Cyber Resiliency of Aircraft Systems: A Literature Review

Antti Luoto[1] and Matti Hakkarainen[2]
[1]Tampere University, Finland
[2]Patria, Tampere, Finland

antti.luoto@tuni.fi
matti.hakkarainen@patriagroup.com

Abstract: Aircraft have an important role in the overall defense of almost every country. However, military aircraft are not only susceptible to traditional kinetic weapons but also to constantly developing cyber weaponry. There has been global growth in the number of cyber threats in recent years, and the field of military aviation is not outside the growing threat. The war in Ukraine and recent military aircraft procurements in Europe make the topic very timely. A highly skilled and resourced adversary is able to conduct complex long-term attacks that penetrate even well-protected systems, such as military aircraft systems. Even air-gap does not protect aircraft from cyber threats as modern aircraft have complex and networked avionics and support systems. The study aims to find the current trends of cyber security research related to aircraft systems. The included topics are, for example, cyber resiliency and cyber protection in the system life cycle. The study concentrates particularly on forming an overall view of the most vulnerable military aircraft systems. The study presents a non-systematic literature review based on public data sources, such as research reports, articles, etc. A set of nine relevant sources was chosen for detailed qualitative analysis. Because of the lack of detailed military sources, applicable study materials related to commercial passenger aircraft were included. The results suggest that the most vulnerable aircraft systems from the viewpoint of cyber security are those that are exposed to threats via communication and satellite systems. Other vulnerable systems are sensors and avionics systems that transfer, or process critical data related to the functions of the aircraft. In addition, the study found that it is difficult to protect aircraft systems from cyber threats because of their complexity, maintenance operations, and supply chains, which also increase the size of the attack vector. To tackle the issue, it is important to follow the development of regulations and policies related to cyber security in aviation and to study the methods of managing the threat in a holistic and cost-effective manner.

Keywords: Cyber Resiliency, Cyber Security, Aircraft Systems, Cyber Defence

1. Introduction

This paper studies the effect of cyber threats to aircraft systems, especially from the viewpoint of combat aircraft. It has been estimated that at least 75 percent of the performance and capability of a modern aircraft is based on software (Alford, 2010). A modern military aircraft is not a closed system even if it is not directly connected to the internet or other networks (Alford, 2010). Rather, it is heavily dependent on external support systems, that increase the size of the attack vector making the aircraft more vulnerable to cyber threats (Alford, 2010).

One reason for a cyber-attack against combat aircraft is that they are an important part of every nation's defense, and it is easy for other nations to exploit weaknesses in airspace defense (Biswas, 2019). In this light, combat aircraft and their systems have a high potential to be targeted by a cyber operation. In addition to influencing a military system in various ways, the attacker may collect intelligence and steal information with an aim to develop their own capabilities (Snyder et al, 2015).

The goal of this study was to investigate the state and the level of cyber resiliency of aircraft systems. There was a need to identify which aircraft systems are the most vulnerable and find ways of testing them from the viewpoint of cyber resiliency. In this context, the study aims to produce knowledge about the current state of cyber protection, cyber testing, cyber monitoring, and cyber research.

The scope of the study is on the systems of combat aircraft. However, it must be noted that, for example, related ground systems, such as mission planning and maintenance systems, need to be also considered because they increase the number of threats that can be exploited when attacking the actual aircraft.

The main research question is: what are the most vulnerable aircraft systems from the viewpoint of cyber resilience? The following sub-questions were used to find answers to the main question. What cyber threats are targeted to aircraft equipment and what makes aircraft equipment prone to cyber vulnerabilities? Which avionics systems stand out as vulnerable systems?

The used research method is a non-systematic literature review based on scientific publications, technical reports, and other related public material. Many of the available data sources concentrate on civilian aviation. In a military context, the public material is more on a general level rather than going deep into the technical

details of military aircraft. The reason may be that detailed studies on the topic do not exist, or the topic is so sensitive that information is not publicly available. However, the study material on civilian aviation may be used as a data source for this study because civilian and military aircraft share common systems.

The material for the analysis conducted was chosen based on the richness of relevant information from the viewpoints of both quality and quantity. A chosen source had to contain a discussion related to cyber resiliency or cyber threats of aircraft systems either from a civilian or military perspective. Nine publications were chosen for the detailed analysis. The collected material was deductively analyzed to form conclusions about the most vulnerable combat aircraft systems from the viewpoint of cyber resiliency.

2. Cyber Threats and Cyber Resiliency of Aircraft Systems

This section describes the related background. First, it motivates the reader by describing the current threat environment. Then it discusses threat analysis that is important for cost-efficient cyber security. Finally, the section introduces attack vectors of aircraft and attack methods that can be used against them.

2.1 Growing and Developing Threat

Many can identify that IT systems belong to a cyber environment, but IT systems are only a subset of systems that are vulnerable to cyber-attacks. These vulnerable systems form a risk to successfully perform military operations (Snyder et al, 2015), (Weinman, 2020). The complexity and the scale of cyber threats make understanding the issue, prioritization, and implementation of countermeasures challenging. It may be difficult to detect, manage, and communicate vulnerabilities, and thus it is difficult to conceptualize cyber threats (IATA Regional Office, 2019).

In civilian aviation, cyber threat is a challenge because all information related to a flight is in networked digital form – even during a flight (IATA Regional Office, 2019). In a military context, the cyber dimension is a challenge for the same reason because the present-day military is dependent on information and communication systems. Even though a modern and continuously developed fighter plane offers ways to fight against evolving military threats, it is dependent on information. This dependency creates a cyber threat by offering various channels to penetrate systems and thus impede or prevent the operation of an aircraft (Lydiate, 2019). In addition, while military sector can adopt solutions from civilian aviation, they cannot rely on the commercial sector to have ready solutions for electronic warfare, Global Positioning System denial of service, and platform attrition (United States Air Force, 2019).

Cyber risk is increased also because the equipment related to weapon systems has not been necessarily designed with cyber in mind. This concerns especially operative equipment that is not considered IT equipment traditionally (Weinman, 2020). Because of the long-life cycle of military aircraft, this may be a cyber issue since cyber-attack methods are continuously evolving while the aircraft is not actively developed anymore. Though the history of cyber-attacks is mostly related to ICT systems with few physical effects, the possibility for such an attack targeted to software or avionics of a fighter plane cannot be excluded (Weinman, 2020). Similarly to the famous Stuxnet worm, that was targeted to a specific piece of hardware, adversaries could attack specific aircraft systems (Weinman, 2020). Lehto and Limnéll (2017) emphasize that a cyber-physical environment, where threats do not only target the virtual world but also physical hardware, is essential in the future.

Defence systems are nowadays more networked than ever before, increasing the overall complexity. For example, the embedded software and information technology systems found from modern military aircrafts include targeting systems, industrial control systems, databases, microelectronics, life support systems, collision avoidance system, logistics system, flight software system, controller area network bus, and communication systems (Chaplain, 2018). In addition, weapon systems that are not directly connected to networks may be, in one way or another, dependent on other networked systems (Chaplain, 2018). Examples of such systems include radar receiver, radio communications receiver, wireless communications link, operator's personal electronics, maintenance ports, and onboard diagnostics ports (Chaplain, 2018).

New technologies, such as smart airports and e-enabled aircraft, developed to improve the quality of service of aviation introduce new cyber-attack surfaces (Ukwandu et al, 2022). The roots of such technology are in relatively recent developments such as IoT, sensors in physical systems, blockchain, AI, cloud and big data (Ukwandu et al, 2022).

Many technology development projects, that are important for the United States Air Force, are executed by commercial companies instead of the United States defence administration (United States Air Force, 2019). This international technology business offers possibilities for other nations to develop new military capabilities (United States Air Force, 2019). Examples of such important technologies are related to advanced computing and wireless technologies (United States Air Force, 2019).

Implementing solid cyber protection for aviation is a massive challenge because of the networked architecture, the complexity of the technology, and its speed of change (Ukwandu et al, 2022). The challenge is increased because there are legacy systems used in parallel with the new emerging solutions (Ukwandu et al, 2022). For example, in 2017 a team of government, industry, and academic researchers hacked into a legacy Boeing 757 via radio communications (Biesecker, 2017). In addition, the lack of resources for cyber protection does not make the issue easier (Ukwandu et al, 2022). Another challenge in the future is to design systems and services with cyber security in mind but maintain cost-effectiveness and safety.

According to Eurocontrol (2019), cyber-attacks in the aviation sector have risen 530% from the year 2019 to 2020. The majority of these attacks (61%) have been targeted at airlines (Eurocontrol, 2019). 36% of the reported incidents were data theft, 35% fraudulent websites, 16% phishing, 5% malware, and 5% ransomware (Eurocontrol, 2019). Further, the supply chains of the aviation industry pose a threat because actors may have insufficient information security protection in their systems (Eurocontrol, 2019), (Weinman, 2020).

There are a lot of deficiencies in the management of cyber security in aviation and military technology (IATA Regional Office, 2019), (Lydiate, 2019). The reason may be that there seems to be a lack of cyber security regulation and understanding of cyber security among managers and commanders (IATA Regional Office, 2019), (Lydiate, 2019), (Chaplain, 2018). Before 2019, the regulation and standards of aviation and especially aircraft systems were seen to be either under development or being updated so that they will better consider the requirements of cyber security and evolving cyber threats (Chaplain, 2018), (U.S. Department of Defence, 2013). In 2020 and 2021 the standards had been updated to some extent (IATA, 2021). Recent updates to publicly available standards aim to bind management together with cyber security using risk management as a method. However, it is expected that the field of aviation still has a lot to do in determining common goals, strategies, and policies related to cyber security.

Eurocontrol (2019, 2) suggests all actors forget the illusion that there is no cyber threat or that their systems are protected because there have not been incidents recently. Further, the details of severe cyber-attacks are most likely classified (Weinman, 2020). The fact that there are not many publicly known successful attacks against aircraft systems and the belief that airgap protects systems increases the challenge in cyber awareness (Weinman, 2020), (Chaplain, 2018). In addition, the security certificates received by system vendors are often incorrectly trusted as a guarantee of security. For example, general cyber security expertise is not the same as weapon systems cyber security expertise (Chaplain, 2018).

There are a lot of open challenges in the cyber security of aviation. These challenges and defects are related, for example, to inadequate testing methods (Chaplain, 2018), monitoring of cyber security (Weinman, 2020), reacting to defects (Muckin and Fitch, 2014), sharing knowledge regarding cyber incidents (Muckin and Fitch, 2014), complexity (Chaplain, 2018), and lack of open information (Chaplain, 2018). In addition, maintenance (Weinman, 2020) and integration with legacy systems (Ukwandu et al, 2022) increase the threat. Last but not least, the fact that humans are often the weakest link makes the cyber threat an obvious challenge.

2.2 Methods of Threat Analysis

An adversary must perform the following five tasks to succeed in a cyber-engagement (Bryant and Ball, 2020). An active cyber weapon must search for aircraft. The aircraft must then be detected in cyberspace. The adversary must decide which pathway to the target will be used. The launched cyber-warhead must be successfully transported into the target aircraft's systems. And finally, the cyber-warhead is triggered causing system malfunctions.

Cyber Kill Chain is a framework developed by Lockheed Martin for making countermeasures and analyzing cyber threats (Ranum, 2014). The framework presents a cyber threat as a chain of attacks with which the attacker aims to achieve their goals (Ranum, 2014). The framework aims to combine organizations that develop a system with those that operate the system so that threat analysis and intelligence together can break the chain of attacks (Muckin and Fitch, 2014).

Weinman (2020) notes that the Cyber Kill Chain is mainly targeted for threat analysis of traditional IT systems and suggests that aircraft cyber threat analysis may be conducted with the Aircraft Combat Survivability (ACS) model, which is traditionally used for analyzing aircraft survivability against kinetic weapons. Based on ACS, Weinman (2020) proposes an Aircraft Cyber Combat Survivability (ACCS) model, that may be used to analyze an aircraft's survivability against cyber-attacks. Weinman (2020) identifies the following five key differences between ACS and ACCS. (1) Detecting cyber weapons may be more difficult when compared to traditional weapons. (2) Cyber weapons have basically an unlimited range and do not have physical limitations as traditional kinetic weapons may have. (3) Cyber weapons are not as predictable as traditional kinetic weapons. (4) Cyber weapons do not have a long military history which makes estimating their effects difficult. (5) Cyber weapons can be rendered harmless relatively easily after detection.

2.3 Attack Vectors and Methods of Attacking Aircraft Systems

While cyber threats can be analyzed with frameworks, such as Cyber Kill Chain, a challenge related to combat aircraft is that there are multiple networked systems that are dependent on each other. There is always a possibility for an attack when information is transferred in or out of the system (Chaplain, 2018). The technical reasons that make aircraft systems vulnerable are numerous electronic interfaces, networking, information exchange, and external systems (Chaplain, 2018).

Weinman (2020) states that the communication channels of an aircraft are not always encrypted. Thus, it is possible for an adversary to intercept such a channel and inject false information or cut the channel off (National Business Aviation Association, 2016). Weinman (2020) lists the following aircraft's attack surfaces: radar, radio communications, data links, GPS, SATCOM, software development, supply chain, pods, smart weapons, maintenance systems, mission planning, mission debriefing, and data transfer devices (referencing to a presentation by Bryant & Young).

Systems with a capability for direct external communication include data links that communicate with command and control or identification, friend or foe (IFF) systems that communicate with the flight control systems situated on the ground. These two external systems differ from each other significantly. A military command and control system is part of a classified military system, whereas a flight control system is part of a globally networked civilian system. Despite the fact that military systems are classified, they are networked in various ways.`

A cyber adversary may affect the operative capabilities in two ways (Snyder et al, 2015). It is possible to steal technology or data or to directly hit operative systems which can weaken the operative capabilities of the target (Snyder et al, 2015). The methods of attacking aircraft systems are the same as against any other IT system. For example, Weinman (2020) mentions Trojan horse, trapdoor, backdoor, virus, worm, keystroke logging, and impersonation (Weinman, 2020).

Modern aircraft has a lot of sensors for data collection. Sensor jamming, spoofing, and meaconing are types of methods that have a degrading effect on the collected data (Sabatini, 2016), (Blasch et al, 2019). Jamming means transmission of high-power signals to impede reception of radio signals (Wei et al, 2007). Spoofing means synthesizing a false signal to deceive a target's positioning or tracking, whereas meaconing means capturing a signal and rebroadcasting it with alterations (Manesh et al, 2019). Radiofrequency (RF), electro-optical, and global navigation satellite system (GNSS) interfaces are susceptible to such attacks (Sabatini, 2016). By attacking via the sensors of an aircraft it might be possible to effect situational awareness (Henselmann and Lehto, 2019). Such an attack could prevent systems from functioning (Chaplain, 2018) or inject falsified data (Henselmann and Lehto, 2019).

While the focus of protection has been on software, the attacks have stepped towards hardware (Lehto and Limnéll, 2017). The attacks can occur already during the production process when malware is installed during assembly or warehousing (Lehto and Limnéll, 2017). For aviation systems, such attack possibilities include systems under maintenance, testing, or repair (Lehto and Limnéll, 2017). Therefore, systems require surveillance and management during the whole life cycle (Lehto and Limnéll, 2017). For example, a subversive die, that modifies the behavior of the processor, can be added to an integrated circuit, and detecting such a modification can be difficult (U.S. Department of Defence, 2013).

An attack operation may be very complex, distributed, and it may be executed over a long period of time by combining different attack methods (Weinman, 2020). For example, a backdoor in software can wait for a trigger command that is delivered using a different method (Weinman, 2020).

3. Results

Nine publications were chosen for the detailed literature analysis: (Henselmann and Lehto, 2019), (Lydiate, 2019), (Bogoda, Mo, Bil, 2019), (Mink et al, 2016), (Sabatini, 2016), (Weinman, 2020), (Ukwandu et al, 2022), (Chaplain, 2018), and (Thudimilla, 2020). These publications discuss the topic so extensively that it was possible to use them for answering at least two research questions. Possible attacks on systems of fighter planes can be conducted using similar attack methods that can be used to attack any electronic or IT system. While the systems used by the military often have better protection than civilian systems, for example, from the viewpoint of facility, personnel, and information security, the protections are not, however, on an adequate level to completely protect from cyber threats. The air interface and facility security cannot protect aircraft systems because they are networked with other systems and have long maintenance and supply chains. It must be noted that networking in this context does not mean that a system needs to be continuously connected to an IT network. It means that it is repeatedly connected, via various interfaces, to other systems during its life cycle. These connections always offer possibilities for attacking.

Even though combat aircraft and civilian passenger aircraft vary a lot from the viewpoints of system design and applications, they are threatened by similar cyber threats to some extent. When military aircraft operate in the same airspace or airfields as civilian aircraft, military aircraft use the same or similar systems for navigation, communication, identification, and landing. Examples of such systems include global positioning system (GPS), very high frequency (VHF) omnidirectional range with distance-measuring equipment (VOR/DME), ground-based augmentation system (GBAS), identification, friend or foe (IFF), and automatic dependence surveillance-broadcast (ADS-B) (Bogoda, Mo, Bil, 2019).

Based on the analysis, the most vulnerable systems are communication systems that are used for transferring speech or data between aircraft and external systems. From ground-to-air systems, the most critically vulnerable seem to be data link systems (also known as data flow systems), that transfer data between aircraft and ground systems. Five references mentioned these systems (see Table 1). Other mentioned systems include, for example, the Aircraft Communication Addressing and Reporting System (ACARS), software radio, and RF systems.

Satellite-based communication and navigation systems were also seen as critically vulnerable systems. A common factor in these systems is that by penetrating the ground system, it is possible to directly influence the aircraft during the flight.

Another vulnerable category was sensors. It is also possible to influence these systems directly during the flight. From the other aircraft and avionics systems, systems related to flight control, data buses (such as Avionics Full-Duplex Switched Ethernet (AFDX)), operating systems, and mission support were seen as vulnerable. Table 1 categorizes and summarizes the identified vulnerable systems.

Table 1: The categorization of vulnerable aircraft systems.

Avionics (tot. 5)	Communication (tot. 11)	Recording (tot. 2)	Sensors (tot. 5)	Satellite (tot. 10)
Data buses (Henselmann and Lehto, 2019)	Data links (Henselmann and Lehto, 2019), (Weinman, 2020), (Ukwandu et al, 2022), (Lydiate, 2019), (Bogoda, Mo, Bil, 2019)	Mission & Maintenance (Henselmann and Lehto, 2019), (Weinman, 2020)	Radar (Henselmann and Lehto, 2019), (Weinman, 2020), (Chaplain, 2018), (Bogoda, Mo, Bil, 2019)	GNSS/GPS (Henselmann and Lehto, 2019), (Weinman, 2020), (Bogoda, Mo, Bil, 2019)
Operating systems (Ukwandu et al, 2022)	Software radio (Henselmann and Lehto, 2019)		Infrared (Henselmann and Lehto, 2019)	Galileo (Henselmann and Lehto, 2019)
AFDX (Henselmann and Lehto, 2019)	RF (Weinman, 2020), (Henselmann and Lehto, 2019), (Chaplain, 2018)			SATCOM (Weinman, 2020), (Ukwandu et al, 2022)
Flight control (Bogoda, Mo, Bil, 2019), (Mink et al, 2016)	ACARS (Ukwandu et al, 2022), (Bogoda, Mo, Bil, 2019)			ADS-B/ADS-C (Sabatini, 2016), (Ukwandu et al, 2022), (Thudimilla, 2020), (Bogoda, Mo, Bil, 2019)

We answer the research questions presented in the introduction section as follows. The main research question was “what are the most vulnerable aircraft systems from the viewpoint of cyber resilience”. According to the

literature analysis, the most vulnerable systems are communication systems, such as data links, followed by satellite systems, such as ADS-B/ADS-C. However, there are vulnerabilities also in sensors, avionics and recording systems.

The first sub-questions were "what cyber threats are targeted to aircraft equipment and what makes aircraft equipment prone to cyber vulnerabilities". The threats are very similar to traditional IT equipment. However, long supply chains, complexity, lack of information, integration with legacy systems, networking, and various communication channels are highlighted in the context of this paper.

The last sub-question was: "which avionics systems stand out as vulnerable systems". There was no system that was clearly mentioned more often than others but data buses, operating systems, ADFX and flight control systems were mentioned in the analyzed literature.

4. Conclusions and Future Work

Developing the cyber security of aircraft systems is important despite the fact that there have not been a lot of reported successful cyber-attacks on aircraft systems. Because of the complexity of military systems and their operational environment, alternative approaches to managing cyber security risks have been suggested as opposed to traditional information security-based approaches. One reason for this is that the cyber threat against combat aircraft needs to be managed cost effectively.

The results of the study cannot be considered very surprising considering the context and the available material. The most critically vulnerable aircraft systems seem to be those whose functions may be effected during flight by penetrating their ground or satellite systems. Following these, there are systems that an attacker may manipulate during flight and directly affect the operations of the aircraft. In addition, there are vulnerable systems that have an effect on flying and are heavily connected to other systems, such as databases or operating systems. These include mission and maintenance systems that require transferring data in to or out of aircraft via external systems.

Cybersecurity regulation and standards of aviation are under development, and it is important to follow the results of such work. Understanding the threat is crucial, so understanding counter methods, such as cyber threat intelligence (CTI), and tactics, techniques, and procedures (TTP) may be key in implementing cost-efficient cyber security.

A report by Snyder (2015) states that cyber security is implemented in the U.S. Air Force via acquisition events during procurement which does not provide continuous involvement of cyber security during the system life cycle (Snyder et al, 2015). In addition, a system may grow out of different programs which leads to a situation where a single program does not cover the whole system (Snyder et al, 2015). Dealing with a great number of policies and laws that can change faster than a military system with a long-life cycle was also considered a challenge (Snyder et al, 2015). Further, the governmental cyber security approach directs more toward securing IT systems than, for example, operating or weapon systems (Snyder et al, 2015). Finally, a relatively fast-changing and complex cyber environment makes management of cyber security difficult (Snyder et al, 2015). Cyber security of military systems should be about making robust and resilient designs that consider the survivability requirements (Snyder et al, 2015).

At the moment, risk management in cyber security is often based on fulfilling the requirements of various policies (Muckin and Fitch, 2014). It directs the organization's actions toward information security management and vulnerabilities (Muckin and Fitch, 2014). This explicit attention to information security and vulnerabilities may lead to a situation where risk management does not consider the most critical factor, the threat (Muckin and Fitch, 2014). Such an imbalance may turn out as reactive actions after cyber incidents instead of pre-emptive actions (Muckin and Fitch, 2014).

Muckin and Fitch (2014) list three gaps that restrict the development of cyber security. (1) Culture, behavior, and the amount of "resources allocated to implementing and adhering to compliance requirements". (2) The lack of scalable and formal cyber threat intelligence. (3) The lack of cooperation and integration between different parts of the organization. The gaps lead to a reactive environment, where the system is designed with a controls-first mindset that emphasizes, for example, compliance with the implemented information security controls, where money is wasted on controls that do not address actual threats (Muckin and Fitch, 2014).

As a future work, it might be interesting to make a review on the cyber security of a related topic, such as logistics systems and supply-chain management of aviation. The aspects included might be, for example, the usage and

the role of artificial intelligence and machine learning in the cyber protection of logistics. Specific cyber security tools and components used in the field could also be investigated.

References

Alford, L. D. (2010) "Cyber Warfare: The Threat to Weapon Systems", *The WSTIAC Quarterly*, Vol 9, No. 4.

Biswas, K. (2019) "Military Aviation Principles", *Military Engineering. Ed. by George Dekoulis. Rijeka: IntechOpen*, Chap. 1, DOI: 10.5772/intechopen.87087, [online], https://doi.org/10.5772/intechopen.87087.

Biesecker, C. (2017). "Boeing 757 testing shows airplanes vulnerable to hacking, DHS says." *Avionics International*.

Blasch, E., Sabatini, R., Roy, A., Kramer, K. A., Andrew, G., Schmidt, G. T., Carlos, C. and Fasano, G. (2019) "Cyber awareness trends in avionics", *IEEE/AIAA 38th Digital Avionics Systems Conference (DASC)*, IEEE, September, pp 1–8.

Bogoda, L., Mo, J., and Bil, C. (2019) "A systems engineering approach to appraise cybersecurity risks of CNS/ATM and avionics systems", *Integrated Communications, Navigation and Surveillance Conference (ICNS),* IEEE, 2019, pp 1–15.

Bryant, W. D. and Ball, R. E. (2020) "Developing the Fundamentals of Aircraft Cyber Combat Survivability: Part 2", *Aircraft Survivability Journal*, Joint Aircraft Survivability Program Office.

Chaplain, C. (2018) *Weapon Systems Cybersecurity: DoD just beginning to grapple with scale of vulnerabilities*, GAO Report No. GAO-19-128. Washington, DC, USA.

Eurocontrol (2019) *Aviation under Attack: Faced with a Rising Tide of Cybercrime, Is Our Industry Resilient Enough To Cope?,* [online], https://www.eurocontrol.int/sites/default/files/2021-07/eurocontrol-think-paper-12-aviation-under-cyber-attack.pdf.

Eurocontrol (2019). *Being cyber secure is an illusion... let's become cyber resilient all together!,* [online], https://www.eurocontrol.int/sites/default/files/2020-01/eurocontrol-think-paper-3-cybersecurity-aviation.pdf.

Henselmann G., and Lehto, M. (2019) "Where Cyber Meets the Electromagnetic Spectrum". *18th European Conference on Cyber Warfare and Security (ECCWS)*, Academic Conferences and publishing limited, pp 209–218.

IATA (2021) *Compilation of Cyber Security Regulations, Standards, and Guidance Applicable to Civil Aviation*, *Edition 3.0,* Tech. rep.

IATA Regional Office, Asia Pasific (2019). *Aviation Cyber Security Roundtable,* Tech. rep, Singapore.

Lehto, M. and Limnéll J. (2017) "Kybersodankaynnin kehityksesta ja tulevaisuudesta", *Tiede ja ase,* Vol. 75, [online], https://journal.fi/ta/article/view/67730.

Lydiate, D. (2019) "Military Aviation's Cyber Challenge; Are Cyber-Vulnerabilities a Credible Threat to a Modern Air Force?", *Air Power Review*, Vol 22, No. 1, pp 6–38.

Manesh, M. R., Kenney, J., Hu, W. C., Devabhaktuni, V. K., Kaabouch, N. (2019) "Detection of GPS spoofing attacks on unmanned aerial systems". *16th IEEE Annual Consumer Communications & Networking Conference*, pp 1–6.

Mink, D., Yasinsac. A., Choo. K. and Glisson, W. (2016) "Next Generation Aircraft Architecture and Digital Forensic.", *22th Americas Conference on Information Systems*, San Diego, pp 1–10.

Muckin, M. and Fitch, S. C. (2014) *A threat-driven approach to cyber security*, Lockheed Martin Corporation.

National Business Aviation Association (2016) *Cyber Security: Top Flight Department Threats*, [online], https://nbaa.org/aircraft-operations/security/cyber-security-top-flight-department-threats/.

Prisaznuk, P.J. (1992) "Integrated modular avionics", *Proceedings of the IEEE 1992 National Aerospace and Electronics Conference*, Vol. 1, pp 39–45, doi: 10.1109/NAECON.1992.220669.

Ranum, M. (2014) "Breaking Cyber Kill Chains", [Blog], https://www.tenable.com/blog/breaking-cyber-kill-chains (visited 03/15/2023).

Sabatini, R. (2016) "Cyber security in the aviation context", *First Cyber Security Workshop*.

Snyder, D., Powers, J. D., Bodine-Baron, E., Fox, B., Kendrick, L. and Powell M. H. (2015) *Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles*, RAND Corporation, Santa Monica, CA.

Thudimilla, A. (2020) "Cyber physical security of avionic systems", PhD thesis, Missouri University of Science and Technology.

Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, I., Bellekens, X. (2022) "Cyber-security challenges in aviation industry: A review of current and future trends", *Information*, Vol 13, No. 3, 146.

United States Air Force (2019) *Science and technology strategy: Strengthening USAF science and technology for 2030 and beyond*.

U.S. Department of Defence (2013) *Resilient military systems and the advanced cyber threat*, Tech. rep., Defense Science Board.

Watkins, C., B. and Walter, R. (2007) "Transitioning from federated avionics architectures to Integrated Modular Avionics", *2007 IEEE/AIAA 26th Digital Avionics Systems Conference*, 2.A.1–1–2.A.1–10. DOI: 10.1109/DASC.2007.4391842.

Wei, M., Chen, G., Cruz, J. B., Haynes, L. S., Pham, K., Blasch, E. (2007) "Multi-Pursuer Multi-Evader Pursuit-Evasion Games with Jamming Confrontation," *Journal of Aerospace Computing, Information, and Communication,* Vol 4, No. 3, pp 693–706.

Weinman A. K. (2020) "Aircraft Cyber Combat Survivability", MA thesis, NAVAL POSTGRADUATE SCHOOL MONTEREY CA.