2016 8th International Conference on Cyber Conflict
Cyber Power
N.Pissanidis, H.Rõigas, M.Veenendaal (Eds.)
2016 © NATO CCD COE Publications, Tallinn

Assessing the Impact of Aviation Security on Cyber Power

Martin Strohmeier
Department of Computer Science
University of Oxford
Oxford, United Kingdom
martin.strohmeier@cs.ox.ac.uk

Vincent Lenders
Science and Technology
armasuisse
Thun, Switzerland
vincent.lenders@armasuisse.ch

Matthias Schäfer
Department of Computer Science
University of Kaiserslautern
Kaiserslautern, Germany
schaefer@cs.uni-kl.de

Ivan Martinovic
Department of Computer Science
University of Oxford
Oxford, United Kingdom
ivan.martinovic@cs.ox.ac.uk

Matt Smith
Department of Computer Science
University of Oxford
Oxford, United Kingdom
matthew.smith@cs.ox.ac.uk

Abstract: We analyse the impact of new wireless technology threat models on cyber power, using the aviation context as an example. The ongoing move from traditional air traffic control systems such as radar and voice towards enhanced surveillance and communications systems using modern data networks causes a marked shift in the security of the aviation environment. Implemented through the European SESAR and the US American NextGen programmes, several new air traffic control and communication protocols are currently being rolled out that have been in the works for decades. Unfortunately, during their development the shifting wireless technology threat models were not taken into account. As technology related to digital avionics is getting more widely accessible, traditional electronic warfare threat models are fast becoming obsolete.

This paper defines a novel and realistic threat model based on the up-to-date capabilities of different types of threat agents and their impact on a digitalised aviation communication system. After analysing how the changing technological environment affects the security of aviation technologies, current and future, we discuss the reasons preventing the aviation industry from

quickly improving the security of its wireless protocols. Among these reasons, we identify the existing tradition of the industry, the prevalence of legacy hard- and software, major cost pressures, slow development cycles, and a narrow focus on safety (as opposed to security). Finally, we analyse how this major technological shift informs the future of cyber power and conflict in the aviation environment by looking at tangible effects for state actors.

Keywords: *aviation security, cyber power, critical infrastructures, wireless attacks, communication security, aviation privacy*

1. INTRODUCTION

Modern wireless data networks are becoming increasingly important as a communication tool for aircraft and ground surveillance alike. While it has been well known for years within the computer security community [1] that both current and future aviation communication and surveillance systems do not offer enough – or any – protection against cyber attack, the concrete impact on cyber power has not been analysed so far.

As wireless communications technology advanced rapidly over the past two decades, commercial-off-the-shelf (COTS) hardware with the ability to affect wireless systems within aviation has become widely available. The long technological upgrade cycles for digital avionics systems guarantee that the employed wireless technology becomes dated at some point during its life cycle, which profoundly affects the security of these technologies in particular. As a result, traditional electronic warfare threat models have become obsolete and can no longer provide the basis for the security analysis of civil aviation.

Instead, a modern threat model must consider the impact of potential attacks not only on the electromagnetic spectrum but also on the increasingly digitalised aviation communications system as a whole. Combining both modern cyberspace operations, and traditional electronic warfare under the umbrella of Cyber Electromagnetic Activities (CEMA) is a relatively new concept which is quickly gaining importance within the defence community [2]. This article examines how CEMA can directly affect the critical infrastructure system of aviation with potentially devastating consequences.

We analyse how the wide proliferation of software-defined radio hardware and the accompanying development and accessibility of software tools and knowledge enable a large group of actors to both passively and actively engage with the aviation communications system. Because of these advances, the technological advantage and obscurity on which aviation's communications security is based has become untenable. As proprietary knowledge on aviation protocols is widely accessible, even unsophisticated actors with few resources cannot be prevented accessing the wireless communication used for ensuring air safety any more.

As the awareness of this issue has only started to increase recently [3], newly developed future communication technologies such as the Automatic Dependent Surveillance Broadcast protocol (ADS-B) do not solve this security problem but rather exacerbate it. We postulate that these existing security and privacy issues already have a measurable impact on current cyber conflicts, and analyse how this democratisation of wireless capabilities affects the cyber power of state actors.

The contributions of this paper are:

- We analyse the impact of recent technological advances in wireless communications and the digitalisation of avionics on the security of aviation protocols. Based on these insights, we develop a novel realistic threat model replacing the traditional electronic warfare model.
- Using the newly developed threat model, we classify the relevant threat agents based on their motivation and wireless capabilities. We analyse the security of wireless air traffic control protocols, current and future, based on our taxonomy.
- Finally, we discuss the impact of the changing threat environment on the cyber power of state actors in the aviation system. We postulate a democratisation of power, shifting away from nation states towards a much wider range of actors.

The remainder of this article is organised as follows. Section 2 discusses the new threat model faced by actors in aviation, and then Section 3 examines some of the threat agents involved in this model. Section 4 provides a security analysis of exemplary current and future aviation technology. Section 5 looks at the reasons for the current lack of security within civil aviation. Section 6 discusses the impact of security- and privacy-related technology advances on nation state actors and their cyber power. Section 7 briefly presents the related work on critical infrastructures and aviation security in particular. Finally, Section 8 concludes this work.

2. THE NEW CYBER THREAT MODEL IN AVIATION

In this section, we discuss recent advances made in wireless technologies, and how they have changed the threat landscape in the aviation context. As civil aviation systems increasingly move towards modern digital data networks, we further argue that this increased digitisation and automation leads to new vulnerabilities not present in the traditional aviation safety mind-set. We illustrate the impact of these developments on the security of aviation.

A. Recent advances in wireless technology

The technological advances in wireless technology happening in the late 1990s and 2000s drastically changed the assumptions about the capabilities of adversaries in wireless communication settings. One of the main drivers of this development has been software-defined radio (SDR) technology. SDRs were first developed for military and closed commercial use in the 1990s followed by open-source projects such as GNU Radio [4], which was released in 2001. In conjunction with the availability of cheap commercial off-the-shelf SDR hardware, new

technological capabilities became available to a large group of people. Anyone with a relatively basic technological understanding can now receive, process, craft, and transmit arbitrary radio signals such as those used in aviation systems. Where previously radio hardware needed to be purpose-built, an expensive and complicated endeavour feasible only for specialists, SDRs can be programmed and seamlessly adapted using software easily available on the Internet.

B. Move towards digital communication networks and automation

Complementing the technological advances available to the general public, we observe a trend in aviation towards transmitting data using unauthenticated digital communication networks. This digital data, which is as diverse as flight clearances, aircraft positions, or passenger information, is subsequently processed by increasingly automated systems on the ground and in the aircraft, which implicitly relies on the integrity of the received information to ensure the safety of air travel. Without authentication of the underlying protocols, attacks on the data link level are inherently more difficult to detect for both aviation systems and their users than attacks on traditional analogue technologies such as voice communication or primary surveillance radar.

C. Impact on aviation security

Together, the discussed technological trends and advances have had a profound impact on the security of wireless aviation protocols and consequently caused a fundamental shift in the applicable threat model. The move towards unsecured digital networks and increased deployment of COTS hard- and software in avionics enables new adversarial groups, which stand far outside the former military-inspired electronic warfare threat model [5].

The advent of SDR technology has provided a surge of applications for radio communications in general. The former assumption that access to the frequencies used by important communication technologies is hard has been voided. Modulations of virtually all radio applications are well known and made available freely through the SDR community. Thus, the ability to eavesdrop and manipulate any communication wireless channel is available to any interested observer without the requirement for significant resources and specialist knowledge. Examples of such possibilities are the trivial access to mobile phone networks, satellite signals, television channels, or wireless sensor networks.

One of the most active and enthusiastic SDR communities is concerned with aviation communication and flight tracking. Using, for example, the popular RTL-SDRs, a $10 USB stick repurposed as a software-defined radio receiver, a plane-spotter can choose between several different software options to receive virtually all air traffic communication protocols in use today (e.g. ADS-B [6]). Countless enthusiasts and volunteers around the world use such hard- and software to power a multitude of services such as flightradar24.com, opensky-network.org, or adsbexchange.com, where an ever-increasing number of flight movements can be followed live and without delay. Data from flight trackers has been involved regularly in investigations following flight incidents such as the Germanwings crash [7], or the two Malaysian Airlines aircraft lost over the Ukraine and the Indian Ocean in 2014, illustrating the impact of the changing communications landscape on aviation.

With more powerful SDRs, which are capable of sending as well as receiving, becoming cheaper and widely available, it is possible to manipulate virtually all aspects of the wireless channel used by aviation protocols [8]. These possibilities stand in stark contrast to the pre-SDR electronic warfare threat model focused on nation states being the only actors with the expensive and sophisticated capabilities required to attack ATC systems. The impact of this development on ATC is discussed in Section 4.

3. A TAXONOMY OF CYBER THREAT AGENTS

Based on the insights from the previous section, we develop a new threat model for wireless attacks in the aviation context focusing on CEMA threats. We analyse possible attackers based mainly on: a) their resources; b) their subject-matter expertise; and c) their motivation. Table 1 presents the threat agents applicable to wireless security in aviation, which we go on to discuss in detail. Our taxonomy is very loosely inspired by the relevant NIST definitions [9], but adapted for the unique context of the cyber-physical aviation system. While our approach to threat agents in aviation is novel, we believe that tying it into the existing NIST framework leads to easier application in practice. Our taxonomy provides new insights into the specific technological capabilities of different classes of threat agents, and how these can be exploited to achieve their respective goals, even in light of potential countermeasures.

TABLE 1: OVERVIEW OF THREAT AGENTS

Threat	Resources	Type	Goal/Motivation
Passive Observers	None - Very low	Passive	Information collection / Financial or personal interest
Script Kiddies / Hobbyists	Low	Active	Any noticeable impact / Thrill and recognition
Cyber Crime	Medium - High	Active	Maximising impact / Financial gains using e.g. blackmail or valuable information
Cyber Terrorism	Low - Medium	Active	Political or religious motivation / Massive disruption and casualties
Nation State	Unlimited	Active	Weapons / Targeting specific, potentially military objects

A. Passive observers

Passive observers are interested people who exploit the open nature of air traffic communication protocols to glean information. This class of threat agents does not actively interfere with air traffic communication, but instead uses public and private websites and mobile applications, which display air traffic and its communications in real time, to gather information about private or secret air traffic movements. Alternatively, they can employ cheap SDR receivers to gather their own undistorted picture of all air traffic in their vicinity, in real time or stored for later analysis. The information collected by such merely passive observers can be exploited in many ways, ranging from privacy concerns to the detection of military operations, which are discussed in detail in Section 6.

B. Script kiddies and hobbyists

Script kiddies and hobbyists are the lowest active threat in our model, based on their abilities concerning both hardware and knowledge. Their aim is to exploit well-known security holes with existing, easy-to-use attacks with typically low sophistication. Their motivation is regularly not rational; instead any identifiable impact is sought for thrill and recognition [9]. We assume an attack to be the following:

> Using a programmable transponder, they listen in to legitimate radio communication, modify the call sign and/or information such as position and velocity, and play it back. The objective of the attacker is to have their signals either shows up as a new aircraft with an unexpected call sign, or as an existing aircraft causing conflicting information. We assume that the attacker is on the ground and sends with the standard parameters of their transponder.

Hobbyists are typically interested in plane-spotting and more familiar with the norms and protocols in modern ATC, either due to personal interest in aviation or because it relates to their job. They are also more knowledgeable about radio communication and the basic characteristics of the wireless channel. They have access to SDRs and are able to operate them with matching software frameworks such as GNU Radio. Their attack is similar to that of the script kiddies, but it is not detected by naïve plausibility checks on the data link or physical level.

C. Cyber crime

The cyber crime attacker class seeks to attack systems for monetary gain. With sufficient subject-matter knowledge, software-defined radios, and potentially even small unmanned aerial vehicles (UAV), they are able to inject new messages or modify existing ones in such ways that they are not flagged by current detection systems. Cyber crime attackers are typically interested in causing maximum damage and exerting credible threats, as a pre-requisite for blackmail or to take advantage of captured inside knowledge.[1] Consequently, they are seeking to exploit any possible and effective way to attack ATC and aircraft systems.

D. Cyber terrorism

Attacks on cyber-physical systems powering critical infrastructures such as aviation are a natural target for terrorists and politically motivated attacks. Terrorists seek to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence [9]. By exploiting the vulnerabilities in wireless aviation communications, terrorist groups, which traditionally hijack or crash planes using physical weapons, could mount attacks on planes from the ground and from safe distances.

E. Nation states

With sufficient knowledge of intrusion detection systems and near-unlimited resources, it is possible to bypass plausibility checks and redundancy-based defences. While it becomes increasingly difficult to deceive many ATC systems at the same time, it is possible. However, we argue that it is only achievable by a nation state actor and part of the electronic warfare threat model traditionally outside the scope of securing civil aviation. In this case, non-transparent

[1] Aircraft movement information has allegedly been used for stock trading, see, e.g., [35]

countermeasures such as authentication through cryptographic means may help further, although this requires a complete overhaul of the protocol set and administrative planning [10]. Thus, it is unlikely to happen in the near future.

4. THE CASE OF AIR TRAFFIC CONTROL SURVEILLANCE

In order to demonstrate more clearly how aviation has to deal with the changing cyber security threat, this section presents an example technology: air traffic surveillance. The set of technologies used is integral to the safe operation of airspace, yet as it becomes more technologically advanced, it also becomes more insecure. This change is representative of avionic technology as a whole [11]. Throughout this section, we assess the technologies with respect to our threat model as seen in Table 2. From this, we attempt to match which systems are 'in reach' of a given attacker, which is summarised in Table 3.

TABLE 2: SUMMARY OF SURVEILLANCE TECHNOLOGIES

Technology	Ground/Air Dependent	Cost[2]	Deployment Status
PSR	Ground	High	In use
SSR	Ground	High	In use
TCAS (STANDARD)	Air	Moderate	Mandate by 2015[3]
TCAS (HYBRID)	Air	Moderate	Optional
ADS-B	Air	Low	Mandate by 2020
WAM	Ground	High	In deployment

A. Surveillance fundamentals

In order for ATC to safely manage airspace, each controller needs to understand the status of each aircraft under their control. Traditionally, Primary Surveillance Radar (PSR) and Secondary Surveillance Radar (SSR) in various forms have fulfilled this role since World War II.

Both systems were designed at a time when radio transmission required a great financial investment and expertise. Hence, no thought was given to securing the systems, as it was presumed that they would remain out of reach. The rise of SDRs voided this assumption; they marked the shift from potential attackers being well resourced to those with much less resource and capability.

PSR describes non-cooperative radar localisation systems. In civil aviation, these typically employ a rotating antenna radiating a pulse position-modulated and highly directional electromagnetic beam on a low GHz band. Potential targets in the airspace reflect the pulses; measurement of the bearing and round trip time of these reflections provides the target's

2 High cost is considered to be >$1 million, moderate > $100,000, low < $100,000.
3 For most civil aircraft, see Section 4.B.2.

position. Whilst PSR is not data-rich, it is relatively hard to attack as it relies on physical properties [11]. As such, we consider attacks on PSR to be out of scope of all but sophisticated nation state actors.

SSR is a cooperative technology with modern versions including the so-called transponder Modes A, C, and S. SSR provides more target information on ATC radar screens compared to PSR. Ground stations interrogate aircraft transponders using digital messages on the 1030 MHz frequency, which reply with the desired information on the 1090 MHz channel. Commodity hardware can receive and transmit on these frequencies, making them accessible to attack [3]. Very few skills are needed to receive SSR today, bringing it into reach of script kiddies and hobbyists, who might also be able to disturb ATC systems by simply injecting or replaying old SSR messages. To mount more sophisticated active attacks such as denial of service, slightly more skill and resource are needed, as is a definite motivation to disrupt, placing it in the cyber terrorism and cyber crime domains.

B. Current and next generation surveillance

NextGen and SESAR incorporate a range of surveillance technologies as part of the effort to reduce costs and increase efficiency [12]. Even though these technologies are in the early stages of deployment, they were designed decades ago. The result is that these systems have yet to be adapted to a modern threat model.

Mode S is a particularly important part of the current SSR system. It provides two systems of increasing significance in modern aviation: Automatic Dependent Surveillance-Broadcast (ADS-B), and Traffic Collision and Avoidance System (TCAS).[4] These systems are being rolled out as key factors in surveillance, in conjunction with multilateration techniques to provide redundancy. Due to an intentional lack of confidentiality, all SSR systems are subject to eavesdropping attacks by passive observers.

1. ADS-B

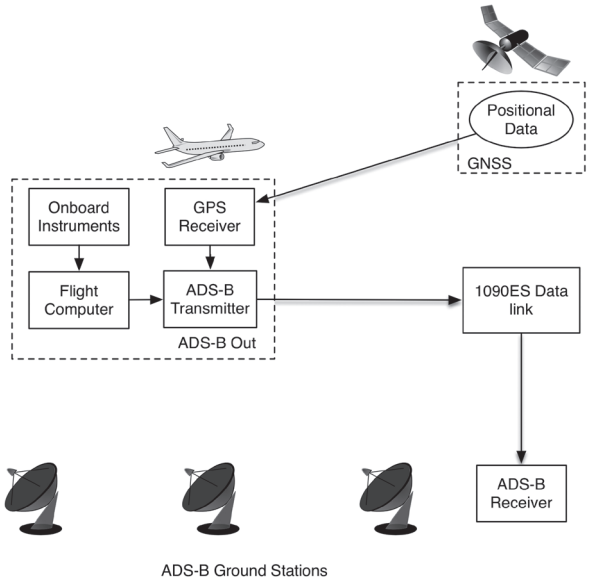
ADS-B is a protocol in which aircraft continually broadcast their own ID, position and velocity as well as further information such as intent or urgency codes. These broadcasts do not require interrogation but independently send the aircraft's position and velocity twice a second and unique identification every 5 seconds; Figure 1 provides a diagram of the system. It is currently in the roll-out phase, but as of today ADS-B is already operational within the Atlantic airspace and is integrated into modern collision avoidance systems (see Section 4.B.2). It is mandated for use by all aircraft from 2020 in all European and American airspace, and considered a key part of NextGen and SESAR [12].

The rise of SDRs has increased concerns about the security of ADS-B. Modern attacks only require standard COTS hardware to execute, as demonstrated in [8]. Trivially injected ADS-B messages claiming to be non-existing aircraft are impossible to distinguish from authentic ones on the link layer, regardless of the placement of the attacker. To conduct such an attack, it is sufficient to have a line of sight connection from the attacker to the legitimate ADS-B receivers operated by ATC, which are typically located in known positions on the ground at an airport or Area Control Centre.

4 TCAS is part of a larger family of technologies known as Airborne Collision and Avoidance System (ACAS)

Although in many cases redundant systems (such as multilateration) could help mitigate this isolated attack, this is unaccounted for in current standards and left to the implementation of every ADS-B user. Other attacks virtually modify the trajectory of an aircraft by selectively jamming an aircraft's messages and replacing them with modified data. This causes discrepancies between the real position and the one received by ATC. This is a worrying prospect, as ADS-B is set to be the main ATC protocol in the long term, with the FAA considering elimination of Mode A/C/S transponders at some point in the future [13].

FIGURE 1: ADS-B SYSTEM DIAGRAM



ADS-B is an example of a digitally networked surveillance protocol causing a move in the balance of power. Even script kiddies and honest-but-curious threat agents such as the hobbyist can exploit the protocol with commodity hardware able to send and receive on 1090 MHz and a range of open source decoders such as dump1090 [14]. Using the same tools, more capable and aggressive threat agents such as cyber terrorists and cyber criminals could launch attacks with relative ease. Works such as [8] describe in detail how attacks could take place with equipment costs in the thousands of dollars. Although attacks are theoretically cheap on ADS-B, if data fusion with other surveillance systems were used, then attacks would be required on all systems, increasing complexity for the threat agent. This would put it out of the reach of less sophisticated hobbyists and potentially even only in the reach of nation state attackers, depending on the resilience of the most secure technology.

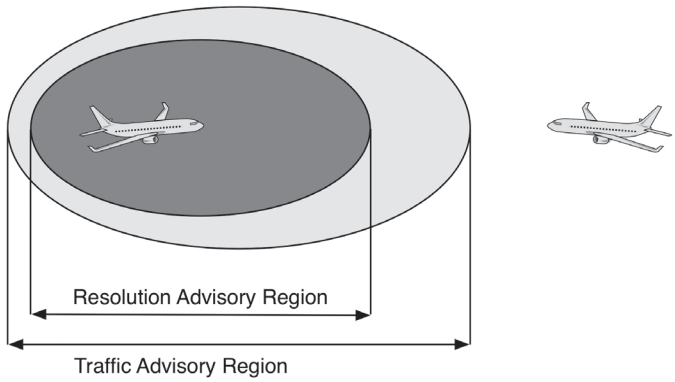
2. TCAS

TCAS allows aircraft to interrogate nearby aircraft in order to resolve airspace conflicts. For example, should another aircraft (referred to as the intruder) come within some predefined

range, TCAS will initially produce a Traffic Advisory (TA) notifying the pilot of traffic nearby. Should the intruder enter the immediate airspace of the aircraft, a Resolution Advisory (RA) will be produced which instructs one of the aircraft to change course. These regions are shown in Figure 2. Usually, the crew will have around 15 seconds to make this change. From 1st December 2015, TCAS is mandated for inclusion on civil aircraft carrying more than 19 passengers or with a minimum take-off weight of 5,700kg [15].

Since TCAS is based on Mode S, it uses an unauthenticated channel. This means that interrogations or responses can be injected as with ADS-B through the use of SDRs. An exemplary vulnerability would be an attacker causing large-scale interference on the 1090 MHz channel without sending on the target frequency, but on the 1030 MHz interrogation frequency instead. Interrogations are currently limited to a maximum of 250 per second [16], but these restrictions are placed on the interrogators, not on the Mode S transponders in aircraft. TCAS would then struggle to operate in a timely fashion given the noise created by answers from surrounding aircraft.

FIGURE 2: TCAS ALERT REGIONS (SIMPLIFIED)



TCAS is also an example of where the interaction of insecure systems produces concerning results. TCAS II, the most modern version, has an optional capability for hybrid surveillance in which ADS-B data from nearby aircraft is used to judge whether intrusions are likely and thus whether a given aircraft should be monitored. The system reduces the number of interrogations required for TCAS without a loss to safety [17]. However, as discussed above, ADS-B faces a number of security challenges that affect the trustworthiness of the data it reports. Thus, attacks on ADS-B could also affect safety systems such as TCAS.

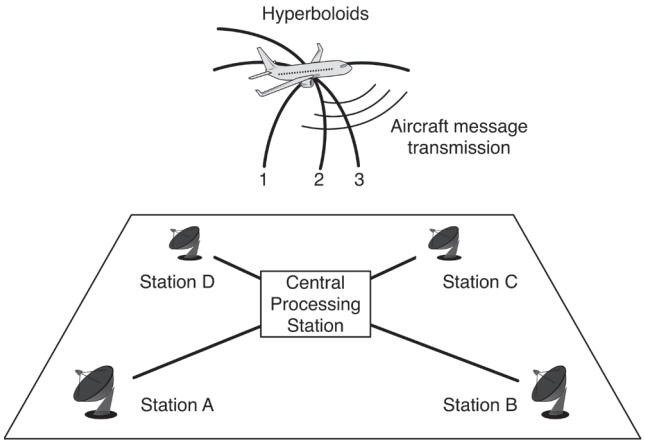
Whilst TCAS is vulnerable due to its design and technologies used, the implications of launching an attack on TCAS are extremely serious. In the best case, ATC may be unable to manage airspace, or aircraft may have a near miss. Jamming the channel or injecting wrong data, however, could cause mid-air collision. As such, we consider that a threat agent who chooses to launch attacks on TCAS would require the motive to cause loss of life or severe disruption, placing it in the domains of nation state and cyber terrorism. However, due to the

lack of control one would have in attacking TCAS, we consider cyber terrorists as the likely threat agent.

3. Multilateration

ADS-B is referred to as 'dependent' due to its dependence on the aircraft in reporting its own measurements such as location and speed. Multilateration provides an alternative method of measuring location and speed without relying on the information reported by the aircraft. Instead, it just relies on receiving a signal from the aircraft, and the Time Difference of Arrival (TDoA) is measured at a number of receivers and a central processing station calculates the transmitter position within a margin of error (see Figure 3).

FIGURE 3: TDoA MULTILATERATION – THE INTERSECTION OF HYPERBOLOIDS 1-3 CALCULATED FROM THE FOUR RECEIVERS A-D REVEALS WHERE THE SIGNAL ORIGINATED



Wide Area Multilateration (WAM) is particularly useful for ATC since it allows location estimation of an aircraft using 1090 MHz messages over large areas. WAM, combined with ADS-B, will form a key part of the next generation surveillance technologies [18] and can help to detect unusual ADS-B reports.

WAM does have a number of challenges of its own, mostly in operation [19]. Due to the number of sensors and data processing equipment required to cover large areas, the cost of installation is very high. As one of the main drivers for ADS-B surveillance is its low cost, this is at odds with WAM.

Due to the inherent redundancy of WAM, attacks would be very costly and resource intensive, which likely makes them possible only for nation states (see Table 3). To spoof an aircraft, one would need to be able to spoof to any receivers in range with perfect timing, and the set of receivers will change as the aircraft moves. This makes WAM very hard to attack, and we consider it to only be in reach of nation states or similarly capable actors.

Table 3 summarises the capabilities of the different threat agents and the surveillance systems that are of interest to them, further estimating the possible cost of the required hardware.

TABLE 3: OVERVIEW OF ATTACKER CAPABILITIES

Threat Agent	Capabilities	Hardware / Cost	Systems of Interest
Passive Observers	Eavesdropping, use of website & mobile apps.	Internet access, $10 SDR receiver stick	ADS-B, Mode S
Script Kiddie / Hobbyist	Eavesdropping, replay attacks, denial of service.	COTS SDR transmitter, $300-$2,000.	ADS-B, Mode S
Cyber Crime	Resources for large-scale operations with sophisticated transponders.	Directional antennas, small UAVs with SDR transmitters, $5,000-$10,000.	ADS-B, Mode S
Cyber Terrorism	Resources for specific high-impact operations, though usually on a limited scale	As with cyber crime but potentially on a smaller, more targeted scale.	ADS-B, TCAS, Mode S
Nation State	Anything physically and computationally possible.	Military-grade radio equipment, capability for electronic warfare.	Any ATC system

5. REASONS FOR THE CURRENT STATE OF WIRELESS SECURITY IN AVIATION

After providing an exemplary overview of wireless security in aviation with our case study, we investigate the underlying reasons of how the current situation came to be. We identify five causes that have led to the apparent lack of communications security within the air traffic system, and which explain the difficulties in fixing it quickly.

A. Long development and certification cycles

The development and certification cycles for new technologies in aviation are typically up to two decades. Taking ADS-B as our running example, the development of its current form started in the late 1990s. The widespread rollout and mandatory use will however only be completed by 2020 in the most advanced airspace. This slow and cautious approach reflects the safety-focused thinking within the aviation community, where a multitude of tests and certifications are required before giving a technology the green light. Unfortunately, while this approach is extremely effective in reducing technical failures, it does not take into account the increased adversarial potential and shifting threat model created by the recent advances in wireless technologies discussed in Section 2.

B. Legacy and compatibility requirements

As a truly global and interconnected system, civil aviation requires technical protocols and procedures that are understood as widely as possible. New protocols and technical advances are not introduced in all airspace at the same time, but depend on local authorities and available infrastructure. It follows that older technologies are kept in service not only for backup reasons, but also to offer the largest compatibility for air traffic control all over the world.

C. Cost pressures

Tying into the previous point, the aviation industry is famously competitive and under major cost pressures [20]. Changes to existing aircraft equipment are expensive and thus unpopular unless they provide immediate cost or operational benefits to the aircraft operators who foot the bill for the installation of new technologies. Apart from these two main drivers, fundamental equipment changes happen primarily through regulatory directives, which are often subject to long lead times and struggle with extensive industry lobbying. As a compromise, legacy technologies are sometimes overhauled to save costs. An example for this is the ADS-B protocol developed in the 1990s, which relies on the old Mode S technology instead of using a new data link (such as the Universal Access Transceiver, or UAT) that was developed from the bottom up.

D. Frequency overuse

As shown in [12] and [21], some of the ATC frequencies such as the 1090 MHz channel are severely congested. An ever-increasing number of aircraft share the same frequencies, exacerbated by UAV set to enter the controlled airspace in the near future. As a consequence, existing ATC protocols suffer from severe message loss, inhibiting potential cryptography-based security solutions at the same time.

E. Preference for open systems

There is a case for air traffic communication protocols to be open to every user; while authentication would be highly desirable, confidentiality through encryption of the content would not. Despite the associated security and privacy problems, the International Civil Aviation Organisation (ICAO) plans for future protocols to be openly accessible. This approach is supposed to fulfil typical aviation requirements such as ease of communication, compatibility, and dealing with administrative differences across countries and airspace [22]. While we acknowledge that open systems are a requirement for the effectiveness of air traffic control for the foreseeable future, it is crucial to start considering and mitigating the downsides, which are rapidly increasing due to previously discussed technological changes.

A further complication for the use of cryptographic means to secure air traffic communication is the inherent complexity of public key infrastructures (PKI). While there are military equivalents to civil SSR in use and under development (STANAG 4193 / Mode 5), due to obvious secrecy requirements, very few details are publicly available. The main problem for a PKI to solve is key distribution and management, [10], which is comparatively easy in closed military environments but very difficult in the open and worldwide system of civil aviation, also tying into the point on compatibility requirements.

A PKI shared by all countries in the world (presumably through ICAO and national agencies) is a monumental task for which no proper suggestions yet exist, and the creation of entirely new protocols is certainly required. The 112 bit message size of ADS-B is too small even for today's computing capabilities, let alone future capabilities; keys would be broken in seconds [10]. While certainly not impossible, experiences with the Internet have also shown that PKI certificate breaches are very common, leaving us with no great solution to the problem.

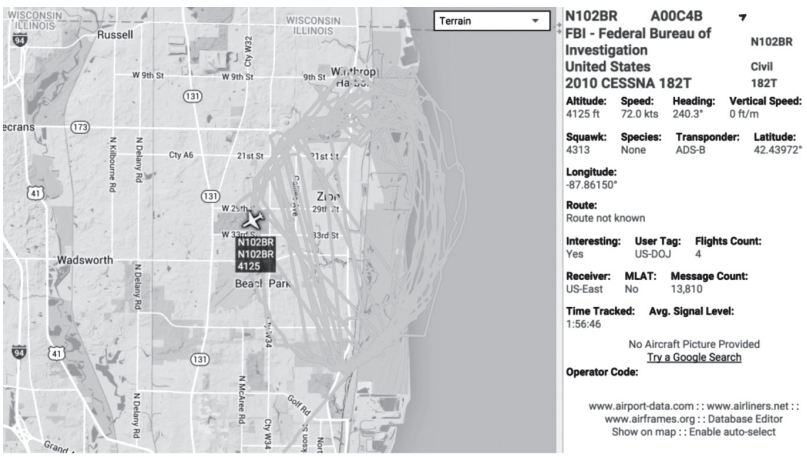
6. AVIATION COMMUNICATIONS SECURITY AS A NEW CYBER POWER ISSUE

Open systems and insecure wireless technologies raise concerns that go beyond active attacks on critical infrastructures: powerful actors increasingly lose their informational edge and privacy as aircraft information becomes available widely and easily on the Internet. We postulate that the democratisation of information has led to a partial erosion of power for state actors, as airborne missions become known immediately to even passive observers.

Traditional 'offline' solutions to maintaining privacy and secrecy for aircraft such as the ASDI scheme [23], which prevents the public display of aircraft movements, have become long obsolete in the SDR era. Plane-spotters around the world detect anomalies, potential incidents, and 'interesting aircraft' practically immediately, and on a large scale, a capability previously limited to state actors. Social media accounts tracking emergency broadcasts provide instant news coverage for both the press and interested individuals, much to the chagrin of some in the traditionally closed aviation community. Hijacked airplanes, too, are detected easily by individuals at home and shared in real-time over Twitter while the aircraft is still in the air [24].

The same effect can be observed for intelligence and security services. With increasing automation and availability of online aviation feeds, the development has gone from occasional sightings of aircraft operated by domestic security services to the large-scale and immediate detection of all transponder-equipped aircraft. An example of the implications of this technological shift is the recent uncovering of a large number of surveillance aircraft employed through front companies of the FBI, an operation that had previously gone unnoticed for some decades [25]. While some of the largest online flight tracking services such as FlightRadar24 comply with requests to not display private or sensitive aircraft data, there are many unregulated sources available that clearly identify such aircraft as interesting to the public (see Figure 4).

FIGURE 4: TRACKING A DOMESTIC SURVEILLANCE AIRCRAFT ON ADSBEXCHANGE.COM

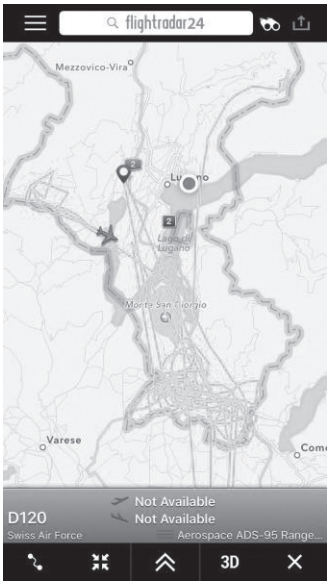


In military settings, this type of open surveillance using data gleaned from Mode S and ADS-B broadcasts has led to similar information leakage through the intentional or unintentional use of transponders during active missions. The diligent tracking of recent airborne engagements in Syria by NATO and Russian aircraft illustrate this point [26]. As airstrikes and reconnaissance missions can easily be detected and anticipated, potentially sensitive strategic and operational information is broadcasted, and deniability of airborne actions becomes difficult; the impact of insecure civil aviation protocols on military users is growing.

The advance of UAVs might offset some or all of this loss of power, as manned missions are replaced with more covert drones. However, in non-military settings, the same problems that are causing concern for current manned surveillance aircraft also apply to UAVs. As aviation authorities are expected to maintain a similar standard of rules for drones in civil airspace, the mandatory use of ADS-B transponders will retain the broadcasts of sensitive data to anyone who is listening.

As an example, Swiss military drones are forced to fly with their ADS-B transponders on when they perform surveillance missions searching for criminals and border breaches [27]. Human traffickers and smugglers can easily track their positions using their smartphones, and avoid discovery by moving only when the drones are not operating.

FIGURE 5: TRACKING BORDER SURVEILLANCE UAV IN REAL TIME USING A MOBILE APP [27]



These examples illustrate the impact that merely passive threat agents have currently. Active attacks on wireless air traffic communication protocols, such as the possibilities discussed in Section 4, could have much greater effects on critical infrastructures in the future.

7. RELATED WORK

Many critical infrastructure industries besides aviation have to adapt to a shifting threat model caused by the rapid advance of technology. We briefly discuss some of the work related to ours in this section.

In the area of transport infrastructure, recent work has shown that current cars use weak authentication and often offer no integrity mechanisms for their on-board systems. Koscher et al. [28] demonstrated this on car data networks even as attempts at using security were being made. This is a dramatic shift whereby cars are now attackable via computer systems, with which the automobile industry has not yet dealt. When scaled up to public transport such as trains, we see the inclusion of industrial control systems (ICS). As demonstrated by Igure et al. [29], the rise of conventional networking technology in ICS without proper security has led to a range of new challenges. Typically, these are similar to those faced in aviation and automotive, such as a lack of authentication or integrity of data networks. Unlike aviation, however, the Repository of Industrial Security Incidents database [30] indicates that attacks on these systems are already occurring. This indicates that, given the opportunity, attackers will exploit these vulnerabilities.

As the use of COTS technologies increases in aviation, scenarios such as those seen in ICS become more common. This has led to a number of works addressing aviation security at a conceptual level. For example, McParland [31] discusses how cryptography can help in protecting the Aeronautical Telecommunications Network (ATN) and some of its applications. Stephens [32] provides a range of security methods and primitives used in typical networking scenarios that could be relevant to aviation. More recently, Li et al. [33] propose a security architecture for next generation communications in air traffic control (ATC). It presents a defence-in-depth approach, and extends to navigation and surveillance at a conceptual level, but does not deal with specific systems.

Within the wireless security community, much work has been done on ADS-B, as it provides a popular example of changing threat models rendering next generation systems insecure. Schäfer et al. [8] experimentally test wireless attacks on ADS-B integrity and availability, analysing the power, timing and range constraints in the real world. Strohmeier et al. [12] assess ADS-B as a system including the intended use, current deployment status, and analysis of the channel characteristics. It also analyses the security issues such as ghost aircraft injection at a high level and comprehensively discusses potential security measures for the future.

To the best of our knowledge, ours is the first work to introduce a threat agent model for modern aviation, and to analyse the impact on the cyber power of nation state actors by novel wireless security threats to air traffic communication.

8. DISCUSSION AND CONCLUSION

In this article, we outlined how technological advances change security threat models in aviation and influence the current cyber power balance. We developed a taxonomy of different threat agents able to affect the cyber-physical aviation system. We postulate that the evolution of cyber power of these agents in the present and in the expected future is an important aspect of future cyber conflicts. Advances in wireless technology and increased digitalisation and automation in aviation enable simpler attacks with few resources. This trend moves power away from nation states towards cyber criminals and terrorists, and even unorganised hobbyists or passive observers.

If nation state actors want to restore the previous balance of power, and increase the security of the aviation system, awareness of cyber security issues among aviation circles and governments is a key factor. Only by raising awareness can the necessary research and development happen, enabling the responsible bodies to address the problem, and prevent the exploitation of existing vulnerabilities in the future.

Considering the decades-long development and certification cycles, research on protocols that include security by design is required as quickly as possible even though it will only pay in the long-term. Existing examples of security designs and analyses for the ADS-B protocol (see, e.g., [34]) can inform the directions of such future research.

New protocols can also provide improvements for the issues of aviation privacy and secrecy. With proper design and implementation of pseudonymous identifiers, most of the relevant information leakage could be reduced to the level of previous, non-technologically enhanced, plane-spotting days, particularly concerning military, government, and private aviation.

Finally, we argue that top-down regulations are crucial in an industry such as aviation that is very cost-conscious and where actions are often taken only when required by regulators. Tying in with the previous point about awareness, the authorities need to be put in a knowledgeable position to issue the necessary regulations, and they should further consider the effect of their actions – or inaction – on the future balance of cyber power.

REFERENCES

[1] M. Strohmeier, M. Schafer, V. Lenders, and I. Martinovic, "Realities and challenges of nextgen air traffic management: the case of ADS-B," *IEEE Commun. Mag*., vol. 52, no. 5, pp. 111–118, 2014.

[2] Department of the Army, "FM 3-38: Cyber Electromagnetic Activities," *F. Man*., no. 1, p. 96, 2014.

[3] A. Costin and A. Francillon, "Ghost is in the Air(traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices," in *Black Hat USA*, 2012.

[4] "GNU Radio," 2016. [Online]. Available: https://gnuradio.org. [Accessed: 12-Apr-2016].

[5] D. Adamy, *Introduction to electronic warfare modelling and simulation*. SciTech Publishing, 2006.

[6] N. Foster, "gr-air-modes GitHub Repository," 2015. [Online]. Available: https://github.com/bistromath/gr-air-modes. [Accessed: 12-Apr-2016].

[7] J. Croft, "Forensic Mining With ADS-B," *Aviation Week & Space Technology*, 2015. [Online]. Available: http://aviationweek.com/commercial-aviation/forensic-mining-ads-b. [Accessed: 12-Apr-2016].

[8] M. Schäfer, V. Lenders, and I. Martinovic, “Experimental analysis of attacks on next generation air traffic communication,” in *Applied Cryptography and Network Security*, pp. 253–271, 2013.
[9] K. Stouffer, J. Falco, and K. Scarfone, “Guide to Industrial Control Systems (ICS) Security,” *Recomm. Natl. Inst. Stand. Technol*., no. SP 800–82, pp. 1–157, 2007.
[10] M. Strohmeier, V. Lenders, and I. Martinovic, “On the Security of the Automatic Dependent Surveillance-Broadcast Protocol,” *IEEE Surv. Tutorials*, vol. 17, no. 2, pp. 1066 – 1087, 2015.
[11] M. Strohmeier, M. Schäfer, R. Pinheiro, V. Lenders, and I. Martinovic, “On Perception and Reality in Wireless Air Traffic Communications Security.” 2016.
[12] M. Strohmeier, M. Schäfer, V. Lenders, and I. Martinovic, “Realities and challenges of NextGen air traffic management: the case of ADS-B,” *IEEE Commun. Mag*., vol. 52, no. 5, 2014.
[13] Federal Aviation Administration, “ADS-B Frequently Asked Questions,” 2015. [Online]. Available: https://www.faa.gov/nextgen/programs/adsb/faq/. [Accessed: 12-Apr-2016].
[14] “dump1090 GitHub repository,” 2016. [Online]. Available: https://github.com/antirez/dump1090. [Accessed: 26-Dec-2015].
[15] The European Commission, *Commission regulation laying down common airspace usage requirements and operating procedures for airborne collision avoidance*, no. 1332. European Union, 2011, pp. 2008–2010.
[16] Aeronautical Surveillance Panel, “Draft Doc9924 guidance material for the measurement of all-call reply rates,” International Civil Aviation Organisation, 2013.
[17] S. Henely, “Traffic Alert and Collision Avoidance System II (TCAS II),” in *Digital Avionics Handbook*, 3rd ed., C. R. Spitzer, U. Ferrell, and T. Ferrell, Eds. CRC Press, pp. 1–9, 2015.
[18] International Civil Aviation Organisation, “Initial capability for ground surveillance,” in *Global Air Navigation Plan* 2013-20282, 2013, p. 56.
[19] G. Galati, M. Leonardi, P. Magarò, and V. Paciucci, “Wide area surveillance using SSR Mode S multilateration: advantages and limitations,” *Eur. Radar Conf*., pp. 225–229, 2005.
[20] M. Franke, “Competition between network carriers and low-cost carriers—retreat battle or breakthrough to a new level of efficiency?,” *J. Air Transp. Manag*., vol. 10, no. 1, pp. 15–21, 2004.
[21] Eurocontrol, “Updated work on 5 - Final report on electromagnetic environmental effects of, and on, ACAS,” Aug. 2009.
[22] International Civil Aviation Organisation, “Review report of the thirteenth meeting of Automatic Dependent Surveillance-Broadcast (ADS-B) study and implementation task force.” Beijing, 2014.
[23] National Business Aviation Administration, “Blocking display of Aircraft Situation Display to Industry (ASDI) data,” 2016. [Online]. Available: https://www.nbaa.org/ops/security/asdi/. [Accessed: 22-Feb-2016].
[24] J. Walton, “How I broke the Ethiopian Airlines #ET702 hijacking on Twitter,” 2014. [Online]. Available: https://medium.com/@thatjohn/how-i-broke-the-ethiopian-airlines-et702-hijacking-on-twitter-6c2cc1d2f2e4#.pmobgbtqu. [Accessed: 12-Apr-2016].
[25] C. Friedersdorf, “Congress Didn’t Notice the FBI Creating a ‘Small Air Force’ for Surveillance,” *The Atlantic*, 2015. [Online]. Available: http://www.theatlantic.com/politics/archive/2015/06/congress-didnt-notice-the-fbi-creating-a-small-air-force-for-surveillance/395147/. [Accessed: 12-Apr-2016].
[26] D. Cenciotti, “Online flight tracking provides interesting details about Russian air bridge to Syria,” *The Aviationist*, 2015. [Online]. Available: http://theaviationist.com/2015/09/11/ads-b-exposes-russian-air-bridge-to-syria/. [Accessed: 12-Apr-2016].
[27] “App zeigt Kontroll-Flug von Armeedrohne,” *20 Minuten*, 2015. [Online]. Available: http://www.20min.ch/schweiz/news/story/App-zeigt-Kontroll-Flug-von-Armeedrohne-27294424. [Accessed: 12-Apr-2016].
[28] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, “Experimental security analysis of a modern automobile,” 2*010 IEEE Symp. Secur. Priv*., pp. 447–462, 2010.
[29] V. M. Igure, S. A. Laughter, and R. D. Williams, “Security issues in SCADA networks,” *Comput. Secur*., vol. 25, no. 7, pp. 498–506, 2006.
[30] Exida LLC, “Repository of Industrial Security Incidents (RISI) Online Incident Database,” 2015. [Online]. Available: http://www.risidata.com/Database. [Accessed: 12-Apr-2016].
[31] T. McParland and V. Patel, “Securing air-ground communications,” in *20th Digital Avionics Systems Conference,* 2001, pp. 1–9.
[32] B. Stephens, “Security architecture for aeronautical networks,” in *23rd Digital Avionics Systems Conference*, 2004, vol. 2.
[33] W. (Wenhua) Li and P. Kamal, “Integrated aviation security for defense-in-depth of next generation air transportation system,” *2011 IEEE Int. Conf. Technol. Homel. Secur*., pp. 136–142, 2011.

[34] C. Finke, J. Butts, R. Mills, and M. Grimaila, “Enhancing the security of aircraft surveillance in the next generation air traffic control system,” *Int. J. Crit. Infrastruct. Prot.*, vol. 6, no. 1, pp. 3–11, Mar. 2013.
[35] J. Carney, “Is Spying on Corporate Jets Insider Trading?,” *CNBC*, 2012. [Online]. Available: http://www.cnbc.com/id/100272132. [Accessed: 12-Feb-2016].