Cyber Threats in United States Aviation: A Review of Inherent Blind Spots

Dreyton J. Schafer
Utah State University Center for Anticipatory Intelligence

Author Note

While the author and several subject matter experts cited are affiliated with the United States Air Force, their views are their own and protected by academic freedom. Those views expressed within this paper are not those of the United States Air Force and should not be construed or interpreted as being endorsed by the United States Air Force in any way.

Abstract

Aviation is a fundamental part of the US economic and national security sectors, facilitated by highly complex aircraft and support systems that became more efficient using cyber technology for management, maintenance, and daily operations; however, this increased efficiency has come at the cost of increased vulnerability to systemic disruptions through those cyber systems, placing both US civilian and military aviation at significant risk of debilitating cyberattacks. Potential areas of aviation cyberattack include interference with air traffic control, direct attacks on an aircraft's flight control systems, hacking of logistics systems handling maintenance and safety for aircraft, and "spoofing" of the Global Positioning System (GPS) to confuse the essential ability to correctly navigate an aircraft. In addition, potential avenues already exist for cyberattacks in various support components of the aviation sector, especially through attacks upon the supporting infrastructure for airplane operations. The tools and hardware necessary to engage in cyberattacks are proliferating, while barriers to entry are low. Of particular concern, military aircraft are potentially vulnerable to logistics interference that could cause a crucial grounding of F-35s in a "Pearl Harbor" style first strike cyberattack. Hostile foreign actors are already in possession of the schematics for the F-35 and other critical military aircraft, heightening the potential for subtle sabotage through digital maintenance systems. In civilian aviation, two 2018/2019 Boeing 737 MAX 8-variant aircraft accidents and its subsequent fleet grounding provide a stark example of the consequences of negligence in aviation design and support that can be cross-applied to the potential fallout from an aviation cyberattack.

Accepting the existence of cyber vulnerabilities in aviation is the first step in crafting preventative and resilient responses to catastrophe. Transparency in the process of creating regulation and responding to cyberattacks will best serve the public interest in safety and security while facilitating the continued regular operation of commercial transport and military aircraft. Irreparable damage to public confidence in aviation and regulators may be the outcome if plans to "bounce back" from cyberattacks are procrastinated until disaster strikes.

Cyber Threats in United States Aviation: A Review of Inherent Blind Spots

Air travel is a ubiquitous and integral part of US social and economic life, and disruption in commercial and military aviation through cyberattack would have significant impacts on the current paradigm of US society. Aircraft, which are defined here as vehicles capable of flight, are widely trusted and utilized to connect the nation with an average of 5,000 planes in US airspace at any given time (*Air Traffic Dataset | Science On a Sphere*, n.d.). These aircraft are reliant on a vast communication and navigation network that is supported by the cyber domain, opening up the possibility for cyberattacks—defined by the Department of Homeland Security (DHS) as "malicious attempts to access or damage a computer system" (*Cybersecurity | Ready.Gov*, n.d.). Cyber vulnerabilities are openings or flaws in a cyber system or network that allow access to an individual or group conducting a cyberattack (*Overview of Cyber Vulnerabilities | ICS-CERT*, n.d.).

As highly complex systems, aircraft transportation and military aircraft are demonstrably vulnerable to indirect cyberattacks on logistics and diagnostic systems. Meanwhile, real concerns exist that avionics systems could potentially be compromised by passengers or through other cyber-interfacing componentry on an aircraft (Zetter, 2015). GPS spoofing exists as a proven avenue of attack on commercial aircraft through the cyber domain and the electromagnetic spectrum. Transparent and clear-eyed examinations of these potential threats are the first steps towards recognizing their reality and creating preventative countermeasures.

An industry response to cyber vulnerabilities has been almost non-existent, with comprehensive examinations of the potential implications of these risk scenarios coming primarily from government watchdogs like the Government Accountability Office's report on potential for cyberattacks on aircraft avionics systems (Zetter, 2015). Significant and transparent studies of those avionics systems have not occurred, and the necessity of conducting them has been openly disparaged by former Boeing engineers and former Federal Aviation Administration (FAA) investigators who have expressed skepticism of the technical feasibility of such an attack (Zetter, 2015). Yet members of federal security agencies (led by DHS) claim to have successfully carried out controlled tests of such cyber penetration as recently as 2017 (Davis, 2017; Zetter, 2015; Ramsdell, n.d.). Recent revelations about the relationship between Boeing and the FAA in the wake of the tragic 737 MAX 8 accidents have also demonstrated that expert opinion is not infallible or immune to economic incentives (David Gelles et al., 2019).

To examine the threat of cyberattacks to manned aircraft, this report will individually assess the sub-categories of US military and commercial aviation. Within each of these sub-categories, organizations face distinct challenges, such as military aviation seeking to counter cyberattacks by rival states and commercial aviation facing threats from non-state actors like criminals or terrorist groups. Confronting these threats requires the inculcation of resilience, or the ability to "bounce back" across a broad spectrum of potential scenarios ranging from constant low-level cyberattacks to

cataclysmic attacks on systemic integrity. Creating a framework to promote safety and protect US military airpower and commercial air travel will be essential for national security as the digital world continues to evolve.

Scope Note

This inquiry into the vulnerability and resilience of US aircraft and aviation to cyberattack has been deliberately limited to highlight specific vulnerabilities to aircraft that have a significant impact on national security and US citizens' daily life. Unmanned aerial vehicles (UAVs) and remotely piloted aircraft (RPAs) are excluded, to highlight the human dangers and costs in the event of a cyberattack on aircraft or the supporting aviation systems. However, the findings on vulnerabilities for manned craft are largely transferrable to unmanned systems. Among manned aircraft, this report mainly focuses on commercial transportation and military aircraft rather than cargo transport or smaller private planes; but again, these findings can be cross-applied in many cases.

Cyber Threats Are Varied and Creative, Leaving Many Vectors of Potential Attack

There are many possibilities for cyberattack in the aviation sector, and they need not be directed towards an aircraft in flight to cause disruption or even catastrophic kinetic effects. A discussion of some of these threats will put examples from military and commercial aviation into perspective, but strategies for cyberattacks on the aviation sector are by no means exhaustive as cyberweapons used by states and criminals continue to evolve and exploit vulnerabilities.

One potential segment of US aviation vulnerable to attack is **air traffic control.** The complexity and age of the air traffic control system controlled by the FAA leave it vulnerable to hacking or interference, putting aircraft safety and navigation at risk (Cooper, 2015; Wenz, 2015). In order to increase efficiency of communication, most of this infrastructure is computerized, creating vulnerability to sophisticated penetration and attack (Arntz, 2018).

Second, assessments about **avionics** (i.e. the computer systems tasked with automating or running physical controls of an aircraft) vulnerability come primarily from industry, which has a vested economic interest in claiming their resistance to such an attack—but as case studies on a malware-infected Spanair flight accident and more recent Boeing 737 MAX 8 demonstrate, even significant vetting of avionics code can still leave vulnerabilities that allow aircraft to be infected by malware or represent fatal flaws (Davis et al., 2019). Creativity and tech savviness are indispensable tools for all hackers, and those with malicious intent will exploit any openings they have (Arntz, 2018). Even if avionics are secured, in-flight entertainment and Wi-Fi used by passengers are highly vulnerable to hacking, and data shared through wireless connection can be compromised by determined hackers utilizing equipment that would pass a Transportation Security Administration (TSA) airport screening (Higgins, n.d.).

The logistical systems utilized by airlines and the military are also open to tampering. The greatest risk scenarios would be the destruction or altering of digital

maintenance records leading to vital work not being performed on aircraft. An analogous situation has occurred in military aviation since 2013 budget cuts led to the departure of many experienced aircraft maintainers (*Why The Number Of Military Aviation Accidents Has Sharply Increased*, 2018). The decrease in maintenance expertise precipitated an increase in accidents—168 servicemember deaths total—with 2018 being a five-year high for fatalities in military aviation accidents (Copp, 2018). If such incidents occurred in the commercial sector the impact on consumer confidence would be significant, as well as the potential toll of human life.

A final potential system vulnerable to interference is GPS**.** GPS spoofing is a demonstrated technology that disrupts the reception of GPS signals from US satellites by navigational receivers. It disrupts the positioning and timing functions that allow our devices and vehicles to determine their correct location on Earth. Signals broadcast by GPS satellites are very weak, and therefore it is inexpensive to build or purchase a device that can mimic or drown out their signals. These methods of disrupting GPS navigation are called “spoofing” and “jamming” respectively (Humphreys, 2019). Proliferation of this technology and its relative ease of use mean that the number of instances in which pilots report losing GPS connection are on the rise, with over 100 incidents reported in the US since 2013 (Huber, 2018; Bellamy, 2017). There is an obvious threat to military aircraft presented by GPS spoofing, with Russia jamming GPS signals in Norway for a week in 2017 and more recently spoofing ships, aircraft, and other devices thousands of times in an apparent security measure to protect military assets and President Vladimir Putin personally (Huber, 2018; Mizokami, 2019; Humphreys, 2019). In one case, a ship in the Black Sea found its AIS navigation system showing the vessel incorrectly at Gelendzhik Airport, 32 miles inland from its true location (Hambling, 2017). This type of navigation manipulation could drive ships and aircraft off course or diminish the effectiveness of militaries’ GPS-guided munitions, potentially jeopardizing civilian lives and commercial navigation at sea and in the air (Hambling, 2017).

These avenues of cyberattack have real world consequences that will be explored in both the military and commercial domains of aviation. This report will seek to illustrate that the possibilities for enemy actors to interfere in U.S.’ daily aviation life and defense through cyber is real and growing.

Interconnected Aircraft Systems Two-Edged Sword, Leaving US Vulnerable To Crippling First-Strike Cyberattack

Military aviation is unique in attempting to walk a balancing act of leveraging “data-fusion” (i.e., connecting data from various disparate sources to provide a pilot a more comprehensive view of the battlefield) versus increased vulnerability with reliance on networked cyber systems. A recently concluded US Air Force “Red Flag” training event demonstrated the superiority of information fusion in the F-35 Lightning II. the F-35’s enhanced capabilities enable a higher level of coordination that could be the difference in establishing air supremacy when pitted against a near-peer adversary yet leave the Air Force more vulnerable in a changing threat-scape that includes cyberspace as a warfighting domain.

Interconnected command and weapons systems are particularly vulnerable to a "cyber first-strike" or "cyber–Pearl Harbor" that could cripple US airpower in a potential conflict. In conflicts like Iraq and Afghanistan where the US has enjoyed almost uncontested air superiority, increased system integration has made US aircraft highly successful by allowing greater joint coordination to deliver airpower where most needed. This has also left the US vulnerable and uncertain about the effectiveness of these systems when it encounters a foe with the capabilities necessary to undermine and compete with US technological prowess. Cyber vulnerabilities are not limited to aircraft because of the networked nature of US joint operations, compelling creativity and scrutiny of Department of Defense (DoD) weapons systems and a focus on developing simplicity over complexity in new systems (Dan Grazier, 2019).

Interconnected systems are designed to improve efficiency in operations and maintenance but create critical vulnerabilities, as demonstrated by the Autonomic Logistic Information System (ALIS) in the F-35 (Mizokami, 2018). ALIS constantly collects data from every operational F-35 in the world, which could be compromised to ground the US fighter fleet during a first-strike attack (*Autonomic Logistics Information System (ALIS)*, n.d.; Grazier, 2019; Mizokami, 2018). While military diagnostic systems like ALIS are designed to increase savings and mission efficiency, they require a heavy reliance on the private sector for troubleshooting (Insinna, 2019). One maintainer supporting the F-35 mission at Hill Air Force Base (AFB) pointed out that the only way to contact Lockheed Martin for his shop is by phone, a simple although monotonous task in peacetime but perhaps a fatally slow or severable connection in a high tempo contest for air superiority (Parker, 2019). Military maintenance workers are legally bound to follow procedures outlined in "Technical Orders" to troubleshoot and fix aircraft, and often need to contact civilian counterparts in to fix cyber-dependent craft. These phone and internet communication channels are open to disruption or manipulation. Even the utility of the ALIS system for its intended purpose of preventive maintenance and training management is called into question by the fact that F-35 flight training squadrons at Eglin AFB and Luke AFB have chosen to stop using the Training Management subcomponent of ALIS (Insinna, 2019). The Air Force's top acquisition official has said that ALIS has a "…bad user interface and a bad architecture…"(Insinna, 2019). Additionally, online access to the ALIS system for Air Force maintainers is limited by the speed of the ALIS servers, which only support access to a certain number of users simultaneously (Insinna, 2019). The advantages of the information fusion that make the F-35 more combat effective versus large groups of less integrated aircraft are tempered by its greater vulnerability to communication and supply chain disruption. Maintenance issues, private sector vulnerability, and adversarial espionage are combining to make a cyberattack on complex maintenance structures like Lockheed's ALIS increasingly probable.

More worryingly, potential rival powers like Russia and China have incorporated a "cyber first-strike" into their military doctrine to cripple complex US weapons systems, illustrating that "a trillion dollars of hardware is worthless if you can't get the first shot off" (Dreyfuss, 2018). Shutting down the F-35 fleet through attacking the

maintenance system is a real possibility, especially as the US works towards the goal of a fleet with 80 percent fifth generation aircraft by 2040 (Gould, 2019). Additionally, shortages in skilled maintainers exacerbate the threat of cyber interference in the logistics system, while also demonstrating the potential threat of long-term sabotage through data manipulation to delay or frustrate maintenance schedules. The Air Force lost a significant portion of its most experienced maintainers during the 2014 force reductions, leading to a shortage of 4,000 maintainers by 2015 (Woody, 2017). The gap has been closed, but retention of skilled maintainers remains lower than the service retention average, at 73.4 percent in 2017 (Losey, 2019).

The possibility of indirect assaults on US aircraft with a sophisticated cyberattack are increased by the fact that potential adversaries stole designs of US aircraft and other military hardware. For example, in 2013, Chinese hackers gained access to the designs of "more than two dozen" DoD weapons systems, including aircraft like the F-35, V-22, C-17, and the Global Hawk. "Detailed schematics" for the F-35 were stolen again by hackers in November 2016. An October 2018 Government Accountability Office report found that every DOD weapons system tested between 2012 to 2017 was found to be vulnerable to hacking (Grazier, 2019). Furthermore, a January 2019 report by the DOD Inspector General identified 266 specific cyber vulnerabilities across all DOD components, showing a large attack surface for the US military (Grazier, 2019; *Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft*, 2019). When these systems are potentially networked together, the vulnerabilities of one system could be compromising to another that is "cyber hardened" because they are connected and sharing information. The joint nature of US operations advantages the US military in carrying out successful aircraft operations yet compromises efforts to safeguard digital information and assets. China's past success in stealing US defense information raises the likelihood that vulnerabilities in these systems will be exploited in a potential conflict.

Reliance on high technology laid the foundation for US airpower dominance in the decades since Desert Storm, facilitating efficient and complex operations abroad on a scale unsustainable for most states, including potential adversaries (*Air Power in the Gulf War Brief*, n.d.). In fact, a critical RAND brief suggests that "…perhaps the most significant advances in technology came in the form of information systems" which were able to increase the coordination of aircraft that had an average age of 14 years (*Air Power in the Gulf War Brief*, n.d.). But in the growing age of cyberwarfare, the advantages of networked weapons systems are being transformed into potentially crippling vulnerabilities. Resilience in the face of this challenge may require simplifying future aircraft and weapons systems by reworking their networked capabilities, and training military members on operations in a highly degraded environment of cyber combat (Grazier, 2019; Singer & Cole, 2015).

The Air Force is making moves to train its pilots to operate in an adversarial cyber and electromagnetic spectrum environment. The emphasis remains on the interconnectivity facilitated by the F-35. A concrete example of the F-35's data fusion

and stealth capabilities is that they enabled it to attain a 20:1 kill ratio in February 2019 Red Flag exercises (Cenciotti, 2019; Kitfield, 2019; Pickrell, 2019). The Air Force stated that these capabilities were simulated as a highly contested environment against aircraft with capabilities like those of potential adversaries like China or Russia (Kitfield, 2019). Additionally, former Air Force Chief of Staff, General Goldfein called the F-35 "Quarterback" for data fusion in combat, enhancing the capabilities of less advanced aircraft by being able to communicate to them a clearer picture of the battlefield as well (Martin, 2019). The Air Force invested heavily in the fighter and hopes to have the craft compose 50 percent of the fighter fleet within the next several years (Rempfer, 2019).

It is important to recognize that some of the benefits of the F-35 system make the larger US military air fleet more resilient to traditional kinetic attacks. Decentralized command allowed by F-35 data fusion mitigates some of the danger of losing large command and communications aircraft like the Joint Surveillance and Target Attack Radar Systems (JSTARS) and the Airborne Warning and Control Systems (AWACS) in a major war with a near-peer power (Insinna, 2018; Kitfield, 2019; Martin, 2019). However, utilizing the enhanced capabilities of the F-35 and protecting it from cyberattack will be a balancing act, with increased complexity making resiliency difficult. Retention of experienced maintainers and decreased dependence upon Lockheed's corporate systems may be some of the most feasible steps to close vulnerable gaps in the F-35's cyber protection and the resilience of the entire US military air fleet.

Commercial Air Travel Extremely Vulnerable to Profit-busting Disruptions

It is underacknowledged in the security and commercial communities that in air travel's networked infrastructure single failures have cascading effects across multiple airports and airlines, with cyberattacks potentially leading to system paralysis like what occurred during 9/11. Regular delays have been demonstrated to be economically destructive, and loss of confidence in the system in future cyberattacks could be catastrophic. According to an industry report, eight percent of airline profit is lost because of normal delays each year (Gershkoff, n.d.). A 2007 Berkley academic study found that domestic delays alone at that time cost the US economy $32.9 billion annually (Guy, 2010). Delays are 'viral' in nature, demonstrated by the estimate that one minute of delay is likely to cause at least 30 seconds of delay at the next location in the network (Rogers, 2019). Failures at one location or wide-spread delays can have unpredictable second and third order effects because of these network connections (Gershkoff, n.d.; Rogers, 2019). Lack of adaptability in these systems in the face of terror or violence led on 9/11 to a declaration of a "ground stop" or full system paralysis as all planes in the United States were grounded (Mola, 2007; Donnelly, 2001). Another example of the disruptive effects of flight delays is the 2010 eruption of the Icelandic volcano of Eyjafjallajökull resulted in the closure of airspace over Europe (Bressan, 2017). One hundred thousand total flights were cancelled, 10 million people were stranded or unable to travel, $1.7 billion was lost by airlines, and in one fell swoop, 30 percent of worldwide airline capacity was prevented from operating ("How the 2010 Ash Cloud Caused Chaos," 2011). In the event of a coordinated cyberattack over days or

weeks that causes accidents or deaths, the costs might be comparable or of greater magnitude because cyberattacks need not discriminate by geography or distance.

Another neglected fact is that barriers of entry for cyberattacks on aircraft are decreasing, as hacking tools proliferate that could be applied against aircraft or indirectly to support systems. Ransomware is an example that disrupted German train systems and held the computer networks of British hospitals hostage (*German Rail Operator Affected by Global Cyber Attack | Reuters*, 2017). While these threats grow in number and these vulnerabilities have been officially and empirically demonstrated, these findings have not mobilized a coordinated response to prevent or cultivate resilience in these cyber systems. In 2017, a DHS-led team demonstrated the ability to hack into a Boeing 757's computer system, showing vulnerabilities in a widely used aircraft (Davis, 2017; Ramsdell, n.d.). Open source reports are unclear whether the team gained control of the system they penetrated or simply gained entry, and to what systems within the aircraft they had access, but the hack was accomplished with materials that would have been allowed through a normal TSA security check (Biesecker, 2017; Davis, 2017; Ramsdell, n.d.). The potential threat is clear: cyber kinetic attack strategies like GPS spoofing allow control of aircraft to be gained with common computer technologies, and then for those aircraft to be directed in an alternate course (Kerns et al., 2014).

Another important case-study is Spanair flight 5022, which crashed in 2008 and killed 154 people, partly due to malware in a diagnostic software system that caused pilots and maintenance workers to incorrectly identify problems with flight configuration (Cusick et al., 2017). This incident is often dismissed as merely pilot error, but is significant in demonstrating that malware can infect avionics computer systems and that human reliance on those systems can be fatal. Automation and the proliferation of UAVs may make pilots and operators more complacent as more of their responsibilities are completed by the computer, but the consequences of aviation accidents remain as serious and final as they have ever been.

Boeing 737 MAX 8 Case Study Illustrates Aviation Community Response to Crisis

Because the risks of a cyberattack on commercial aircraft or the aviation sector have been underexamined, the response to the 2018 Lion Air and 2019 Ethiopian Airlines crashes of the Boeing 737 MAX 8 is a recent and illustrative case study of potential risk scenarios if cyber technology threatening to aircraft were proliferated and deployed. While the impact on air travel has been relatively minimal because the 737 MAX 8 is a new aircraft model not highly represented in commercial fleets, disruption in the aftermath of the accident demonstrates a probable reaction to a future hypothetical cyberattack that would be magnified if a more widely used commercial aircraft were targeted.

An important part of the initial response to the MAX 8 accident in Ethiopia was the cascade of regulatory action as governments from more than 30 countries grounded the MAX 8, and airlines even grounded the aircraft themselves in several more countries (Associated Press, 2019; Zimmerman, 2019; Chiwaya & Wu, 2019). The next trading day after the accident, Boeing's stock initially took a 13 percent hit,

rebounded, and then ended the day at a five percent loss (Tsang & Kitroeff, 2019). Loss of consumer and investor confidence in aerospace manufacturing firms and airlines in the case of a fatal cyberattack on an aircraft would likely be comparable or worse. Another element of the investigation applicable to a potential cyberattack is the length of time needed to investigate, with the flight data recorded to the Ethiopian Airlines jet's "black box" during its 10 March 2019 crash not being examined until April, all while speculation fueled popular worries about the aircraft model and safety features (Rushe, 2019). Southwest Airlines had the largest 737 MAX 8 fleet in the world of 34 and saw up to 150 flights per day cancelled as a result of the grounding (Rucinski & Lampert, 2019). However, flight cancellation impacts not only those flights, but other flights and passengers that are "bumped" as a result of the reallocation of customers previously scheduled to fly on 737 MAX 8s (Rucinski & Lampert, 2019).

The most probable cause of the accident was a recent software update that pilots have not been widely educated on, illustrating the need to educate users on cyber updates to systems that could impact safety (Johnson et al., 2019). Former Boeing engineers stated the competitive pressure to field the 737 MAX 8 to compete with Airbus resulted in an abbreviated design process and increased reliance on software rather than structural redesigns of the aircraft in order to avoid long FAA examinations (Gelles et al., 2019).

The Ethiopian Airlines accident and subsequent grounding of the Boeing 787 MAX 8 also demonstrated the economic and commercial impacts that occur when an unknown failure occurs in a commercial aircraft. The initial findings of the Ethiopian report suggested a flaw in the software was the fatal variable, ruling out human error on the part of the pilots who "followed the Boeing recommended and FAA-approved emergency procedures" (Davis et al., 2019). The software, called the Maneuvering Characteristics Augmentation System, is designed to automatically force the nose of the aircraft down to avoid a stall (Davis et al., 2019). A software malfunction sent the aircraft diving toward the ground at 575 mph. Most recently, a second flaw was discovered in the avionics system's software that controls flaps and flight control which are considered essential to safety, but a Boeing spokesman downplayed the second flaw, calling it "relatively minor" (Davis et al., 2019). Questions about the technical feasibility and the forms that potential cyberattacks will take remain unexamined, but continued inaction will receive heavy scrutiny if and when a future accident is definitively linked to interference in the cyber domain.

The MAX 8 disaster also illustrates the slow turnaround in investigating aviation accidents. In the case of a cyberattack it could take weeks or months after an accident to determine that an aircraft was brought down via cyber interference. While not impossible to attribute cyberattacks to specific actors, cyberattacks take significant time to uncover once occurred. A hypothetical cyberattack on an aircraft or on the aviation supply sector could occur with the root cause taking months to ascertain, while the reliance of aircraft upon cyber systems continues to grow as the Internet of Things proliferates. According to a 2018 survey, data breaches take an average of 197 days to

detect, a timeframe that systems linked to aviation do not have if a hostile actor is interfering or stealing data (Goolik, 2018). Sixty-seven percent of airlines in a 2018 survey planned to invest in connecting their operations to the Internet of Things in the coming years, and with engines like the Bombardier Geared Turbo Fan, which features 5,000 sensors capable of generating 10 gigabytes of data per second, "data generated by the aerospace industry alone could soon surpass the magnitude of the consumer Internet" (Rapolu, 2018; Cenciotti, 2017; Sitaonair, 2018). This would consist of data on aircraft performance, such as data on location, direction, engine diagnostics, and other system information to paint a complete picture of the function of an aircraft, potentially allowing predictive maintenance to be conducted or for logistical planning to be streamlined (essentially becoming the civilian equivalent of the aforementioned military ALIS program). Because of this future potential and current data practices, indirect cyberattacks need not only target the physical aircraft to threaten commercial aviation. This vulnerability is underscored by a 2018 survey indicating that only 41 percent of airlines have established cybersecurity standards for their suppliers (Prentice & Mee, 2018). Meanwhile, the costs of compromised or lost data is high; a 2018 study by IBM found the average cost of a data breach is $3.86 million (*Cost of Data Breach Study | IBM Security*, 2018).

Aviation Sector Resilience Possible, But Dynamic Solutions Necessary

A framework for resilience in the event of cyberattack on aircraft requires an honest study by the FAA, aircraft manufacturers, airlines, and militaries about the feasibility and possible avenues of cyberattack on the aviation sector. The vulnerabilities previously identified are by no means comprehensive and reflect research from a national security perspective. White hat hacking could be utilized to probe and test both physical aircraft and the supporting infrastructure that facilitates their regular operation. The Air Force set an example of drawing on hacking skills from civilians through its "Hack the Air Force" events (Zazulia, 2018; Chappellet-Lanier, 2018). In December 2018 that event paid out $130,000 to hackers for finding 120 vulnerabilities in its cyber infrastructure (Zazulia, 2018; Chappellet-Lanier, 2018). Community events patterned after this one to draw in white hat hacking expertise should feature information sharing between these interest groups in order to improve the general knowledge of cyber vulnerabilities and solutions across the industry.

As evidenced by the MAX 8 disaster, transparency in the process of FAA approval and crafting of regulations on cybersecurity is essential. An innovative idea on fostering transparency regarding cyberattacks and data breaches from the Harvard Business Review suggests that companies are currently disincentivized from acknowledging cyberattacks when they have been compromised. This is because investors and regulators move to punish the company when these events occur. The analogy is then contrasted with the case of a bank robbery. The bank is not punished for a robbery; instead, a system of insurance kicks in to help it remain resilient. The opposite is true with cyberattacks that allow malicious actors to steal data, money, or take harmful action against a corporate entity. The suggestion is to instead change

tactics and treat companies like victims of a crime rather than punish them (Jain & Ropple, 2018).

Another reality that governments must recognize is that human reliance on automated systems will continue to grow. These systems will become enmeshed in daily life even beyond their current state over the next decade. This extends to aircraft as manufacturers add features like MACs and automated maintenance monitoring systems. Potential delays caused by hacking of commercial airlines and air traffic control will have significant economic consequences because of the strain that the commercial air travel system undergoes with normal activity. Developing resiliency in an over-taxed system is not economically possible through equipment redundancy because unused "backup" planes and maintenance would make profitability extremely difficult. But resilience could be developed through FAA regulation mandating response plans from airlines. This pushes industry to take the first step by considering the potential problems and risk scenarios to cyberattack. It would also allow the airlines to build their own resistance to threats with cybersecurity and for the development of insurance regimes to "bounce back" from delays and damage caused in future cyberattacks. The potential threat must be engaged realistically and acknowledged in order to create an aviation culture and community ready to respond to cyberattacks if and when they impact the industry. Bringing the FAA itself up to a higher mark on cybersecurity standards is also important in helping it craft effective regulation on cybersecurity for the aviation industry. For instance, the FAA has yet to adopt 2013 government standards on security controls, according to a Government Accountability Office report (Williams, 2015).

Military resilience, like commercial, is complicated by resource scarcity (Smith, 2019). Acquisition is an inflexible process and the scale of implementation of military aircraft means that current decisions will have an impact for decades on readiness and vulnerability. Time is also scarce, with pilots, maintainers, and support crew unable to keep up with regular operations and even less able to undertake exercises simulating the partial or complete impairment of those normal operations (Losey, 2019; Smith, 2019). It is impossible to address all of these issues because of resource constraints, but opportunities to make progress do exist. For instance, while the full picture of the vulnerabilities of networked military aircraft is difficult to accurately assess based solely upon open-source data, it does seem feasible to attempt to curtail the use of ALIS and other systems connecting these aircraft to wider or more vulnerable networks and instead rely on decentralized maintenance diagnostics and management. To support such a "back to basics" approach would also require talent management in recruiting and retaining experienced maintenance personnel in sufficient numbers to support the military air fleet.

A singular, "hard and fast solution" to the dangers posed by cyberattacks on aircraft does not exist because of the diversity of the American aviation system, but the previously mentioned measures offer the possibility to create a "patchwork" of resiliency, in which as many large problems across the spectrum of military and commercial aviation are guarded against as possible. This would provide a basic

framework of standards—which does not currently exist even at a rudimentary level—for implementation in situations that have not been mentioned or imagined in this report. A cyberattack analogous to (or surpassing) the MAX 8 disaster should not be necessary to precipitate an effort to respond to the clear and mounting cyber vulnerabilities in the US aviation domain. This high-tech sector that has long been a staple of US economic and national security clout may not have the chance to recover if flex and tensile strength is not built into its daily operations before a serious challenge emerges.

References

Aaron C. Davis, Luz Lazo, & Paul Schemm. (2019, April 4). *Additional software problem detected in Boeing 737 Max flight control system, officials say*. The Washington Post. https://www.washingtonpost.com/world/africa/ethiopia-says-pilots-performed-boeings-recommendations-to-stop-doomed-aircraft-from-diving-urges-review-of-737-max-flight-control-system/2019/04/04/3a125942-4fec-11e9-bdb7-44f948cc0605_story.html?noredirect=on&utm_term=.f6552ddc26c8

Air Power in the Gulf War Brief. (n.d.). Rand Corporation. Retrieved April 5, 2019, from https://www.rand.org/pubs/research_briefs/RB19/index1.html

Air Traffic Dataset | Science On a Sphere. (n.d.). [Government Website]. National Oceanic and Atmospheric Administration. Retrieved April 3, 2019, from https://sos.noaa.gov/datasets/air-traffic/

Ann Brody Guy. (2010, October 18). *Flight delays cost $32.9 billion, passengers foot half the bill*. Berkeley News. https://news.berkeley.edu/2010/10/18/flight_delays/

Associated Press. (2019, March 14). *Which countries have grounded the Boeing 737 Max jets*. PBS NewsHour. https://www.pbs.org/newshour/world/which-countries-have-grounded-the-boeing-737-max-jets

Autonomic Logistics Information System (ALIS). (n.d.). Lockheed Martin. Retrieved February 21, 2019, from https://www.lockheedmartin.com/en-us/products/autonomic-logistics-information-system-alis.html

Bhoopathi Rapolu. (2018, January 18). *Internet Of Aircraft Things: An Industry Set To Be Transformed | Connected Aerospace content from Aviation Week*. Aviation Week. https://aviationweek.com/connected-aerospace/internet-aircraft-things-industry-set-be-transformed

Bressan, D. (2017, November 26). *How Volcanic Eruptions Disrupt Air Travel*. Forbes. https://www.forbes.com/sites/davidbressan/2017/11/26/how-volcanic-eruptions-disrupt-air-travel/

Brian Prentice, & Paul Mee. (2018, April 11). *Aviation Industry May Be Vulnerable To Cyberattack Through Its Global Supply Chain*. Forbes. https://www.forbes.com/sites/oliverwyman/2018/04/11/how-aviations-global-supply-chain-may-open-up-the-industry-to-cyberattack/

Calvin Biesecker. (2017, November 8). *Boeing 757 Testing Shows Airplanes Vulnerable to Hacking, DHS Says*. Avionics. https://www.aviationtoday.com/2017/11/08/boeing-757-testing-shows-airplanes-vulnerable-hacking-dhs-says/

Cenciotti, D. (2019, February 16). The First Reports Of How The F-35 Strutted Its Stuff In Dogfights Against Aggressors At Red Flag Are Starting To Emerge. *The Aviationist*. https://theaviationist.com/2019/02/16/the-first-reports-of-how-the-f-35-strutted-its-stuff-in-dogfights-against-aggressors-at-red-flag-are-starting-to-emerge/

Cooper, A. (2015, April 2). *Report: Air Traffic Control System Vulnerable to Cyber-Attack - CNNPolitics*. CNN. https://www.cnn.com/2015/03/02/politics/cyberattack-faa-air-traffic-control-hacking/index.html

Copp, T. (2018, May 6). *As fatal aviation crashes reach 6-year high, Pentagon says 'this is not a crisis.'* Military Times. https://www.militarytimes.com/news/your-military/2018/05/06/as-fatal-aviation-crashes-reach-6-year-high-pentagon-says-this-is-not-a-crisis/

Cost of Data Breach Study | IBM Security. (2018). IBM. https://www.ibm.com/security/data-breach?lnk=mpr_buse_uken&lnk2=learn

Cybersecurity | Ready.gov. (n.d.). Department of Homeland Security. Retrieved April 3, 2019, from https://www.ready.gov/cybersecurity

Dan Grazier. (2019, January 31). *What Should We Do About a Generation of Weapons Vulnerable to Cyberattacks?* Project On Government Oversight. https://www.pogo.org/analysis/2019/01/what-should-we-do-about-a-generation-of-weapons-vulnerable-to-cyberattacks/

David Cenciotti. (2017, June 20). *Cybersecurity In The Sky: Internet of Things Capabilities Making Aircraft More Exposed To Cyber Threats Than Ever Before – The Aviationist*. https://theaviationist.com/2017/06/20/cybersecurity-in-the-sky-internet-of-things-capabilities-to-make-aircraft-more-exposed-to-cyber-threats-than-ever-before/

David Gelles, Natalie Kitroeff, Jack Nicas, & Rebecca R. Ruiz. (2019, March 23). *Boeing Was 'Go, Go, Go' to Beat Airbus With the 737 Max—The New York Times* [News]. The New York Times. https://www.nytimes.com/2019/03/23/business/boeing-737-max-crash.html

Davis, J. (2017, November 14). *Boeing 757 Hacked by DHS in Test* -. Security Today. https://securitytoday.com/articles/2017/11/14/boeing-757-hacked-by-dhs-in-test.aspx

Dominic Rushe, D. (2019, March 14). Boeing's 737 Max fleet "will remain grounded for weeks." *The Guardian*. https://www.theguardian.com/world/2019/mar/14/ethiopian-airlines-boeing-737-max-black-boxes-arrive-paris

Dreyfuss, E. (2018, October 10). US Weapons Systems are Easy Cyberattack Targets, New Report Finds. *Wired*. https://www.wired.com/story/us-weapons-systems-easy-cyberattack-targets/

Eric M. Johnson, Tim Hepher, & Jason Neely. (2019, April 3). *Ethiopia to issue first Boeing investigation report on Thursday | Reuters* [News]. Reuters. https://www.reuters.com/article/us-ethiopia-airplane-software/ethiopia-to-issue-first-boeing-investigation-report-on-thursday-idUSKCN1RF0YU

German rail operator affected by global cyber attack | Reuters. (2017, May 13). Reuters. https://www.reuters.com/article/us-cyber-attack-germany-rail/german-rail-operator-affected-by-global-cyber-attack-idUSKBN1890DM

Hambling, D. (2017, August 10). *Ships fooled in GPS spoofing attack suggest Russian cyberweapon*. New Scientist. https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/

Henry Zimmerman. (2019, March 12). *Dozens Of Countries, Including The U.S., Ground Boeing's 737 Max 8 Planes*. NPR.Org. https://www.npr.org/2019/03/12/702568990/dozens-of-countries-ground-boeings-737-max-8-following-deadly-crash-in-ethiopia

How the 2010 ash cloud caused chaos: Facts and figures. (2011, May 24). *The Telegraph*. https://www.telegraph.co.uk/finance/newsbysector/transport/8531152/How-the-2010-ash-cloud-caused-chaos-facts-and-figures.html

Huber, M. (2018, May 22). *GPS Jamming and Spoofing On the Rise*. Aviation International News. https://www.ainonline.com/aviation-news/business-aviation/2018-05-22/gps-jamming-and-spoofing-rise

Insinna, V. (2018, July 25). *JSTARS recap is officially dead*. Defense News. https://www.defensenews.com/air/2018/07/24/jstars-recap-is-officially-dead/

Ira Gershkoff. (n.d.). *Shaping the future of Airline Disruption Management*. Amadeus. http://www.amadeus.com/documents/airline/airline-disruption-management/amadeus-airline-it-disruption-white-paper.pdf

James Kitfield. (2019, March 6). Red Flag 2019: First Great Power Air War Test In Years. *Breaking Defense*. https://breakingdefense.com/2019/03/red-flag-2019-first-great-power-air-war-test-in-years/

Joe Gould. (2019, April 4). *US Air Force defends F-15X buy to skeptical Inhofe, Reed*. Defense News. https://www.defensenews.com/congress/2019/04/04/usaf-defends-f-15x-buy-to-skeptical-inhofe-reed/

Kelly Jackson Higgins. (n.d.). *IoT Malware Discovered Trying to Attack Satellite Systems of Airplanes, Ships*. Dark Reading. Retrieved April 5, 2019, from https://www.darkreading.com/vulnerabilities---threats/iot-malware-discovered-trying-to-attack-satellite-systems-of-airplanes-ships/d/d-id/1332529

Kerns, A. J., Shepard, D. P., Bhatti, J. A., & Humphreys, T. E. (2014). Unmanned Aircraft Capture and Control Via GPS Spoofing. *Journal of Field Robotics*, *31*(4), 617–636. https://doi.org/10.1002/rob.21513

Kim Zetter. (2015, May 26). *Is It Possible for Passengers to Hack Commercial Aircraft? | WIRED*. Wired. https://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft/

Kuni Parker. (2019, February 23). *Resiliency in Utah Air National Guard* [Personal communication].

Kyle Rempfer. (2019, February 20). *Air Force chief defends F-35A against critics, boasting kills at Red Flag* [News]. Air Force Times. https://www.airforcetimes.com/news/your-air-force/2019/02/20/air-force-chief-defends-f-35a-against-complaints-boasting-kills-at-red-flag/

Losey, S. (2019, February 8). *The Air Force still has a serious maintainer staffing problem, GAO says—But no strategy to fix it*. Air Force Times. https://www.airforcetimes.com/news/your-air-force/2019/02/08/the-air-force-still-has-a-serious-maintainer-staffing-problem-gao-says-but-no-strategy-to-fix-it/

Martin, J. (2019, February 27). *US Air Force chief on the F-35 'quarterback,' new and improved F-15, and future of light attack*. Defense News. https://www.defensenews.com/interviews/2019/02/27/us-air-force-chief-on-the-f-35-quarterback-new-and-improved-f-15-and-future-of-light-attack/

Mizokami, K. (2018, November 14). *The F-35's Greatest Vulnerability? Being Hacked.* Popular Mechanics. https://www.popularmechanics.com/military/aviation/a25100725/f-35-vulnerability-hacked/

Mizokami, K. (2019, April 3). *Report: Russia Engaging in Widespread Satellite Navigation Spoofing*. Popular Mechanics. https://www.popularmechanics.com/military/weapons/a27032602/report-russia-engaging-in-widespread-satellite-navigation-spoofing/

Mola, R. A. (2007, October 8). *Shutdown of National Airspace System was 'organized mayhem.'* Aviation International News. https://www.ainonline.com/aviation-news/aerospace/2007-10-08/shutdown-national-airspace-system-was-organized-mayhem

Nick Zazulia. (2018, February 21). *US Air Force Hacked in the Name of Security*. Avionics. https://www.aviationtoday.com/2018/02/21/air-force-hacked-name-security/

Nigel Chiwaya, & Jiachuan Wu. (2019, March 13). *MAP: These are the countries that have grounded the Boeing 737 MAX 8*. NBC News. https://www.nbcnews.com/news/world/country-banned-boeing-737-max-airplanes-list-n982776

Overview of Cyber Vulnerabilities | ICS-CERT. (n.d.). US CERT Dept of Homeland Security. Retrieved April 3, 2019, from https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities

Pieter Arntz. (2018, November 15). *Compromising vital infrastructure: Air traffic control*. Malwarebytes Labs. https://blog.malwarebytes.com/security-world/business-security-world/2018/11/compromising-vital-infrastructure-air-traffic-control/

P.W. Singer, & August Cole. (2015). *Ghost Fleet: A Novel of the next World War* (2016th ed.). First Mariner Books.

Ramsdell, K. W. (n.d.). *Boeing 757 Hacked in DHS Test*. Aviation International News. Retrieved February 7, 2019, from https://www.ainonline.com/aviation-news/air-transport/2018-02-01/boeing-757-hacked-dhs-test

Rogers, A. (2019, January 26). The Excruciating, Impossible Science of Airport Delays. *Wired*. https://www.wired.com/story/the-excruciating-impossible-science-of-airport-delays/

Ryan Pickrell. (2019, February 21). *Air Force F-35s absolutely wrecked their enemies during a mock air combat exercise, officials say*. Task & Purpose. https://taskandpurpose.com/air-force-f35-red-flag-exercise

Sally Donnelly. (2001, September 14). *The Day the FAA Stopped the World—TIME* [News]. Time. http://content.time.com/time/nation/article/0,8599,174912,00.html

Samir C. Jain, & Lisa M. Ropple. (2018, December 14). *Stopping Data Breaches Will Require Help from Governments*. Harvard Business Review. https://hbr.org/2018/12/stopping-data-breaches-will-require-help-from-governments

Scott Goolik. (2018, September 27). Cyber Security Threats: Why Detection Takes So Long. *Symmetry Corporation*. https://symmetrycorp.com/blog/cyber-security-threats-detection-takes-long/

Sitaonair. (2018, July 16). *SITAONAIR's Aircraft Internet of Things Takes Off With Pioneering AirBridgeCargo and CargoLogicAir Project*. AviationPros. https://www.aviationpros.com/aircraft/press-release/12420600/sitaonair-sitaonairs-aircraft-internet-of-things-takes-off-with-pioneering-airbridgecargo-and-cargologicair-project

Stephen K. Cusick, Antonio I. Cortés, & Clarence C. Rodrigues. (2017). *Commercial Aviation Safety* (6th ed.). McGraw-Hill Education. https://www.accessengineeringlibrary.com/browse/commercial-aviation-safety-sixth-edition/c9781259641824ch06lev1sec08

Steven J. Smith, PhD. (2019, February 28). *Conversation with Lt Col Steven Smith* [Personal communication].

Tajha Chappellet-Lanier. (2018, December 20). *Hack the Air Force 3.0 pays out $130,000 for 120 vulnerabilities found*. FedScoop. https://www.fedscoop.com/hack-the-air-force-3-results-hackerone/

Todd Humphreys. (2019, March 22). *GPS Interference and Countermeasures Arms Race*. Center for Anticipatory Intelligence Course Session, Utah State University.

Tracy Rucinski, & Allison Lampert. (2019, March 20). With 737 MAX grounded, airlines face daily scheduling challenges. *Reuters*. https://www.reuters.com/article/us-ethiopia-airplane-usa-flights-idUSKCN1R11X3

Tsang, A., & Kitroeff, N. (2019, March 12). Boeing Shares Drop After Ethiopian Airlines Crash. *The New York Times*. https://www.nytimes.com/2019/03/11/business/boeing-stock.html

Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft. (2019). United States Government Accountability Office. https://www.gao.gov/assets/690/689478.pdf

Valerie Insinna. (2019, March 8). *Key piece of F-35 logistics system unusable by US Air Force students, instructor pilots*. Defense News. https://www.defensenews.com/air/2019/03/08/key-piece-of-f-35-logistics-system-unusable-by-us-air-force-students-instructor-pilots/

Wenz, J. (2015, March 2). *Air Traffic Control Is Vulnerable to Cyberattack*. Popular Mechanics. https://www.popularmechanics.com/technology/security/a14354/faa-air-traffic-control-cyberattacks/

Why The Number Of Military Aviation Accidents Has Sharply Increased. (2018, April 11). NPR.Org. https://www.npr.org/2018/04/11/601630170/why-the-number-of-military-aviation-accidents-has-sharply-increased

Williams, M. (2015, April 14). *US sounds alarm on hacking of passenger jets, air traffic control*. Computerworld. https://www.computerworld.com/article/2909527/us-sounds-alarm-on-hacking-of-passenger-jets-air-traffic-control.html

Woodrow Bellamy III. (2017, January 31). *Are GPS Jamming Incidents a Growing Problem for Aviation?* Avionics. https://www.aviationtoday.com/2017/01/31/are-gps-jamming-incidents-a-growing-problem-for-aviation/

Woody, C. (2017, December 4). *An overlooked part of the Air Force's personnel problem is going to take years to fix*. Business Insider. https://www.businessinsider.com/air-force-chief-of-staff-describes-effects-of-maintainer-shortage-2017-12