuss a wormhole anti-jamming technique for sensor networks. The research is meant to counter stealthy jamming of an appropriate subset of nodes in a sensor network, and introduces the concept of probablistic wormholes, via a combination of a wired pair of nodes in the sensor network, frequency hopping, and uncoordinated channel hopping. Wired nodes would not be suseptable to jamming, and would provide a relay out to the controller (in the case of UAS, a ground control station). This approach works well if wired nodes can be placed in the area of the unmanned aircraft, but if UAS are flying over contested airspace, or access to the ground to establish ground stations is otherwise unavailable,

this approach is not feasible. This approach would work better in the NAS, since the ground stations could be built into existing ground-based FAA navigation devices.

Wood, Stankovic, & Son (2003) discuss a way to detect jamming in swarms of small sensor nodes. The Jammed-Area Mapping (JAM) service allows a group of sensors in a geographic area to isolate where jamming is occurring, so base stations or other anti-jamming support measures can be taken. Sensors detect jamming based on a decrease in utility of a communications channel caused by factors such as bad framing, checksum failures, missing acknowledgment messages, and low signal-to-noise ratio. They broadcast a jam message to neighboring nodes, who will work to isolate which nodes in the sensor network are being jammed, as shown below.

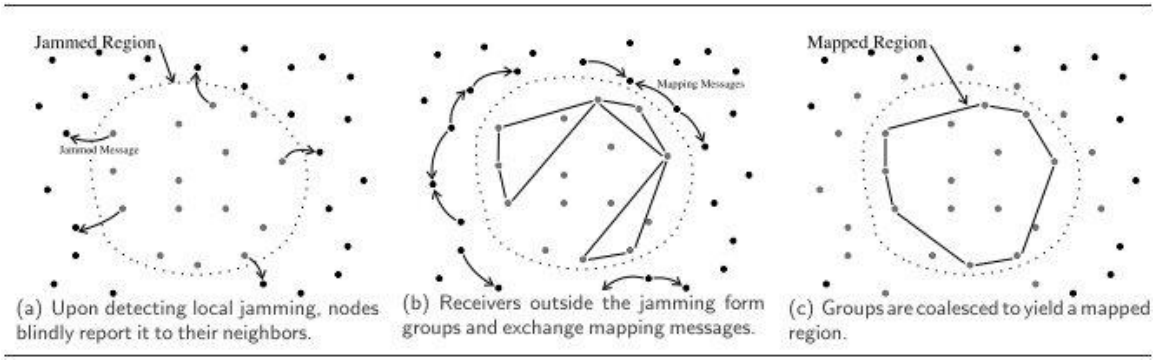

Figure 2: A Visual Representation of the JAM Algorithm. This illustration is showing nodes working collaboratively to identify a jammed region in a network. From "JAM: A Jammed-Area Mapping Service for Sensor Networks" by A.D. Wood, J.A. Stankovic, and S.H. Son, 2003, *IEEE International Real-Time Systems Symposium*, p. 288.

JAM and other techniques for detecting jammed regions in sensor networks are most applicable to groups of small UAS flying together, and are less relevant to a single high-altitude UAS that would likely be resistant to jamming anyway because of its

operating altitude. A potential application for this kind of technology is for small UAS that are deployed as a group to conduct low-altitude surveillance.

Another approach to UAS network security is to take the technologies being used by higher-end UAS, and find inexpensive ways to move them down to the smaller and less expensive drones. L3 Communications produces the ROVER series of portable receivers and transceivers that can securely communicate with UAS over Ultra High Frequency (UHF), C-Band, and satellite communications frequencies (L3, 2011). These units are designed to be used in austere conditions, and incorporate military encryption schemes, so they are surely not inexpensive. However, given the way the hobbyist community has decreased the cost of deploying a simple drone, the author believes a "poor man's ROVER" is inevitable. Being able to cheaply and securely communicate, using built-in anti-jamming techniques such as channel hopping, and using encrypted communications to avoid spoofing will help to make less expensive UAS more resistant to cyber attack.

On the Use of an Offensive Cyber Attack UAS

Thus far, the author has focused on defending "blue force" (friendly) UAS from a cyber attack initiated by a hostile adversary. This section will consider the use of an unmanned aircraft to prosecute a cyber attack.

Perhaps the most well-known cyber attack drone, at least in the hobbyist community, is the Wireless Aerial Surveillance Platform (WASP) demonstrated at the 2011 DEFCON security conference. The designers started with a U.S. Army surplus WASP drone and outfitted it with electronic attack capabilities. The WASP has a miniature computer with 32 gigabytes of storage onboard running BackTrack Linux, a

customized version of the Ubuntu Linux distribution that contains a suite of network vulnerability scanning and penetration testing tools (BackTrack Linux, n.d.). Using BackTrack Linux allows attackers to compromise wireless networks and to exploit vulnerabilities in PCs on those networks. The WASP also has a GSM cellular antenna, and can spoof a cellular tower and record its interactions with any GSM devices that connect to it (Humphries, 2011). The WASP is interesting for several reasons. The first is that it can be built with surplus components and hardware and software available to anyone. There is no special engineering talent required to replicate the WASP. The second is that the WASP can fly fully autonomous along a pre-planned route, allowing the attackers who launched the aircraft to remain undetected while the drone is conducting the attack.

Reed, Geis, & Dietrich (2011) propose an interesting use of drones called SkyNET, which is used to compromise computers on home wireless networks, and to use those computers as bots in a botnet where the botmaster is not actually connected to the Internet. In their research, they fly one or more unmanned aircraft over a proximal urban area looking for Wi-Fi networks. Once a connection to a wireless network is established, the drones attack computers on the network and leave a bot on the computer allowing for remote access and remote execution of botnet C2 instructions. Subsequent drone flights can be used to issue commands to the botnet, and the botmaster does not need to be connected to the public Internet to issue those commands.

There are several novel ideas at work in this scenario. First, to overcome the lack of computational power on the drone itself, the work of cracking wireless network keys is off-boarded via a 3G cellular data connection to an Amazon Elastic Cloud Compute

(EC2) instance. EC2 is a web service that provides resizable computing capacity in the cloud (Amazon.com, n.d.). EC2 instances are essentially pay-as-you-use virtual machines, but they can be started, stopped, and cloned via a web service as the need for computing power fluctuates. This expandable processing capability makes up for the relatively small amount of computing power on the drone. Also, it's interesting to note that SkyNET is built with commodity hardware and software, including an ARM4 250 megahertz processor (which is less power than an average smartphone has in 2012), a quad-band Mini-PCI wireless network card, the Debian Linux operating system to drive the hardware, and an installation of the Metasploit penetration testing framework (Reed, et al., 2011). Lastly, the botnet that gets injected into the host computers on compromised wireless networks is not easily traceable to a botmaster. Even if the malicious code is discovered, it cannot be reverse engineered to find who the bot is communicating with.

Lastly, a combination airborne and ground node attack is considered. At the 2012 ShmooCon security conference, a researcher presented his Falling or Ballistically-launched Object that Makes Backdoors (F-BOMB) sensor package. Built for under $50 from a repurposed cloud storage hardware device called a Pogoplug, the F-BOMB can be dropped from an unmanned aircraft and outfitted with a Wi-Fi antenna or any other sensor the attacker wishes to deploy (Greenburg, 2012). It's essentially a disposable sensor network, because if any one sensor is discovered, it was inexpensive enough to lose. There are a number of cyber attack ideas that can grow from these devices. They can be dropped (by air, thrown over a fence, etc.) and can compromise wireless networks within range. Because they can be left on the ground, they overcome the problem of a UAS running out of fuel before it can attack the network. Once in position, a drone can

be flown over the area where the units have been dropped, and read the data off of them. It allows for persistent surveillance without having to keep an aircraft airborne.

Summary

In this section, scholarly and popular literature relevant to the research questions has been reviewed. The goal was to find supporting and opposing evidence to answer how UAS are vulnerable to cyber attack, what the impact of an attack would be, how likely a successful attack would be, what countermeasures can be employed to mitigate the risk of an attack, and lastly, what a cyber attack conducted by an unmanned aircraft might look like.

The employment of UAS in the DoD, law enforcement and federal agencies, and the hobbyist community were all explored. It was noted that DoD has thousands of unmanned aircraft in their inventory, the majority of which are man-portable UAS that can be launched by hand. Groupings of UAS based on their maximum payload and effective range were presented, and the author concluded that the smaller UAS would likely be an easier target for cyber attack. Current law enforcement uses of UAS were listed, along with the potential limitations of UAS usage by civilian entities, particularly their use in the U.S., and Posse Comitatus, which may restrict how military UAS are used over domestic airspace. Lastly, the latest developments in the hobbyist community were considered.

Next, the design considerations of UAS were reviewed, namely cost and weight. One of the principal advantages to using unmanned aircraft is that they are less expensive than their manned counterparts. However, as the sensor packages and other capabilities become more sophisticated, that cost advantage begins to erode. Weight is also an issue,

because a heavier aircraft requires more propellant and more lift (i.e., a bigger wingspan) in order to operate. Every offensive and defensive capability that is added to a UAS must be done with weight in mind.

The author then explored current and potential UAS cyber attack vectors. Attacks against an unmanned aircraft itself involved mostly spoofing or other attacks against the sensor package, or a jamming attack to deny the aircraft the ability to perform its mission. Attacks against the ground station and supporting network were also considered. Although military ground control stations may be operating in a closed loop system, they are still vulnerable to an insider attack, or to being the endpoint in a multi-stage attack that starts by acquiring other information that can be used to break into the secure system. Also, less sophisticated support networks used by less expensive UAS are more vulnerable to a successful attack that could negatively impact mission effectiveness. Fortunately, numerous defenses against these attacks are already in place, and those defenses were surveyed as part of the literature review.

Having discussed attack vectors, numerous mitigation strategies were then considered, including making the aircraft more autonomous and resilient to electronic attack, and also making the network that supports the aircraft more durable and resistant to jamming and other attacks.

Lastly, the focus shifted from attacks on blue force aircraft to the idea of creating a UAS to prosecute a cyber attack. Three different approaches were considered, including a single aircraft in a single flight, one or more aircraft in multiple flights to create a botnet not easily attributed over the Internet, and a hybrid approach of dropping disposable ground-based sensors and controlling them via an unmanned aircraft.

Having reviewed the relevant literature, the next section will discuss the themes of the findings from the literature, a comparison of findings to existing research, and the limitations of this study.

Discussion of the Findings

In the previous section, scholarly and popular literature relevant to the research questions were summarized and analyzed. In the pages that follow, the themes that emerged from the literature review will be discussed, comparisons will be made between these themes and other relevant scholarly literature, and the limitations of the author's research will be addressed.

To recap, the research explored during the literature review was summarized and analyzed in the context of the previously defined research questions:

- What are the ways each component of a UAS is vulnerable to cyber attack?
- What is the impact of a successful cyber attack?
- What is the likelihood of a cyber attack being successful?
- What countermeasures can be employed to mitigate the risk of attack?
- What are the implications of creating offensive cyber UAS capabilities?

The literature review provided an in-depth study of the major uses of UAS, the constraints that shape how all UAS are designed and built, a definition of cyber attack to use while considering answers to the research questions, a survey of the latest cyber attack methods, a discussion on the likelihood of cyber attack, risk mitigation strategies, and finally, a discussion of UAS for offensive cyber operations. The literature review was structured in this manner to bring a reader from only passing familiarity with UAS to a more comprehensive understanding of how they're employed, how they can be attacked,

and how to prevent those attacks. Sources were selected based on their relevance to UAS, although not all of the scholarly literature related directly to flying unmanned aircraft. For example, there has been research on wireless sensor networks that is applicable to a UAS scenario, and those sources were also incorporated where applicable.

Earlier, in the opening section, it was noted that this research focused on the concept of risk. The components of risk defined by the author were the vulnerabilities of a system, the impact of an attack on the system, the likelihood of an attack, and the countermeasures that can be deployed to reduce the magnitude of vulnerabilities, impacts, or likelihood. With the research questions and the components for a qualitative risk analysis in mind, the major findings can now be reviewed.

Major Findings

The themes that emerged during the research are that (a) the bigger budget UAS platforms are considerably more resistant to ground-based cyber attack than the less expensive platforms; (b) UAS cyber attack risk over U.S. airspace has the potential for a greater impact than one over foreign airspace, and thus needs to be considered when allowing UAS to fly in the NAS; (c) indirect and multi-stage cyber attacks are a subtle threat and could have a greater impact than a direct airborne cyber attack; and (d) as other nation states develop more sophisticated UAS capabilities and electronic countermeasures, the risk of cyber attack increases across the spectrum of blue force UAS operations, and the U.S. should be prepared for this.

Variance in the likelihood of a successful cyber attack. The susceptibility of an unmanned aircraft to cyber attack depends greatly on its operating altitude and airspeed. Aircraft in Groups 4 and 5 in Figure 1 (shown earlier in the Literature Review) operate at

an altitude that leave them out of range of some traditional electronic attacks (e.g., jamming). Getting a malicious signal strong enough, and directed efficiently enough, to interfere with satellite or line-of-sight signals to those aircraft requires sophisticated radio equipment and is all but impossible given the precision with which the attack signal needs to be directed.

For high-altitude UAS platforms, the most plausible cyber attack on aircraft systems would need to come from another airborne system. This is not an unrealistic threat, as Bhattacharya & Başar (2010) discussed. All wireless communications are inherently subject to some EMI, including jamming and spurious emissions or other accidental interference on the frequency. This vulnerability exists even for the UAS equipped with redundant avionics and control systems. The impact of these signal interruptions varies by platform. If a UAS is equipped with lost link procedures, it may be able to fly to its designated safe point if it loses communications with its remote controlling pilot. However, if the navigation and telemetry signals are degraded, this navigation can be difficult or impossible. There is no consensus on the likelihood of such an airborne cyber attack. The attacking aircraft would need to have a comparable operating altitude and cruising airspeed as the target UAS, and at the present time there are few if any adversaries of the U.S. that has such aircraft in their inventory (at least, not ones that are unmanned). Some countermeasures for an airborne cyber attack were discussed in the literature review, such as the jammer mapping algorithm Wood, et al. (2003) proposed. There has also been promising anti-jamming research specific to GPS. Abbott (2002) examines some of these studies, which include the use of “adaptive processing algorithms and antennas that reject unwanted signal interference”, as well as

the development of microelectromechanical Intertial Measurement Units (IMUs), which can be embedded in a GPS antenna and can help narrow the amount of bandwidth a GPS receiver needs to calculate position.

Although large UAS that fly high-profile missions such as the Reaper get a lot of media attention, the author believes the most interesting uses lay with the smaller, less sophisticated UAS, to include man-portable, hobbyist, and some lower altitude systems that law enforcement agencies and other organizations have expressed interest in using. These UAS have a different risk profile than their higher altitude counterparts. Flying lower to the ground, sometimes as low as 500 feet AGL, makes these aircraft much more susceptible to ground-based cyber attack. Weight restrictions prevent these smaller systems from carrying redundant avionics and communications equipment, making them more vulnerable to simpler kinds of jamming or spoofing attacks. Although the likelihood of a successful attack may be higher, one might argue that the impact is lower; the systems are designed to be inexpensive enough to lose. This may be true of a single drone, but those cost savings don't scale. For example, the U.S. Air Force just awarded a $4.2 million extension to a contract with AeroVironment, Inc. to provide an unmanned loitering munitions system known as Switchblade. Switchblade is a tube-launched UAS that can fly over a hostile area providing a live video feed to a ground station. When a target is confirmed, the drone can launch a strike (Mortimer, 2012). This system can be deadly, but if its advantage can be negated with off-the-shelf antennas and jamming or spoofing equipment, then that's $4.2 million that could have been better spent. There are countermeasures available, such as those that were suggested above for more expensive UAS, or incorporating encryption-based communication and avionics redundancy

features from bigger systems into the smaller ones. However, those countermeasures come with a monetary and weight cost, and if one of the primary advantages of a UAS is its small size and low cost, those countermeasures may not be worth implementing. In that case, accepting the risk of attack might be the best option.

One of the advantages of the smaller/cheaper UAS philosophy is that they can be deployed in greater numbers. Redundancy in the context of less expensive drones may involve launching multiple drones at a time. Earlier, the author discussed the use of swarming drones by Price & Lamont (2006), and other research in this area is being conducted as well. Brigham Young University researchers are currently working on an effort funded by C-UAS to perform in-flight geolocation on multiple UAS when some of those aircraft are not equipped with GPS, or if their GPS capability is being denied or degraded (Beard, 2011). This type of cooperative participation by multiple UAS may act as a countermeasure when cyber attacks are being conducted against one or more UAS in a hostile area of operations.

The operating altitude and airspeed of a UAS are perhaps the most significant factors when considering the likelihood of cyber attack that aircraft faces. The larger, higher-flying aircraft are more immune to less sophisticated attacks and most if not all attacks that are ground-based. Smaller UAS are more susceptible to attack, but could also be deployed in greater numbers as a countermeasure to the increased likelihood of a successful cyber attack. Also, UAS of all types are more vulnerable to attack when they are dwelling over targets, as opposed to moving to or from their launch site. The impact of a successful attack is greater as well, since uninterrupted use of the onboard sensor equipment (e.g., video feeds) is most critical during these dwell times.

Risks of UAS usage over domestic airspace. To date, the most common use of UAS by the U.S. has been in overseas ISR and strike missions, and also some border patrol missions along the U.S.-Mexico border. On February 21, 2012, President Obama signed a law that requires the FAA to begin allowing small UAS (under 4.4 pounds) operated by law enforcement to fly in the NAS within 90 days. The law also compels the FAA to ease its restrictions on the use of autonomous aircraft by private citizens by September 30, 2015 (Wingfield & Sengupta, 2012). This loosening of restrictions is going to come with a heightened vulnerability of cyber attack on drones flying domestically. Vulnerabilities that were previously identified on UAS flying over foreign nation states apply equally for those flying in the NAS. Jamming, spoofing, ground station disruption, and ground-based network attacks are all possible in the U.S. Cuadra & Downs (2006) discussed the use of the T-Hawk micro air vehicle and Draganflyer X6 miniature helicopter. Both of these aircraft operate at lower altitudes and would be vulnerable to a disruption from ground-based attackers. Although a cyber attack may be beyond the capabilities of an average citizen, it stands to reason that criminal enterprises, drug cartels, and the like would want to develop capabilities to counter these new law enforcement tools, to include launching drones of their own to swarm the ones used by law enforcement.

A notable difference between foreign and domestic use of UAS is in the impact of a successful cyber attack. If a drone's capability is degraded or if the aircraft itself is crashed in hostile territory during military operations, it could be viewed by the American people as merely the cost of doing business. If a drone falls out of the sky into the backyard of a U.S. citizen, or onto a highway in rush hour traffic, it could have a

significant impact on the public's perception of UAS and their utility and feasibility. One of the research thrusts of C-UAS is the technical and policy issues when integrating UAS into domestic airspace. This includes sense and avoid (SAA) technology; the navigation systems and procedures used to keep a UAS from intruding on the airspace of manned aircraft or other obstacles (e.g., antenna towers). C-UAS is currently funding an in-depth survey of the latest in SAA technology, with the goal of documenting SAA requirements and identifying candidate technologies (McLain, 2011). General Atomics is in the process of developing an SAA radar system called Due Regard, which can be installed on their Reaper UAS (General Atomics, 2012). SAA is an interesting problem from an attack risk perspective. Building onboard sensors and computing equipment may be cost prohibitive and likely too heavy for smaller UAS, but ground-based sense and avoid (GBSAA) would need to communicate wirelessly with the aircraft, and is thus vulnerable to the types of attacks examined earlier. Cyber attacks targeting SAA systems could have a significant impact, because an unmanned aircraft would be unable to react to nearby aircraft or obstacles.

Perhaps the worst-case scenario is an attack over domestic airspace on a UAS that is armed. Military Operating Areas (MOAs) are well-marked on aeronautical sectional charts used by private and commercial pilots, so an attacker would know where they need to launch their attack. Fortunately, the likelihood of high-altitude attacks has thus far proven to be negligable, but if an attacker was able to construct an airborne cyber attack capability and launch it into an MOA, it could have devastating consequences. Coutermeasures for this type of threat already exist, in the form of range monitoring systems and personnel, and the inherent difficulty of private citizens procuring a drone

that could fly at the required airspeed and altitude. As UAS proliferate and an aftermarket (or black market) for surplus UAS becomes available in the coming decades, more sophisticated UAS may be available for purchase by private parties with enough money.

The proliferation of UAS in the NAS will occur by September 2015, as the FAA is mandated to overhaul its drone regulations to allow more use of drones by private citizens, corporations, and law enforcement agencies. A recurring theme of the author's research is that every attack that is imaginable over foreign airspace could also occur over domestic airspace. A successful attack over domestic airspace has the potential to have a greater impact on public opinion on the use of UAS in the NAS, and that could affect the ability of law enfocement agencies and private citizens to operate drones in the U.S.

Indirect and multi-state attacks. Most of the research on UAS vulnerabilities focuses on a direct attack on either the aircraft's sensor package, or the ground control station. This type of direct attack would be very difficult on military UAS and other systems that use encryption-based communications. Two different types of attack vectors against these hardened targets were considered during the literature review: an attack by an insider, and a multi-stage attack whereby the encryption method was compromised prior to the attack on the UAS.

Several cases of insider threat were discussed in the literature review: the Harn case where software systems used for managing horse racing wagers were manipulated, the Cooley case where intellectual property was deleted from file servers, and the Shae case where an attack was pre-planned and executed after the employee was dismissed from the company (Udoeyop, 2010). These three cases represent three distinct ways in which a person with sufficient access can sabotage a computer system. Harn was able to

bypass the authentication and software controls for the betting system and enter a winning ticket into the system four races in to a six-race series. Cooley simply deleted files, which were likely recovered later with forensics tools that can recover deleted data off of a hard drive. Shae planted a software program designed to run at a specific date and time, which then proceeded to delete data from the company servers.

An insider attack on military UAS could also take several forms. The attacker could compromise COMSEC cryptologic keys. Compromised keys would allow an unauthorized user to decrypt the communications between the aircraft and its ground station or satellites. Malicious software could be introduced into the closed loop system that is used to remotely pilot the aircraft. It is important to note that this type of attack may very well be impossible. The details of ground stations for the military UAS are not readily available to the public. Nevertheless, the U.S. has experienced a number of high-profile espionage cases over the years, and it's not out of the realm of possibility that UAS technology would be of interest to foreign intelligence services and non-state actors. This is particularly an issue when considering the number of UAS hardware and software components that are manufactured by foreign companies.

The other attack vector that was explored was an external compromise of encryption systems or other sensitive UAS design details that could be used to launch a sophisticated attack against the UAS. The author provided the analogy of the RSA breach, in which seed values for SecurID systems were compromised and used to generate bogus SecurID authentication codes used to breach the network of the defense contractor Lockheed Martin (Kaplan, 2011). The level of effort required to conduct this attack cannot be overstated, and if companies like RSA and Lockheed Martin can be

compromised, then any company can. A good way for a potential attacker to get information about Predator and Reaper systems would be to penetrate the network at General Atomics, the company that makes those UAS. The RSA breach started with a simple phishing E-mail that contained a Microsoft Excel spreadsheet infected with a malicious macro virus (Hypponen, 2011). It used a combination of simple methods, like phishing, with more complex methods, like custom compiling malicious code and injecting it soon thereafter into the network. It is likely that only a nation state would have the resources to plan and execute such an attack, but this is exactly what nation states are already doing. The U.S. government has long held that the Chinese government has been persistently attacking government and corporate networks and exfiltrating sensitive information about defense industrial base technologies in an operation the U.S. has termed Titan Rain (Thornburgh, 2005). With the importance of UAS in warfare and law enforcement, the probability of foreign governments looking for UAS intellectual property is high.

Insider threat and advanced persistent threat (APT) attacks that are used to compromise UAS and their networks are only two examples of what the author has termed multi-stage attacks. It is important to reiterate that there have been no confirmed or suspected cases of these types of attacks, and they will be very difficult to carry out. However, given the level of sophistication of other cyber attacks that have been seen, the author believes it is only a matter of time before closed loop networks employing encryption and other defensive measures are found to be vulnerable to exploitation.

The emergence of a UAS arms race. The U.S. has enjoyed a near monopoly on the use of UAS for strike missions. This exclusivity will soon come to an end, as other

nations work to develop similar capabilities. This creates policy, technology, and military challenges for the U.S. The final theme that emerged from the research is that any UAS capability developed and deployed by the U.S. will eventually be deployed by nation states and non-state actors that are adversaries to the U.S. or its allies, and may be deployed sooner than we would hope.

In November 2010, at the Zhuhai air show in China, Chinese companies unveiled 25 different models of RPAs, and showed an animation of a missile-armed drone launching a strike on an armored vehicle and attacking a U.S. aircraft carrier (Shane, 2011). While these capabilities were not yet operational, they provided a clear signal as to the intent of China's defense industrial base, and by extension the Chinese government. The threat of drone warfare is about more than just the technological capabilities of nation states or non-state adversaries such as terrorist groups. There is also a policy angle. Under both the Bush and Obama Administrations, the U.S. has asserted that it has the authority to fly UAS strike missions over sovereign nations and to attack individuals residing within those nations if they are deemed to be a threat, going so far as to attack U.S. citizens in those nations (Shane, 2011). The precedent has been set, and other nation states will cite this precedent when they launch their own UAS over the airspace of other nation states, maybe even flying them over the U.S. itself.

The development of UAS capabilities by other countries is one reason the author chose to review literature on using UAS to conduct cyber attacks. UAS usage will involve more than just ISR and strike. A theme of the author's research discussed earlier was the difficulty of executing a cyber attack on a high-altitude UAS; that attack would be made easier by launching it from a hostile UAS that could keep up with the friendly

one. Less expensive UAS that could be procured by insurgent groups looking to defeat low-flying U.S. Army drones could create another air-to-air UAS battle space closer to the ground, with potentially more destructive impacts if the aircraft lose their telemetry and communications capabilities and fall to the ground.

Air-to-air unmanned combat and drone wars sound like science fiction, but the U.S. has made the use of UAS in combat an international norm, and governments looking to develop similar capabilities will follow our example when conducting their own UAS operations. The use of drones to conduct cyber attacks on other drones, or to disrupt cellular or Wi-Fi networks, or deny or degrade other types of wireless communications, will be a sought-after capability for entities other than the U.S. The risks of the precedent we're setting, and the risks associated with these new attack vectors, are worth considering when deploying UAS over domestic and foreign airspace in the future.

Comparison of the Findings

The major findings of this study – the variance in the likelihood of a successful cyber attack based on the altitude, airspeed, and COMSEC capabilities of a UAS; the existence of cyber attack risks on UAS over domestic airspace; the potential for insider threat or multi-stage APT cyber attacks on UAS; and the risks of other nation states and non-state actors with comparable UAS capabilities – have all been explained in detail. Having reviewed the major themes of the research, it is now prudent to consider how these findings compare to other research that has been done on this topic.

Perhaps the closest study to the author's research is Yochim's (2010) report on the vulnerability of UAS common data links to electronic attack. Yochim focused specifically on man-portable and other tactical, low-altitude UAS. His vulnerability

assessments were restricted just to wireless data links, and how those data links could be susceptible to jamming or other types of EW attacks. That being said, he did review the current uses of UAS, discussing each type of man-portable and tactical system, then reviewed the ways in which these systems are vulnerable. In contrast to the author, Yochim also included research and recommendations related to U.S. Army doctrine on the use of UAS. The evolution of military doctrine to incorporate UAS is an important topic, but was out of the scope of the author's research.

Much of the research that has been published on UAS cyber attack has focused on a specific vulnerability. For example, there is ample research on jamming, and ways to counter jamming. In contrast, the author's study sought to explore the gamut of attack vectors, ranging from attacks against the unmanned aircraft itself (namely its sensor package and communications capability) to the ground stations and other supporting network infrastructure. This is a wider scope that many of the journal articles and scholarly conference proceedings, which is to be expected given the different scope and purpose of a capstone paper as compared to other scholarly literature. Wherever possible, the author tried to provide contrasting views and research that looked at the same problem from different angles; having a broader research scope facilitated this.

In contrast to popular literature on the subject of UAS cyber attack, the author tried to keep likelihood and feasibility of attack in the forefront of the risk calculations at all times. Much media attention was focused on the Sentinel UAS that crashed in Iran in late 2011, and whether it fell by accident (e.g., mechanical or communications failure), whether it was brought down intentionally by its U.S. controllers, or whether Iran was able to bring it down with a cyber attack. Based on the analysis in the literature review,

the latter option seems the least plausible. High-altitude UAS that use encryption-based communications for telemetry and C2 are very unlikely to be successfully attacked from the ground. Existing cyber attack countermeasures, such as encryption-based communications, frequency hopping, and closed loop computer networks were all considered when analyzing the risk of cyber attack.

Lastly, the author's research differs from some of the scholarly literature in that predictions for future cyber attacks are being made. After surveying the landscape of attack vectors that exist today, the author postulated as to what types of attacks might come next. An example of this is an APT attack against a corporation that produces UAS for the DoD; no attack on such a corporation has been publicly acknowledged, but the author believes research shows that such a breach is inevitable, and only the exact nature of sensitive information that will be exfiltrated remains in question. Exploring the use of drones as delivery vehicles for cyber attacks is another example of a novel use of UAS that is either not widely used, or its use is not widely known.

Limitations of the Study

No research is perfect and all encompassing. It is important to acknowledge limitations of research and constraints that affected how this research was conducted. There are three limitations that the author has identified with this research effort: that no original data was gathered during the study, that there is a dearth of publicly available information for specific vulnerabilities of government/military UAS, and that the research focused on breadth at the expense of depth.

Lack of original data. As outlined in the opening section, the intention of this research was to be descriptive, to review and summarize the current state of the art vis-à-

vis cyber attack vulnerabilities of UAS. As a result, no gathering of original data occurred. No controlled experiments were conducted, and no formal surveys of individuals who use UAS or defend them were conducted. This is a limitation because it prevents the author from comparing the research of others to experiments designed specifically to support or criticize that existing research. The major findings produced by this study were induced solely from the information of others.

An example of an experiment that could have augmented the literature review would be to attempt to jam an inexpensive drone using off-the-shelf hardware technology. Talking about jamming in the abstract is good, but attempting to jam a drone is better. Discussing inexpensive off-the-shelf sensor capabilities is not as definitive as actually trying to construct these sensors as cheaply as possible, as O'Connor did in his research (Greenburg, 2012). Additional suggestions for research ideas will be discussed in the recommendations and conclusions sections that follow.

Lack of open source information on government/military UAS. One of the greatest difficulties in conducting research on DoD aircraft is the procurement of publicly available information on capabilities, on tactics, techniques, and procedures (TTP), and on known vulnerabilities. A private citizen cannot just call the Pentagon and ask them to enumerate the ways in which the sensor packages of its UAS can be spoofed. Thus, the research on vulnerabilities is limited to academic papers and news articles.

As discussed during the comparison of the findings, the news media is often sensationalistic in their reporting of cyber threats. The report of malicious code on Microsoft Windows computers in the Predator/Reaper ground control stations is an

example of this; the closed loop system that actually controls the aircraft was not in any danger of compromise, but one wouldn't necessarily know that from the headlines.

In an attempt to establish the credibility of some of the academic papers on electronic attack, the author would search the Internet for the names of the authors of the papers to see what else they had written and what organizational affiliations they had. Security researchers will often publish papers based on work funded by the federal government. By reviewing all of the publications by a particular author, one can see that they have expertise in the appropriate subject areas and are doing funded contract work for agencies such as DARPA, which lends credibility to their research. Using simple methods such as these helped the author to overcome the lack of public information on specific aircraft systems.

Breadth, not depth. The last limitation identified by the author was the focus on breadth, on examining as many cyber attacks and countermeasures as possible, at the expense of depth, of looking at one particular kind of attack in significant detail. A researcher will not be able to take this study and know exactly the steps they should take to mitigate a specific risk, and will likely not know all they need to know on a particular kind of vulnerability. This was a self-imposed limitation; the author consciously chose to keep the focus at a higher level instead of creating original knowledge on a much narrower subject.

These limitations all point to different ways in which the research could have been approached. The focus could have been on evaluating specific technologies, by procuring small UAS and attacking them. Research could have been focused on non-military uses of UAS to overcome the information gap. A specific type of attack could

have been explored in much greater detail. Lastly, a different way to analyze the literature would have been to incorporate ORM, and use that as the model for calculating risk, rather than the vulnerability, impact, likelihood, and countermeasure qualitative analysis that was used in the literature review and discussion of the major findings. According to Civil Air Patrol (n.d.), ORM classifies risks as low, medium, or high based on their severity and probability. The ORM process involves the following steps:

1. Identifying the hazards, the conditions that could cause loss
2. Assessing the risks, quantifying the severity and probability
3. Analyzing risk control measures, actions that can reduce or eliminate a risk
4. Making control decisions, using cost-benefit analysis
5. Implementing risk controls, taking care to truly integrate them with plans, processes, and operations
6. Supervising and reviewing, to ensure controls are having their desired effect

This approach to classifying risks is more structured than the approach taken by the author, but could also be more cumbersome, particularly for assessing risks for cyber attack vectors that have never happened (or have not been publicly disclosed). These limitations notwithstanding, the author still believes the research captured the state of the art of cyber vulnerabilities when using UAS.

Summary

In this section, the major findings of the literature were discussed, and the themes of the research were explored. First, there are significant differences in the likelihood of a cyber attack between different types of UAS. For aircraft that fly at a high altitude and airspeed, an airborne attacker is a more plausible cyber attack scenario. Smaller UAS that

fly closer to the ground are at a higher risk of a successful ground-based cyber attack, and those attacks can negate the cost savings of inexpensive UAS if they can be consistently reproduced. Second, any attack that can be carried out in foreign airspace can be carried out in domestic airspace, and since UAS will become more prevalent in the NAS in the coming years, the risk of a cyber attack on a domestic UAS will only increase. Third, DoD and other users of sophisticated UAS must not discount the possibility of an insider threat attack, or an attack on the intellectual property of the corporations that design these UAS. An attack on a UAS may actually be step 3 or 4 of a multi-stage long-term APT attack perpetrated by a nation state. Lastly, it is important to consider that the ways in which the U.S. employs UAS will be copied by other nation states as they build their own UAS, including governments and non-state actors that are adversaries of the U.S. Precedents for UAS usage are being set by the U.S. and its allies, and it is not out of the realm of possibility that future warfare between nation states will have an unmanned air-to-air combat component to them. Protecting the sensor package, wireless communications, and computer networks that support those attacks will be critical to unmanned air superiority.

In addition to these themes, comparisons were made between the author's research and other research in this area. Similar studies of UAS vulnerabilities have been conducted, typically focusing on one aspect of operations, such as wireless data links. Other research on cyber attack techniques have been narrow in scope, not considering the whole problem of cyber attack from the aircraft sensor package down to the ground station and all points in between. Existing research on using UAS as cyber attack vehicles typically omits discussion of countermeasures for these attacks. UAS cyber attack threats

in popular literature and the media have neglected to discuss likelihood and true viability of these attack vectors.

Lastly, the limitations of this study were discussed. Relying exclusively on the research of others limits the certainty with which conclusions can be stated. Conducting actual cyber attack experiments would have given the author the ability to confirm or refute ideas discussed theoretically in other research. The difficulty of finding publicly available information on military UAS operations was also a limitation, and prevented a thorough analysis of the most well known UAS operations. Lastly, the research focused on breadth at the expense of depth, potentially leaving questions on the specifics of cyber attack vectors for future researchers. Overall, even with these limitations, the author believes the findings are accurate and that the research contributes to the overall body of knowledge on UAS cyber attack vulnerabilities.

Having now discussed the findings and themes that were developed during the literature review, the author will now provide recommendations for future areas of research, and will conclude with a discussion of how each research question was addressed during the study.

Recommendations

Cyber security is a rapidly evolving field of study, and its intersection with UAS is an area that has not yet been widely researched. There are several areas where additional research would be helpful to advance the body of knowledge, which will be particularly important as UAS usage continues to grow. These areas include: investigating emerging solutions for the SAA problem, considering the feasibility of

cloud-based C2, and the development of an international legal framework for nation states operating UAS in foreign and international airspace.

Sense and Avoid Technology

One of the largest areas of research in the coming years will be the development of technology to overcome the SAA problem. Briefly, unmanned aircraft need SAA solutions because they do not have a pilot onboard to perform "visual separation", which is an aviation term meaning that a pilot visually acknowledged other aircraft and ground-based hazards (e.g., antenna towers). This is an issue in controlled and uncontrolled airspace, and at all altitudes. In Class G (uncontrolled) airspace, it is the responsibility of the pilot in command (PIC) to maintain visual separation with other aircraft; even when overseen by a control tower, pilots are typically asked to provide visual confirmation of nearby hazards. There are still many small aircraft that do not contain a transponder or other beaconing technology to transmit their location, and do not fly in airspace that requires contact with a tower. In Class B, C, or D airspace (those classes of airspace where contact with a control tower is mandatory), the pilot remotely operating the aircraft would need to be in contact with the tower, potentially limiting where the pilot is in relation to the aircraft. In the event of an in-flight emergency, pilots are trained to find the best possible landing site and to bring the aircraft in as safely as possible, all while trying to contact a control tower and following emergency "boldface" procedures (steps that must be memorized, and that appear in boldface font in an aircraft's operating manual). It is clear that these issues can have an impact on the altitude and range of UAS operated in the NAS, and thus their feasibility for future applications such as aerial photography and search and rescue (SAR).

There are a number of SAA research efforts underway. As mentioned earlier, General Atomics is developing an SAA radar that resides onboard the aircraft, and it may be ready to deploy as early as 2015 (General Atomics, 2012). Researchers at Brigham Young University are actively researching SAA requirements, and the current state of the art of SAA technology (McLain, 2011). The U.S. Air Force has developed Cooperative Research and Development Agreements (CRADAs) with numerous companies with the goal of making UAS operation in the NAS safe for civil authorities and U.S. citizens (Francis, 2011). Their efforts have focused on GBSAA, which may be a more attainable near-term goal, given the weight and cost considerations of putting SAA equipment on small UAS.

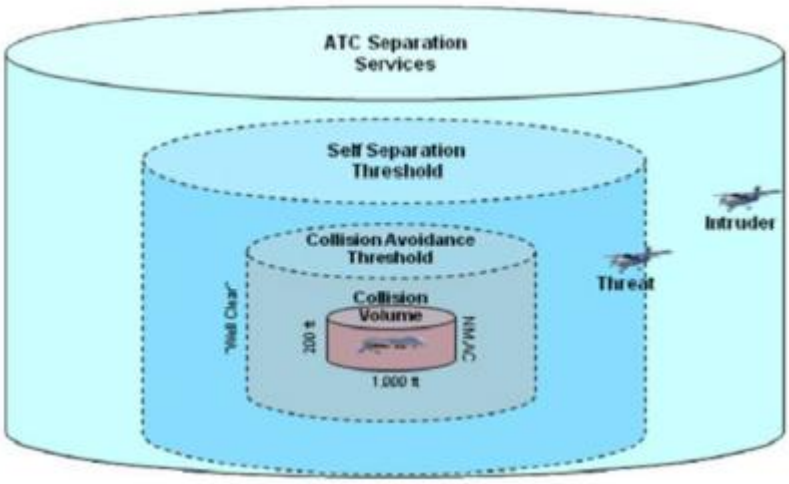

Figure 3: Separation Thresholds between UAS and Manned Aircraft. This illustration shows what is necessary for UAS operation in the NAS, from "Ground Based Sense and Avoid (GBSAA) 101 Overview" by Roger Francis, slide 8.

Although there are numerous SAA research efforts underway, there is always room for new research ideas. The author would like to see research into developing a network of SAA radars on manned aircraft, with the data off-boarded from those aircraft

being aggregated by local control towers. This "crowdsourcing" of SAA data collection would be cost effective if a sufficient number of aircraft were equipped with the technology, and it would alleviate the need for a significant investment in GBSAA, which requires many ground-based radar systems to be deployed nationwide in order to facilitate wide-reaching use of UAS.

Cloud-based Command and Control

Over the last decade, the advances in computing power, the proliferation of inexpensive storage, and the increase in bandwidth penetration have all made the employment of Internet-based computing more feasible. This so-called "cloud computing" is about more than just running servers remotely in a virtual machine. A principal benefit of cloud computing is the ability to rapidly scale, to increase capacity or add capabilities on the fly without having to build out the physical infrastructure (Knorr & Gruman, 2008). Other advantages specific to mitigating cyber attack risk for UAS are fault tolerance and the ability to quickly re-route traffic. Integration of cloud technology into DoD information systems is one of the elements of the DoD's Information Enterprise Strategic Plan, as part of the Information as a Strategic Asset and Interoperable Infrastructure objectives (DoD CIO, 2010), and is thus a relevant research area to consider for future UAS operations.

Using cloud technologies with UAS can take several forms. In the literature review, a cyber attack drone used Amazon's EC2 cloud infrastructure to perform computationally expensive password cracking (Reed, Geis, & Dietrich, 2011). This off-boarding of sensor data into a cloud environment would be useful for all manner of computations, including the aforementioned SAA data aggregation. Off-boarding to the

cloud would allow a large number of consumers to receive sensor data concurrently. A small drone sending a video feed to a single device on the ground can only show the video to one person. A drone sending its video feed to cloud storage could then have its video consumed by many personnel at different locations using different Internet-enabled devices (PCs, tablet computers, etc.).

A long-term strategy for remotely piloting aircraft may be to put the entire C2 infrastructure into the cloud. This approach has several advantages. The software interface to control the drones would be available anywhere, so if one remote cockpit location went offline, another could pick up the C2 feed immediately. If a computer network was compromised, the communications to and from the aircraft could still be protected, because the attacker would also need to gain access to the virtual C2 software. This approach is not without its drawbacks, however. Any additional complexity introduced into a system increases the likelihood that one of the elements can fail. Spolsky (2002) refers to this as the Law of Leaky Abstractions. Spolsky defines an abstraction as "a simplification of something much more complicated that is going on under the covers". The abstraction in this case is pretending that data and programs run from the cloud are just like running them on a computer physically located near the operator. It is not the same, and additional research should be done on secure cloud computing before anything as mission critical as UAS C2 is moved to the cloud. Fortunately, DoD has already been working on more secure cloud solutions. DARPA is funding research on resilient cloud computing platforms (Ackerman, Darpa Looks to Protect Drones From Hack Attacks, 2011). The General Services Administration (GSA) has recently released a concept of operations (CONOP) document detailing how it plans

to assess the security of cloud services providers, as part of its Federal Risk and Authorization Management Program (FedRAMP) (GSA, 2012).

Cloud-based C2 would be beneficial to non-military UAS as well. A single operator could control multiple small UAS from one computer. Existing research that supports this concept include simulation the work by Jin, Minai, & Polycarpou (2003), who demonstrated cooperative real-time search and task allocation in teams of UAS. The combination of more autonomous UAS that are able to work cooperatively, and a C2 framework that could be controlled from any Internet-enabled device, would be a powerful tool for law enforcement, SAR, aerial photography, and a variety of other users.

A Legal Framework for UAS in Foreign Airspace

The author's research has focused largely on technical issues, but there are unresolved legal issues related to the proliferation of UAS, and particularly the use of UAS by one nation state over another nation state's airspace. The final recommendation is to research the feasibility of an international legal framework to facilitate UAS flights, and also, procedures for handing UAS that crash in a foreign country.

Marshall (2009) reviewed International Civil Aviation Organization (ICAO) regulations as they pertain to UAS. ICAO is the United Nations (U.N.) agency responsible for international air navigation procedures. Marshall found that the current definitions of "aircraft" and "aeroplane" are so broad that even an R/C aircraft purchased from a hobby shop would fall under ICAO regulations. In addition, he notes that the current ICAO regulations are ambiguous as to whether civil use of unmanned aircraft in international airspace is permissible, with the legality being largely determined by the laws of the nation state in which the flight originated. Marshall concludes that

> Until ICAO promulgates Recommended Practices and Standards for the certification and operation of unmanned aircraft, or addresses the issue through the Annex amendment process, civil operators of UASs desiring to fly their aircraft at altitudes near the surface of the ocean in international airspace – or at altitudes that do not interfere with traditional commercial operations – currently face no regulatory barriers that would prevent such activity.

The lack of regulatory barriers does not mean it's a good idea for anyone who is so inclined to launch a UAS and fly it into the airspace of another nation state. Research and additional legal reviews are imperative as the U.S. loosens its rules regarding UAS usage, and also as other nation states develop their UAS programs.

Several nation states have UAS experience to draw on when researching international use of unmanned aircraft. Ravich (2009) discusses these efforts. Australia's Civil Aviation Safety Authority has developed guidance on how UAS may be constructed and operated. The Japanese Agriculture Aviation Association has promoted the licensing of unmanned helicopters for crop spraying and plowing rice fields by establishing a UAS registration system, implementing safety standards, and developing training and certification programs. The United Kingdom (U.K.) Civil Airspace Authority developed regulatory guidance relative to UAS usage, establishing that UAS operating in the U.K. "must meet at least the same safety and operational standards as manned aircraft".

In recent decades, it seems that technology has developed at a faster pace than the law. With UAS technology improving every year, it is imperative that research continues into the legality of operating UAS across the borders of nation states. When the Sentinel drone crashed in Iran in December 2011, the U.S. should have been able to cite an

international legal precedent when asking Iran to return the aircraft. The Iranian government may still have refused given the political complexities, but at least the U.S. would have had a legal justification for their request.

Conclusions

The use of UAS by the U.S. military and intelligence community, domestic law enforcement, and private citizens has increased significantly in recent years. From ISR and strike missions overseas, to border patrol, to hobbyists and amateurs, the proliferation of UAS has had and will continue to have a transformative impact in the U.S. and abroad. These ever-evolving applications of UAS highlight the need to protect both the aircraft and the network that enables them from cyber attack.

The purpose of this study was to examine the ways in which UAS of all kinds are vulnerable to cyber attack, and how to best address these vulnerabilities so that the employment of UAS can continue to grow with the lowest risk of disruption possible. To that end, several questions were posed that the study sought to provide answers to. These questions are discussed below.

How Are UAS Vulnerable to Cyber Attack?

UAS have two categories of vulnerabilities: those that affect the sensor and communications equipment onboard the aircraft, and those that affect the ground station and other network infrastructure. Sensor attacks generally take the form of jamming or spoofing, with spoofing being more difficult but also potentially having a bigger impact. Many UAS, especially the smaller, off-the-shelf models, do not encrypt their C2 communications with their remotely operating pilots. This leaves them especially vulnerable to spoofing attacks. Even UAS that use encryption-based communications can

be susceptible to spoofing attacks if the encryption is compromised, either by an insider attack or by an attacker launching an APT attack against the organization(s) responsible for maintaining cryptologic key information.

Attacks on the ground stations or other networks can take several forms. Jamming or spoofing attacks are also possible at the point where the network is broadcasting its wireless signal to the aircraft. If a common wireless communications protocol such as Wi-Fi is used, an attacker could introduce bogus packet traffic to confound the ground station or aircraft. If the ground station resides on a wired network, IP-based cyber attacks can be used to degrade the network's capability or to introduce bogus traffic. Lastly, an insider threat attack can be launched, with the attacker being a trusted user of the network.

What is the Impact of a Successful Cyber Attack?

The impact of a successful attack varies depending on where the UAS is operating, and what the attack was able to do. A successful cyber attack of a military UAS operating overseas could lead to loss of the aircraft and its payload, which could include ballistics. Depending on the acquisition cost of the aircraft, this may be considered the price of doing business; military UAS are designed with a degree of attrition tolerance. However, a successful attack over domestic airspace could bring an unmanned aircraft down on a highway, or onto the private property of a U.S. citizen. These types of accidents could have a significant impact on public opinion of UAS use, and could stymie the expansion of domestic UAS operations.

Although a UAS crash is unfortunate, a cyber attack that results in the attacker taking control of a UAS could be far more serious; it can be essentially stolen out of the

sky, or it can be turned against its remotely operating pilot. If a UAS is brought down intact into hostile territory, its technology can be harvested by the attacker. This would be of particular significance if a military UAS with COMSEC equipment was brought down. Although the cryptologic keys would quickly be revoked, the underlying hardware could be reverse engineered. Unlike manned ISR platforms, an unmanned surveillance drone does not have remote destruction procedures, nor does it have personnel onboard to destroy sensitive hardware and sensor equipment before it can fall into enemy hands.

What is the Likelihood of a Cyber Attack?

Although many worst case scenarios can be envisioned, they remain in the realm of fantasy unless the likelihood of a successful attack can be shown. Indeed, the likelihood of a high-altitude UAS being spoofed or jammed by a ground-based attacker is negligible; for those UAS, only an aerial attacker (manned or unmanned) would be successful in disrupting the communications or sensor equipment. That being said, the smaller, less expensive UAS that fly at lower altitudes, sometimes as low as 500 feet AGL, are at a greater risk of a successful cyber attack. Although these UAS are inexpensive, being able to successfully degrade their capabilities with inexpensive hardware and software negates the advantages that these systems provide.

Also, while attacks on high-altitude unmanned aircraft are unlikely, the ground stations and supporting networks are not immune to ground-based attackers, either via the insider threat vector or by a sophisticated network attack. An attack that is analogous to the RSA breach that then led to the Lockheed Martin breach could occur against military UAS, by first attacking the corporation that designed the aircraft or attacking the military networks on which data about the UAS reside. It’s difficult to gauge the likelihood of a

successful cyber attack on a larger military UAS system because it hasn't happened yet, but it is safe to say that such an attack would be perpetrated by a nation state, and that it would be preceded by a great deal of reconnaissance and possibly cyber attacks against other information systems to prepare for the eventual attack against the UAS.

What Cyber Attack Countermeasures Can Be Employed?

Several different approaches can be taken to reduce the impact or likelihood of an attack. One is to make the UAS more autonomous, so that it can operate even in the absence of a remotely operating pilot. Some high-end UAS already have this capability. UAS that are deployed in groups can have algorithms for cooperative engagement, to work with each other in the event that links to a ground station are lost or degraded. Anti-jamming technologies can also be employed to reduce the impact of a jamming attack. Encrypted communications can greatly decrease the likelihood of a successful spoofing attack. If the redundancy and self-protection technology on high-end UAS is able to trickle down to less expensive systems, it could improve the survivability of those smaller, cheaper UAS.

That being said, every countermeasure comes with a price, in terms of cost and/or weight. The cost savings of small UAS can quickly be erased if expensive ECM or redundant avionics are added to them. This equipment also makes the aircraft heavier, thus requiring a bigger wingspan, a larger engine, and more fuel to operate them. Every capability added to a UAS has a cost and weight tradeoff, and it could be that the UAS operator just accepts the risk of losing some of their aircraft to cyber attack, because the cost of countermeasures are too high.

What are the Implications of Using UAS to Conduct a Cyber Attack?

The preceding research questions have all assumed that the UAS in question is the victim of a cyber attack. However, there has been research into using UAS to conduct cyber attacks, either against other unmanned aircraft or against wireless computer networks. This is a novel use of UAS, and it has the potential to be very effective.

As discussed earlier, UAS that operate at a high altitude and airspeed would be difficult to reach from a ground-based cyber attack. If an adversary was able to launch an airborne cyber attacker, the friendly UAS would no longer be immune to attack. Unmanned air-to-air combat is not as far away from occurring as some might believe. In addition to a single UAS, a swarm of smaller UAS can be used to conduct cyber attacks, most likely on ground-based wireless networks. A benign case would be to fly them over a residential area and compromise or degrade the wireless networks in the houses of private citizens. A more sinister case would be to fly them near corporations that have wireless networks, or in the proximity of military bases. A small UAS would be difficult to pick up on radar, and could be flown surreptitiously into restricted areas. The attacking UAS could drop a sensor package into the area and fly away, if dwelling in the area would be too risky.

As foreign governments and non-state actors develop increasingly complex UAS, the likelihood of using those UAS in cyber attacks against the U.S. and its allies also increases; a UAS doesn't have to be armed with a missile to be dangerous to potential adversaries.

The Way Ahead

Unmanned aircraft are the way of the future. In the coming decades, the author believes UAS will continue to prove their worth in warfare, law enforcement, SAR, crop maintenance, aerial photography and videography, and countless other disciplines. The research contained herein will help UAS designers, customers, and enthusiasts understand the risks of cyber attack on UAS, how those attacks can be mitigated, and what risks will have to be accepted as a cost of operating unmanned aircraft. This research also showed how the growing field of cyber security – of protecting the computers and protecting the network – has implications beyond just corporate networks or data centers.

A cyber attack on a UAS would require a persistent adversary, particularly one targeting military systems. A successful cyber attack could be devastating, but countermeasures do exist today, and emerging research on anti-jamming, autonomous operating, secure cloud computing, and SAA will make domestic and international use of UAS safer and more versatile in the future. Exploring the risks of cyber attack on UAS is not an admission of defeat; it is taking the first step towards mitigating these risks and employing UAS to their full potential.

Appendix

Glossary of Terms

ACLU – American Civil Liberties Union

AFB – Air Force Base

AFRL – Air Force Research Laboratory

AGL – Above Ground Level

BDA – Battle Damage Assessment

C-UAS – Center for Unmanned Aircraft Systems

C2 – Command and Control

CBP – Customs and Border Patrol

Cloud Computing – Using Internet-based servers to store, process, or manage data, as opposed to using servers local to the user

COMSEC – Communications Security

CONOP – Concept of Operations

CRADA – Cooperative Research and Development Agreement

CSAR – Combat Search and Rescue

Cyber – Pertaining to computer systems or networks

Cyber Attack – The use of deliberate actions and operations to alter, disrupt, deceive, degrade, or destroy computer systems or networks

Cyber Security – A field of study focused on the protection of computer systems or networks

DARPA – Defense Advanced Research Projects Agency

DDoS – Distributed Denial of Service

DEA – Drug Enforcement Administration

DoD – Department of Defense

ECM – Electronic Countermeasures

EMI – Electromagnetic Interference

EOD – Explosive Ordinance Disposal

EW – Electronic Warfare

F-BOMB – Falling or Ballistically-launched Object that Makes Backdoors

FAA – Federal Aviation Administration

FBI – Federal Bureau of Investigation

FLAMES – Flexible Analysis Modeling and Exercise System

FY – Fiscal Year

FedRAMP – Federal Risk and Authorization Management Program

GBSAA – Ground-based Sense and Avoid

GPS – Global Positioning System

GSA – General Services Administration

GSM – Global Standard for Mobile Communications

ICAO – International Civil Aviation Organization

IMU – Inertial Measurement Unit

IP – Internet Protocol

ISR – Intelligence, Surveillance, and Reconnaissance

JAM – Jammed Area Mapping

MOA – Military Operating Area

NAS – National Airspace System

NATO – North Atlantic Treaty Organization

PIC – Pilot in Command

R/C – Remote Control

RPA – Remotely Piloted Aircraft

SAA – Sense and Avoid

SAR – Search and Rescue

SEAD – Suppression of Enemy Air Defenses

SIPRNet – Secure Internet Protocol Router Network

SO – Self Organization

TCP – Transmission Control Protocol

TOD – Time of Day

TTP – Tactics, Techniques, and Procedures

U.K. – United Kingdom

U.N. – United Nations

U.S. – United States

UAS – Unmanned Aircraft Systems

UAV – Unmanned Aerial Vehicles

UDP – User Datagram Protocol

UHF – Ultra High Frequency

WASP – Wireless Aerial Surveillance Plane

Wi-Fi – IEEE 802.11 standard for wireless communications networks

WOD – Word of the Day

References

Abbott, A. (2002). *Antijamming and GPS for Critical Military Applications*. Retrieved from http://www.aero.org/publications/crosslink/summer2002/06.html

Ackerman, S. (2011, November 7). *Darpa Looks to Protect Drones From Hack Attacks*. Retrieved from http://www.wired.com/dangerroom/2011/11/darpa-cybersecurity-drones/

Ackerman, S. (2011, October 20). *Libya: The Real U.S. Drone War*. Retrieved from http://www.wired.com/dangerroom/2011/10/predator-libya/

Airforce-Technology.com. (n.d.). *Predator RQ-1 / MQ-1 / MQ-9 Reaper - United States of America*. Retrieved February 1, 2012, from http://www.airforce-technology.com/Projects/predator-uav/

Amazon.com. (n.d.). *Amazon Elastic Compute Cloud (Amazon EC2)*. Retrieved February 10, 2012, from http://aws.amazon.com/ec2/

Anderson, C. (2010, May 1). *ArduPlane home page*. Retrieved January 22, 2012, from http://diydrones.com/profiles/blogs/ardupilot-mega-home-page

BackTrack Linux. (n.d.). *About BackTrack*. Retrieved February 11, 2012, from http://www.backtrack-linux.org/about/

Beard, R. (2011, July 15). *Brigham Young University Proposed Projects*. Retrieved February 9, 2012, from http://c-uas.byu.edu/sites/c-uas.byu.edu/files/userfiles/7/BYU12-01%20GPS%20Denied-Cooperative%20Localization.pdf

Bhattacharya, S., & Basar, T. (2010). *Game-theoretic analysis of an aerial jamming attack on a UAV*. American Control Conference (pp. 818-823). Baltimore: American Automatic Control Council.

Čagalj, M., Čapkun, S., & Hubaux, J.-P. (2007). *Wormhole-Based Antijamming Techniques in Sensor Networks*. IEEE Transactions on Mobile Computing, 100-114.

Carr, J. (2011, October 10). *Cybersecurity Issues with Predators, Reapers, and Unmanned Aerial Systems*. Retrieved from http://jeffreycarr.blogspot.com/2011/10/cybersecurity-issues-with-predators.html

Civil Air Patrol. (n.d.). *Basic Level Operational Risk Management*. Retrieved from https://www.capnhq.gov/SafetyEducation/ORM_Basic_Course.pps

Coviello, A. W. (2011). *Open Letter to RSA Customers*. Retrieved from http://www.rsa.com/node.aspx?id=3872

Crypto Museum. (n.d.). *HAVE QUICK Frequency Hopping System.* Retrieved March 4, 2012, from http://www.cryptomuseum.com/radio/havequick/index.htm

CSO Magazine. (2010). *2010 Cyber Security Watch Survey - Survey Results*. CSO Magazine.

Cuadra, A., & Downs, K. (2011, January 23). *Drones on the home front*. Retrieved from http://www.washingtonpost.com/wp-srv/special/nation/drone-gallery/?sid=ST2011012204147

C-UAS. (n.d.). *Topics*. Retrieved January 22, 2012, from http://c-uas.byu.edu/content/topics

DIY Drones. (n.d.). *ArduCopter Quad v1.0 Fully Assembled*. Retrieved February 4, 2012, from https://store.diydrones.com/ArduCopter_Partial_Kit_V1_0_p/kt-arducopter-04.htm

DoD CIO. (2010). *Department of Defense Information Enterprise Strategic Plan 2010-2012*. Washington, D.C.: Department of Defense.

Draganfly. (n.d.). *Draganflyer X6 Helicopter Tech Specs*. Retrieved February 11, 2012, from http://www.draganfly.com/uav-helicopter/draganflyer-x6/specifications/

Dronepedia. (n.d.). *Main Page*. Retrieved February 4, 2012, from http://dronepedia.com/

Elston, J., Frew, E., & Argrow, B. (2006, August 22). *Networked UAV Command, Control and Communication*. Boulder, CO.

Federal Aviation Administration. (2000). *FAA System Safety Handbook.* Oklahoma City: Federal Aviation Administration.

Francis, R. (2011, June 13). *Ground Based Sense and Avoid (GBSAA) 101 Overview*. Retrieved from http://www.afceaboston.com/documents/events/cnsatm2011/Briefs/01-Monday/04-Francis-GBSAA%20101.pdf

General Atomics. (2012, February 22). *GA-ASI Successfully Tests Due Regard Radar Aboard Manned Aircraft*. Retrieved from http://www.ga-asi.com/news_events/index.php?read=1&id=378

General Atomics. (n.d.). *MQ-1 Predator*. Poway, California, United States of America.

General Atomics. (n.d.). *MQ-9 Reaper/Predator B*. Poway, California, United States of America.

Gertler, J. (2012). *U.S. Unmanned Aerial Systems*. Washington, D.C.: Congressional Research Service.

Greenburg, A. (2012, January 27). *DARPA-Funded Hacker's Tiny $50 Spy Computer Hides In Offices, Drops From Drones*. Retrieved from http://www.forbes.com/sites/andygreenberg/2012/01/27/darpa-funded-hackers-tiny-50-spy-computer-hides-in-offices-drops-from-drones/

GSA. (2012). *FedRAMP Concept of Operations*. Washington, D.C.: GSA.

Hennigan, W. (2011, May 30). *Pentagon seeks mini-weapons for new age of warfare*. Retrieved from http://articles.latimes.com/2011/may/30/business/la-fi-mini-drones-20110531

Humphries, M. (2011, July 29). *WASP: The Linux-powered flying spy drone that cracks Wi-Fi & GSM networks*. Retrieved from http://www.geek.com/articles/geek-pick/wasp-the-linux-powered-flying-spy-drone-that-cracks-wi-fi-gsm-netwokrs-20110729/

Hypponen, M. H. (2011, August 26). *How We Found the File That Was Used to Hack RSA*. Retrieved from http://www.f-secure.com/weblog/archives/00002226.html

Hyundai. (n.d.). *2012 Accent*. Retrieved February 7, 2012, from http://www.hyundaiusa.com/accent/

Jin, Y., Minai, A. A., & Polycarpou, M. M. (2003). *Cooperative Real-Time Search and Task Allocation in UAV Teams*. IEEE Conference on Decision and Control (pp. 7-12). Maui: IEEE.

Kaplan, D. (2011, May 31). *Lockheed admits to hack that may portend more breaches*. Retrieved from http://www.scmagazineus.com/lockheed-admits-to-hack-that-may-portend-more-breaches/article/204205/

Knorr, E., & Gruman, G. (2008, April 7). *What cloud computing really means*. Retrieved from http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031

Kotenko, I. (2005). *Agent-Based Modeling and Simulation of Cyber-Warfare Between Malefactors and Security Agents in Internet*. 19th European Conference on Modelling and Simulation. Riga: ECMS.

L3. (2011). *ROVER 5 Handheld*. Salt Lake City, Utah, United States of America.

Marshall, D. (2009). *Unmanned Aerial Systems and International Civil Aviation Organization Regulations*. North Dakota Law Review, 85(3), 693-713.

McLain, T. (2011, July 15). *Brigham Young University Proposed Projects*. Retrieved February 9, 2012, from http://c-uas.byu.edu/sites/c-uas.byu.edu/files/userfiles/7/BYU12-08%20SAA%20State%20of%20Art.pdf

Miller, G. (2011, December 27). *Under Obama, an emerging global apparatus for drone killing*. Retrieved from http://www.washingtonpost.com/national/national-security/under-obama-an-emerging-global-apparatus-for-drone-killing/2011/12/13/gIQANPdILP_story.html

Montalbano, E. (2011, May 17). *DARPA Seeks More Resilient Cloud Infrastructure*. Retrieved from http://www.informationweek.com/news/government/cloud-saas/229500774

Mortimer, G. (2012, February 16). *US Air Force Awards AeroVironment $4.2m for Switchblade Loitering Munition System*. Retrieved from http://www.suasnews.com/2012/02/11990/us-air-force-awards-aerovironment-4-2m-for-switchblade-loitering-munition-system/

Niland, W. M. (2006). *The Migration of a Collaborative UAV Testbed into the FLAMES Simulation Environment*. Winter Simulation Conference (pp. 1266-1272). Monterey: Informs Simulation Society.

Parry, R. (2012, January 9). *UAS and Cyber Attack*. (D. Brodsky, Interviewer)

Pilkington, E. (2012, February 9). *Bradley Manning to face formal trial on February 23*. Retrieved from http://www.guardian.co.uk/world/2012/feb/09/bradley-manning-formal-trial-23-february

Price, I. C., & Lamont, G. B. (2006). *GA Directed Self-Organized Search and Attack UAV Swarms*. Winter Simulation Conference (pp. 1307-1315). Monterey: Informs Simulation Society.

Puchaty, E. M., & DeLaurentis, D. A. (2011). *A Performance Study of UAV-based Sensor Networks Under Cyber Attack*. 6th Annual Conference on System of Systems Engineering (pp. 214-219). Albuquerque: IEEE.

Ravich, T. M. (2009). *The Integration of Unmanned Aerial Vehicles into the National Airspace*. North Dakota Law Review, 85(3), 597-622.

Reed, T., Geis, J., & Dietrich, S. (2011). *SkyNET: a 3G-enabled mobile attack drone and stealth botmaster*. USENIX Workshop on Offensive Technologies. San Francisco: USENIX.

Roggio, B., & Mayer, A. (2011, November 17). *Charting the data for US airstrikes in Pakistan, 2004 - 2011*. Retrieved December 22, 2011, from http://www.longwarjournal.org/pakistan-strikes.php

Seidman, R. (2011, December 22). *Drones at home: The use of drones in the U.S. on the rise*. Retrieved from http://www.metro.us/newyork/national/article/1056962--drones-at-home-the-use-of-drones-in-the-u-s-on-the-rise

Shachtman, N. (2009, December 17). *Insurgents Intercept Drone Video in King-Size Security Breach (Updated, with Video)*. Retrieved from http://www.wired.com/dangerroom/2009/12/insurgents-intercept-drone-video-in-king-sized-security-breach/

Shane, S. (2011, October 8). *Coming Soon: The Drone Arms Race*. Retrieved from http://www.nytimes.com/2011/10/09/sunday-review/coming-soon-the-drone-arms-race.html

Sheridan, M. B. (2011, March 16). *Mexico confirms use of U.S. drones in drug war*. Retrieved from http://www.washingtonpost.com/world/mexico-confirms-seeking-us-drone-help-in-drug-war/2011/03/16/ABbSEZg_story.html

Spolsky, J. (2002, November 11). *The Law of Leaky Abstractions*. Retrieved from http://www.joelonsoftware.com/articles/LeakyAbstractions.html

Stanley, J., & Crump, C. (2011). *Protecting Privacy From Aerial Surveillance: Recommendations for Government Use of Drone Aircraft*. New York: American Civil Liberties Union.

Tassey, M., & Perkins, R. (2011, August 7). *Wireless Aerial Surveillane Platform*. Las Vegas, Nevada, United States of America.

The Economic Times. (2011, August 5). *Hacker drone launches airborne cyber attacks*. Retrieved from http://economictimes.indiatimes.com/tech/internet/hacker-drone-launches-airborne-cyber-attacks/articleshow/9503016.cms

The Jargon File. (n.d.). *Back Door*. Retrieved February 9, 2012, from http://www.catb.org/jargon/html/B/back-door.html

Thornburgh, N. (2005, August 25). *Inside the Chinese Hack Attack*. Retrieved from http://www.time.com/time/nation/article/0,8599,1098371,00.html

Tippenhauer, N. O., Pöpper, C., Rasmussen, K. B., & Čapkun, S. (2011). *On the Requirements for Successful GPS Spoofing Attacks*. ACM Conference on Computer and Communications Security. Chicago: Association for Computing Machinery.

Todd, A. H. (2003). *Vendor-Supplied Backdoor Passwords - A Continuing Vulnerability*. Bethesda: SANS Institute.

U.S. Air Force. (2012, January 5). *MQ-1B Predator*. Retrieved February 7, 2012, from http://www.af.mil/information/factsheets/factsheet.asp?id=122

U.S. Air Force Scientific Advisory Board. (2011). *Operating Next-Generation Remotely Piloted Aircraft for Irregular Warfare*. Washington, D.C.: U.S. Air Force Scientific Advisory Board.

Udoeyop, A. W. (2010). *Cyber Profiling for Insider Threat Detection*. Knoxville: University of Tennessee.

Villasenor, J. (2011, July 5). *Cyber-Physical Attacks and Drone Strikes: The Next Homeland Security Threat*. Retrieved from http://www.brookings.edu/papers/2011/0705_drones_villasenor.aspx

West, Z. (2011, December 4). *Iranian Cyberattack Brings Down Stealth Drone?* Retrieved from http://blog.cybersecuritylaw.us/2011/12/iranian-cyberattack-brings-down-stealth-drone-al-jazeera.html

Wingfield, N., & Sengupta, S. (2012, February 22). *Drones Set Sights on U.S. Skies*. Retrieved from http://www.nytimes.com/2012/02/18/technology/drones-with-an-eye-on-the-public-cleared-to-fly.html?_r=1

Wood, A. D., Stankovic, J. A., & Son, S. H. (2003). *JAM: A Jammed-Area Mapping Service for Sensor Networks*. IEEE International Real-Time Systems Symposium (pp. 286-297). Cancun: IEEE.

Yochim, J. A. (2010). *The Vulnerabilities of Unmanned Aircraft System Common Data Links to Electronic Attack*. Ft. Leavenworth: U.S. Army Command and General Staff College.