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

UAV Exploitation: A New Domain for Cyber Power

Kim Hartmann
Otto von Guericke University
Magdeburg, Germany
kim.hartmann@ovgu.de

Keir Giles
Conflict Studies Research Centre
Oxford, UK
keir.giles@conflictstudies.org.uk

Abstract: The risks of military unmanned aerial vehicles (UAVs) being subjected to electronic attack are well recognised, especially following high-profile incidents such as the interception of unencrypted video feeds from UAVs in Iraq and Israel, or the diversion and downing of a UAV in Iran. Protection of military UAV assets rightly focuses on defence against sophisticated cyber penetration or electronic attack, including data link intercepts and navigational spoofing. Offensive activity to counter adversary drone operations presumes a requirement for high-end electronic attack systems. However, combat operations in eastern Ukraine in 2014-16 have introduced an entirely new dimension to UAV and counter-UAV operations. In addition to drones with military-grade standards of electronic defence and encryption, a large number of civilian or amateur UAVs are in operation in the conflict. This presents both opportunities and challenges to future operations combating hybrid threats. Actual operations in eastern Ukraine, in combination with studies of potential criminal or terrorist use of UAV technologies, provide indicators for a range of aspects of UAV use in future conflict. However, apart from the direct link to military usage, UAVs are rapidly approaching ubiquity with a wide range of applications reaching from entertainment purposes to border patrol, surveillance, and research, which imposes an indirect security and safety threat. Issues associated with the unguarded use of drones by the general public range from potentially highly dangerous situations such as failing to avoid controlled airspace, to privacy violations. Specific questions include attribution of UAV activities to the individuals actually directing the drone; technical countermeasures against hacking, interception or electronic attack; and options for controlling and directing adversary UAVs. Lack of attribution and security measures protecting civilian UAVs against electronic attack, hacking or hijacking, with the consequent likelihood of unauthorised use or interception, greatly increases the complication of each of these concerns.

Keywords: *drone, UAV, military, communications*

1. INTRODUCTION

As cyberspace has emerged from being a purely computer based virtual reality to bringing about real life impacts, cyber power has become a vital element of hostile action between states, now including military operations. Cyber power is thus no longer a virtual competence. This paper will discuss a field of activity where cyber power has a direct and immediate effect on the conduct of real-world operations, both civilian and military: the use and exploitation of unmanned aerial vehicles (UAVs).

There has been substantial discussion on the issues associated with UAV use in military operations, especially on the ethical aspects of drone strikes [1]. But the specific issue of UAV security has gained broader public attention due to the use of UAVs in non-military activities.

UAVs are rapidly approaching ubiquity, with a growing range of applications. The benefits of utilising UAVs for inexpensive aerial surveillance and survey have been widely accepted. However, with the broader introduction of UAVs to the civilian market for law enforcement, research and entertainment purposes, a new set of security and safety threats have been unwittingly invited. Specific questions currently unresolved include attribution of UAV activities to the individuals actually directing the drone; technical countermeasures against hacking, interception or electronic attack; countermeasures against UAVs which have already been compromised; and options for controlling and directing adversary or hostile UAVs.

Issues associated with the unguarded use of UAVs by the general public range from potentially highly dangerous situations such as failing to avoid controlled airspace, to privacy violations. The lack of security protecting civilian UAVs against electronic attack, hacking, or hijacking, with the consequent likelihood of unauthorised use or interception, greatly increases the complication of each of these concerns. The increased likelihood of hijacking or interception fosters the risk of abusive and dangerous use by cyber attackers, and complicates the attribution issue. The implications are directly relevant to the full range of UAV operations, from use in state-on-state conflict through civilian and law enforcement applications, to simple entertainment use.

This paper explores the use and exploitation of UAVs as a means of implementing cyber power for real-world effects. It discusses why UAVs are targets for cyber actors; how these actors may use UAVs in combat and civilian scenarios; and examples of how UAVs have been exploited in the past through cyber means. It highlights that cyber power as exercised against UAVs demonstrates how cyber competence may be linked to the success or failure of real life combat missions. The paper is written as an aide to policy-makers; an essential technical overview of the range of possible cyber attacks on UAVs is therefore included, but detailed analysis of attacks is not. Instead, the paper aims to provide an introduction to the range of policy implications of the current state of development of UAV security, based on implementation (or lack of it) to date.

2. UAV PAST INCIDENTS

Electronic attacks on UAVs are not new; but while earlier attacks were relatively rare, fairly sophisticated, and directed against military devices due to their tactical, strategic and monetary value, more recently a series of incidents against and/or involving civilian drones have been reported. The latter reflects the recently gained popularity of UAVs for recreational uses, and the resulting potential for abuse. It will be observed that many of these incidents were only possible due to massive flaws in the implementation of security measures, if these measures were implemented at all.

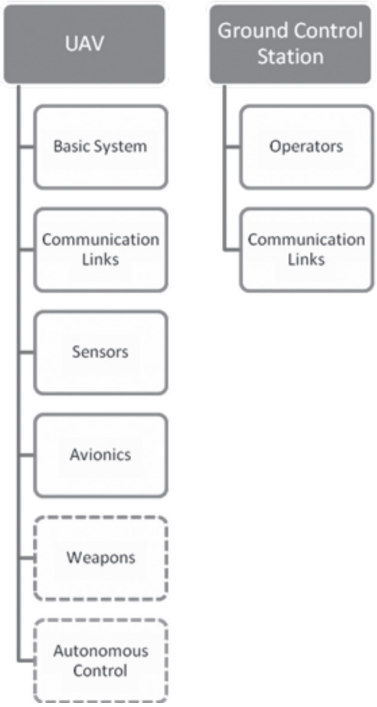
A. Preliminaries

UAVs, even at the hobby level, are increasingly complex aerial vehicles. While the majority of those available for civilian use at present are intended for short-range use under the continuous control of an operator within line of sight, autonomous UAVs with pre-programmed missions or behaviours are beginning to penetrate the civilian market, despite legal and regulatory challenges. It should be noted that the concerns stated in this paper apply equally to both of these sub-types of UAV.

UAVs are used in a variety of applications ranging from military operations such as intelligence, surveillance, target acquisition and reconnaissance (ISTAR), to civilian applications such as border control, monitoring, law enforcement, search and rescue, journalism, transportation, recreational uses, and many more. Throughout 2015-16, media reporting has routinely described new uses for UAVs where they provide significant enhancements to situational awareness or research in civilian uses; such as, to take just one example, assisting in an air accident investigation in February 2016 [2].

All of these purposes demand that UAVs are highly sensor-driven assets. It follows directly that UAVs are highly dependent on functioning sensors, and on receiving correct data from their operators and surrounding environments [3]. This dependence on real-time input, both through communication links and on-board systems, provides a wide range of vulnerabilities, following the general security guideline that any input signal to a system may be exploited to cause its malfunction [4] .

FIGURE 1: UAV COMPONENTS AND INFORMATION FLOW, FOLLOWING [3]



Before exploring past UAV incidents, a general view of UAVs from the point of view of an attacker is given in Figure 1. The UAV itself consists of a 'Basic System', being analogous to an operating system but designed to be less user-centred. This unit is connected to other components of the UAV and/or to its ground station and operator through a system of communications links, which may include any type of communication means available for interaction. A set of sensors is also available, varying according to the type of UAV. Loosely speaking, UAVs designed for purely recreational purposes are likely to have a smaller and less sophisticated set of sensors. Another entity inherent to UAVs is the avionics unit, a set of hard- and software components crucial for controlled flight. The 'autonomous' and 'weapons' systems are most likely to be found in modern military assets. While the autonomous operations system is of course security relevant in terms of vulnerability detection, the 'weapons' system is rather considered an effect carrier than a security threat. Weapons may make a UAV a more valuable target to an attacker; however, weapons are not generally considered typical targets for exploits.

For non-autonomous UAVs, the ground station and operator must also be considered. Communications links may correspond to continuous data link connections, partly-continuous connections (such as WiFi and Bluetooth, which are available upon request and within a limited range) and discrete connections which are only possible with direct access to the hardware,

such as data uploads by USB, CD-ROM, or DVD. Not considered in this article but noteworthy is that the operator himself may impose a security threat through social engineering [5].

B. Implications

In 2010, the US Federal Aviation Administration (FAA) estimated that 15,000 UAVs would be in operation in the US by 2020. In fact, by mid-2015 UAV sales there were already exceeding 15,000 each month [6]. Potentially dangerous UAV encounters by commercial airline pilots in the vicinity of airports in the US have increased accordingly. In 2014, there were 238 such reports. In 2015, the total was 650 in the first seven months [7]. It can reasonably be expected that as UAV markets develop worldwide, similar problems will be replicated elsewhere.

Users may consider that very lightweight drones cannot cause serious damage or danger, but incidents with this class of drone reported in late 2015 range from the trivial [8], through the potentially dangerous and definitely expensive [9], to the horrifying [10]. Sales predictions of up to a million small UAVs purchased for Christmas 2015 in the US raised the alarming prospect of an uncontrollable number of airborne vehicles in the hands of consumers and hobbyists with little grasp of the potential hazards of small UAV operations [11]. This prompted the FAA to rush through regulations on the use and registration of small UAVs, to be discussed below.

The explosion in UAV ownership has outstripped study of its implications, leading to a deficit of reliable studies on the actual danger, and in particular on the implications for a manned aircraft of a collision or engine strike [12]. But even within this knowledge deficit, UAV vulnerability to cyber and electronic attack stands out for an alarming degree of consumer and regulator ignorance [13]. This paper aims to assist in addressing this knowledge gap.

C. Past incidents

A series of successful cyber attacks on UAVs have been reported in recent years. Some of these were performed by researchers under laboratory conditions, while other incidents occurred ‘in the wild’. The following list is not exhaustive, and is intended only to provide evidence of the described vulnerabilities of UAVs to attack.

That UAVs may be potentially vulnerable targets in military operations has been globally acknowledged since the loss of a US RQ-170 Sentinel UAV in Iran in 2011. This incident, explored further below, called into question the US’s cyber competency, and has been frequently cited in arguments against UAV use to highlight their lack of controllability in military scenarios.

This specific incident may constitute the earliest UAV attack which led directly to public questioning of a nation’s cyber power. While the exact method by which the RQ-170 was compromised was never publicly confirmed, researchers proved subsequently that it is possible to hijack drones in flight through GPS spoofing [14]. A further relevant report was released in 2015, where members of the Critical Engineering Working Group developed a stratosphere balloon to intercept radio traffic at higher altitudes, including the frequencies used for data links between UAVs and satellites or other UAVs [15].

One line of argument suggests that this kind of attack constitutes electronic warfare (EW), rather than pure cyber attack. However, the authors of this paper consider that producing a hostile effect by introducing compromised data into an operating system meets a reasonable definition of cyber, rather than electronic, attack.

In any case, experience of current combat operations shows that the dividing lines between these different kinds of warfare are becoming increasingly blurred and irrelevant. Furthermore, regardless of the status of debate over the nature of the attack, the wide variety of available attack scenarios is one of the aspects that make UAVs especially vulnerable. From a pragmatic point of view, it does not matter how control of a software or hardware component is lost.

Besides communication links, another exploitable component is the UAVs operating system (OS) or micro-controller units as applicable. The type of OS varies between UAV manufacturers, and prototypes have been developed using smartphones as UAV control systems [16]. Thus, any known exploit in the smartphone's OS also becomes relevant in a UAV context, leading to a broader security and safety threat. It is also noteworthy that many smartphones are already compromised without the users being aware.

In 2013 Hak5 (https://hak5.org/) demonstrated a range of abuses and vulnerabilities of UAVs, including using one as a flying WiFi sniffer [17], [18]. Hak5 also reported on using a DJI Phantom 2 Vision UAV enhanced with a Pineapple WiFi and BatterPack to force Parrot AR.Drones to fly in failsafe mode, causing the AR.Drone to drop out of the sky [19]. This attack was inspired by Samy Kamkar's SkyJack Project [20] which engineers a drone 'to autonomously seek out, hack, and wirelessly take full control over any other Parrot drones [within] wireless or flying distance, creating an army of zombie drones under your control' [21]. The source code of this project is publicly available on GitHub, meaning that anybody with a rudimentary degree of skill can download it for free and run it on their own UAV.

While the examples to date have focused on interfering with data uplinks, information received from UAVs is also vulnerable to interception and exploitation. An in-combat attack intercepting the video stream between a UAV and its ground station was reported by Iraqi forces in 2009 [22]. In 2014, a research fellow student at Texas A&M University conducted a preliminary survey of the possibilities of hacking into a UAV's video stream, and the potential implications. [23]. And in February 2016 media reports based on alleged classified information stolen by Edward Snowden suggested that video feeds from Israeli UAVs had been intercepted by British signals collection installations in Cyprus [24]. But despite uncritical repetition by a wide range of media, these reports did not in fact support the suggestion of highly sophisticated decryption techniques, since the supposed intercepts were from several years earlier and of signal feeds which were unencrypted or used only basic commercial video encryption techniques [25]. Given the rapid pace of development of military UAV technology and the absence of more recent public exploits, it can be assumed that measures to prevent such simple interceptions are now in place.

3. UAVS IN THE UKRAINIAN CONFLICT

As a result of the high-profile incidents outlined above, in particular the interception of video feeds from a US UAV in Iraq [26] and the diversion and downing of another US UAV in Iran [27], the risks of military UAVs being subjected to electronic attack are well recognised. Protection of military UAV assets rightly focuses on defence against sophisticated cyber penetration or electronic attack, including data link intercepts and navigational spoofing. Offensive activity to counter adversary drone operations presumes a requirement for high-end electronic attack systems. Security in this field is in ongoing development: a US programme known as High-Assurance Cyber Military Systems (HACMS) aims to build cyber resilience for a wide range of applications including UAVs, specifically 'to create technology for the construction of high-assurance cyber-physical systems' [28].

But combat operations in eastern Ukraine in 2014-16 introduced an entirely new dimension to UAV and counter-UAV operations. In addition to drones with military-grade standards of electronic defence and encryption, a large number of civilian or amateur UAVs are in operation in the conflict. Both the Russian-backed separatists and the Ukrainian Armed Forces (VSU) have attempted to introduce UAV capabilities by using commercial civilian or home-built drones with varying degrees of modification [29].

UAVs are seeing extensive use in combat in a number of current conflicts, including in Syria, Iraq, Libya and Yemen, but the Ukrainian conflict represents the most significant use of UAVs in warfare by two opposing sides that has been documented to date. Actual operations there, in combination with studies of potential criminal or terrorist use of UAV technologies [30], provide indicators for a range of aspects of UAV use in future warfare. In addition, due in part to the vulnerabilities described in this paper, they also provide a case study of the interfaces between cyber, electronic warfare, and kinetic responses. According to one analysis, combat operations in Eastern Ukraine are 'a living lesson in how quickly war changes technology, and vice versa' [31].

These developments are being closely observed by major military UAV users. In the US view, eastern Ukraine presents 'an emerging laboratory for future 21st-century warfare' [32]. NATO too has emphasised the importance for future warfighting capability both of unmanned systems and of retaining freedom of action in the electromagnetic spectrum despite adversary capabilities [33]. It is in this respect that cyber or electronic attack on UAVs may constitute one of the most direct and immediate ways of implementing cyber power to achieve an immediate real-world effect. Close observers of Russian operations in Ukraine have noted that this effect is brought about through 'not just cyber, not just electronic warfare, not just intelligence, but […] really effective integration of all these capabilities with kinetic measures' [34].

A. Civilian UAVs

In Ukraine as elsewhere, among a wide range of uses for enhancing situational awareness on the battlefield, obtaining real-time imagery with UAVs greatly improves the accuracy and effectiveness of missile and artillery attacks. The advances in artillery effectiveness are similar

to those brought about by the use of spotters in balloons and then aircraft in the late 19th and early 20th centuries. But the irony is that in the highly sophisticated electronic warfare environment of eastern Ukraine, some of the most effective capability increments for the Ukrainian forces have been relatively inexpensive off-the-shelf consumer drones.

At the beginning of the conflict, Ukraine's military UAV stocks were mostly limited to 1970s-era Tupolev designs, limited in capability, expensive to operate, and vulnerable to attack from ground and air [35]. A number of these were indeed shot down or otherwise destroyed, although much early reporting of UAV use in the Ukraine conflict, particularly referring to US drones, was in fact disinformation [36]. In response, during 2014 programmes like the Aerorozvidka (air reconnaissance) project began to crowdfund the acquisition of UAVs for the volunteer units augmenting the VSU [37].

Many of these were off-the-shelf DJI Phantom UAVs modified for extended range and to carry Sony A-7 video cameras. The cost of acquiring and modifying each UAV was reported as being about $2,300, and the time expended in modifying and testing them followed by user training as less than a week. This compares with a reported cost of approximately $250,000 for a complete implementation package for a comparable military UAV, the US RQ-11 Raven, of which the cost of the UAV itself is approximately $30,000 [37].

However, civilian UAVs have much lower standards of protection against hostile actions. These commercial and 'entertainment' drones generally do not have intrusion detection or security mechanisms present or activated, and can be far more easily hijacked or disrupted. Unless pre-programmed for autonomous operations, small UAVs are unable to fly stealthily. Their data links, as well as being vulnerable to jamming and to cyber attacks seeking to compromise the data in order to control the UAV, broadcast continuous electromagnetic signatures that enable their detection, location and classification, as well as giving away the location of the operators. Ukrainian UAV operators have suffered casualties after being located by Russian communications intelligence operators, and targeted for mortar fire. Precautions now include frequent relocation, positioning antennas remotely, and operating from within cover [31]. The operators swiftly learned that launching from the same location more than once 'guaranteed' mortar or sniper attack [38].

Russian countermeasures thus rapidly neutralised the tactical advantage gained by Ukraine's modified civilian UAVs in late 2014. Electronic attack took the form both of GPS spoofing (feeding the UAV false information on the frequencies used to acquire satellite location data), and straightforward white noise broadcasting on the UAV's control frequency in an attempt to crash it [39]. Russia and the Russian-backed militias made use of their access to highly sophisticated and effective electronic attack technology [31]. The mismatch of resources between high-end Russian military technology and Ukrainian off-the-shelf stopgaps is stark: according to one Ukrainian UAV expert, 'They [Russia] have $7 million systems to jam drones that cost thousands of dollars' [38].

Among further planned modifications, Ukrainian software engineers began working on capability suites to militarise UAV functions, including get-you-home navigation systems for

use when GPS signals are jammed [38]. Faced with potential Russian UAV air supremacy, Ukrainian forces also requested assistance from abroad in the form of electronic countermeasures (ECM) equipment to neutralise Russian UAVs in response [40]. Monitors for the Organisation for Security and Cooperation in Europe (OSCE) also found their Schiebel S-100 Camcopter UAVs targeted by Russian-backed separatists. Attempts to shoot the OSCE UAVs down with gunfire and missiles were largely ineffective, but electronic attack including GPS jamming and spoofing caused far more serious disruption to operations, including grounding the entire OSCE UAV fleet in November 2014 [35].

There are a range of implications for NATO and other nations from UAV operations in eastern Ukraine. One clear development is that airspace for UAV operations is becoming highly contested, with air superiority considerations extending to drone operations [41]. NATO nations in particular have been led to question their long-held presumption of complete control of the air in conflict. In Ukraine, Russia employs 'tiered, multileveled [unmanned aerial systems] of all types' for reconnaissance and targeting – an entirely new challenge for NATO ground forces to deal with [42].

Other US sources note a clear distinction between Russian and US drone use. Whereas the American approach is to undertake prolonged surveillance punctuated by occasional precision strikes, the appearance of Russian UAVs is swiftly followed by intense artillery bombardment. According to Ukrainian troops, 'when they see certain types of UAVs, they know in the next 10-15 minutes, there're going to be rockets landing on top of them' [41]. In addition, Ukrainian reports suggest that Russian UAVs have operated in pairs: one at low level to draw fire, and another higher UAV to observe and provide targeting information on the Ukrainian position doing the shooting.

The UAV campaign in Ukraine has highlighted the display and use of much enhanced electronic warfare capabilities, including not only provision of false GPS data but also a range of other means of electronic attack (EA) [43]. Unofficial reports suggest some of these have already been directed from Russia at US and NATO military units visiting border regions of the Baltic states. If the Russian approach of utilising high-end EW equipment against UAVs is copied, this implies further costly investment in EA equipment which is currently available only in negligible amounts in NATO inventories.

Further afield, lessons from Ukraine can be applicable to any aspect of UAV use. All UAVs combine an array of communications systems and software, each presenting their own vulnerability to attack. These include GPS for location and height determination, digital accelerometers, camera and video suites, data processing and transmission through a variety of channels, flight control, stabilisation, autopilot capability and – for more sophisticated UAVs – pre-programmed semiautonomous operation or mission execution. All of these offer a means by which safe operation can be compromised [44]. Even geofencing software intended to prevent UAVs entering controlled or sensitive airspace, such as that developed by major drone manufacturers DJI, presents vulnerabilities [45]. Owners or adversaries may choose not to install or to disable this software, or to interfere maliciously with code or updates.

4. COUNTERMEASURES

It can be seen that many attacks on UAVs are possible due to a lack of security measures normal in other areas of IT, such as encrypted communication channels, protected software and so on. These technologies have simply not been implemented in the UAV context due to a deficient assessment of UAVs' potential as cyber-attack targets. In this section we will explore some of the ongoing efforts to establish security measures to ensure safer operation of UAVs.

A. Legislative and regulatory initiatives

While the US is undoubtedly the nation with by far the largest number of UAVs in use, it may not be the most advanced in terms of developing regulations for their use. Critiques of the legal position of drone operations highlight the central role of 'a set of rules created 70 years ago based on a chicken farm', a reference to a landmark US legal case in 1946 which determined, based on a unique set of circumstances, that the property of all landowners in the United States extends 83 feet into the air. The ruling remains in effect today [46]. Meanwhile, case law appears to be developing as a result of drones simply being shot down [47].

The significant point for the purpose of this paper is that the FAA regulations on the use and registration of small UAVs, hurriedly introduced at the end of 2015, also indicate the threat perception among US regulatory authorities. In the 211 pages of these regulations and associated commentary, cyber or electronic attack is mentioned only once, in a security proposal from the public that was not implemented. The absence of any response or commentary from the FAA suggests that this aspect of UAV hazard, and the related problem of data compromise through software or signal attack, is not being actively considered in civil operations in the US [48].

It should be emphasised that these are very different regulatory standards than those being developed for professional or military drone operations at higher altitudes and in controlled airspace where, among a range of other measures, standard air transport collision avoidance avionics are to be employed. These include active surveillance and Automatic Dependent Surveillance-Broadcast (ADS-B) to detect aircraft with transponders, TCAS 2 collision-avoidance systems, and on-board radar to detect other aircraft and validate ADS-B [49].

An informed critique of the FAA regulations suggests that a lack of threat perception is was not the only problem with them. It claims the 'interim final rule' has 'lost track of reality, claimed authority it doesn't have, and introduced rules that are destined to fail miserably [...] it is completely unworkable and the moment the FAA tries to enforce the rule, there will be hell to pay' [50].

A similar attitude appears to be held in the UK. At a public discussion in September 2015, representatives of both UK and US air traffic control authorities said that misuse of UAVs ought rightly to be a police issue, but they had been unable to raise police interest in the problem. Since this misuse is not currently a crime, no action can be taken, and consequently there is *de facto* no official concern over malicious use. A representative of the UK's largest airport company, which could expect to be directly affected by UAV misuse, said explicitly that their

concern is with accidental rather than malicious misuse. All representatives confirmed that there had been no consideration of the possibility of UAVs being hacked or hijacked through cyber compromise. The common presumption was that size mattered, but that 'bigger drones equals more risk' – the opposite of the problem in conflict situations [51].

B. Technical countermeasures

A wide range of counter-UAV technologies is rapidly becoming commercially available [52]. The most direct approach to dealing with a hostile UAV remains attempting to shoot it down; but smaller UAVs make exceptionally hard targets, and the problem of collateral damage and of where large amounts of expensive ammunition fired into the air eventually land often makes this approach prohibitive. In addition, as noted above in the context of Ukraine, firing on a UAV immediately reveals your position to other, possibly undetected, surveillance assets and invites counter-fire.

Laser weapons under development avoid the problem of collateral damage, and to some extent detection, but are limited by power consumption and disrupted by dust or fog [53]. Other inventive solutions cover a broad spectrum: 'From the Toyko [sic] police testing a net-deploying UAS to catch drones in flight to the Netherlands police training eagles to snatch quadcopters in midair, the inventiveness of the unmanned aircraft industry is evident in the counter-UAS market' [54]. Nevertheless, at the time of writing, the most promising methods for neutralising UAVs lie in cyber or electronic attack.

Blighter Surveillance Systems, Chess Dynamics, and Enterprise Control Systems of the UK have integrated radar detection, electrooptical and infrared tracking, and radiofrequency jamming to develop countermeasures for small UAVs, evaluated by the US Army in late 2015 [55]. Equipment for detecting and neutralising small UAVs has also been developed by Elta Systems, a subsidiary of Israel Aerospace Industries (IAI). Once a hostile UAV is detected, the systems use electronic attack to shut it down 'by disrupting its command link, navigation system, position location, or situational awareness' [52]. The highly portable Battelle DroneDefender makes use of directed electronic attack to jam GPS and other radio signals to a drone, causing it to land or hover without necessarily destroying it [56]. In many jurisdictions, radio frequency jamming of this kind is illegal; at the time of writing, Battelle has suspended sales and publicity 'while we evaluate the permissible applications of the product under current legislation' [57]. Similarly, recommendations that police forces should be funded for radio frequency jammers and GPS jammers to counter UAVs have to contend with the fact that their use in most countries is currently illegal, for entirely valid safety reasons [58].

In any cyber incident, whether UAV related or not, the question of attribution is fundamental. The issue of attribution in cyberspace is one that has long tormented planners and policymakers, while providing ongoing employment for lawyers. In the context of UAV control, attribution takes on a whole new dimension.

In UAV-related incidents, attribution of who is carrying out an attack is further complicated by a lack of static connections or (usually) of any logging capabilities at the UAV. Where a

UAV itself is used to carry out a physical attack, the attribution of the aggressor is even further complicated by three factors:

- The attacking UAV may not be identified at all (no ID associated with the drone, no logs available);
- The attacking UAV may be identifiable based on hardware components, but cannot be attributed to the person operating it (ID available but not registered, obsolete registration or hijacked UAV, logs only partially accessible or manipulated); and
- The human operator may be identifiable but claim not to have been in control of the drone, which at present is very difficult to prove.

Technologies to counteract these issues are available in other contexts, and their transfer to UAV operations is now under discussion. In September 2015 the EU Parliament considered a resolution to establish the 'safe use of remotely piloted aircraft systems (RPAS), commonly known as unmanned aerial vehicles (UAVs), in the field of civil aviation' [59]. This document calls for means of identifying all UAVs without regard to their size. The document implicitly acknowledges the threat recreational and civilian drones may pose to the public. It explicitly states the need for the installation of 'ID chips' in all UAVs. Furthermore, it recommends compulsory registration for buyers of UAVs throughout the EU.

As noted above, UAV registration has also been announced by the FAA in the United States [60]. A range of technical proposals for practical registration schemes is available [61], but under US regulations, tracking is carried out not by an on-board ID chip, but with a certificate and registration number to be placed on the UAV itself, in the same manner as conventional aircraft. This startlingly unimaginative approach fails to enable electronic enforcement and control methods, and is entirely unhelpful for the installation of automated logging mechanisms.

Another route to easier attribution is under consideration in the UK, which is studying the feasibility of a UAV traffic system where UAV pilots operating below 500 feet are requested to register their routes in an online database to allow tracking and avoid collisions. This attempt raises several questions:

- Usability is questionable as operators are requested to manually enter details of every flight and the exact route taken. Especially in recreational uses, this appears impractical;
- The database itself may present an additional vulnerability, as it is intended to be permanently accessible and easily updated by the public. This opens possibilities for more traditional and unsophisticated cyber attacks against the online database, such as DDoS;
- It raises questions of how the routes entered are to be monitored for correctness and accuracy, and violations addressed;
- It is unclear how false data inserted into the database are to be identified and eradicated; and
- Without a registration system, it is unclear how is the UAV is to be described uniquely within the system.

5. CONCLUSION AND OUTLOOK

Development of UAV operations continues at a startlingly rapid pace. At the time of writing, the following five scenarios belong in the future; but it is entirely possible that one or more of them will already have taken place by the time this paper reaches publication.

- At present, unmanned aircraft operations still assume permissive airspace. No UAVs have yet been announced, even by military programmes, which are able to survive in contested or denied airspace [62]. But some Ukrainian programmes to modify civilian UAVs include plans to fit weapons to them in order to target adversary drones. If this were achieved, it would be the first documented case of UAV-on-UAV warfare, and akin to the very earliest days of aerial combat during the First World War when pilots of unarmed reconnaissance aircraft began to take rifles in the cockpit to take potshots at each other.
- Ukrainian forces repeatedly refer to being 'swarmed' by Russian drones. But in the US, two separate programmes are testing genuine swarming capabilities, where large number of autonomous UAVs act as a mass to overwhelm an adversary's defences. DARPA's Gremlins programme is to trial launching numbers of small UAVs from aircraft to carry out coordinated and distributed operations. The Office of Naval Research's Locust (LowCost UAV Swarming Technology) programme, understandably, envisages launching the swarm of small UAVs from ships [63].
- Mixing manned and unmanned operations will also be on trial. In an approach with some similarities to the concept for manned aircraft with different roles to cooperate and share information using the Talon HATE pod [64], the US Air Force Research Laboratory's 'Loyal Wingman' programme aims to team manned fighters with 'survivable UAVs that collaborate as offboard sensors, jammers and weapons trucks' [65].
- Progress in regulating civilian UAV use is likely to lead to additional sensors and communications devices to avoid restricted airspace and collisions with other aircraft. Autonomous systems small enough to be mounted on micro-UAVs, including implementations of the ADS-B system used on manned aircraft, are already available [66]. Secure failsafe mechanisms can be expected to be built in to UAVs as standard, providing for controlled descent or return to base when ground or GPS communications are lost or when the UAV detects electronic attack. But systems such as these present yet another vulnerability to hostile interference: if their software, data or communications are not adequately protected, then they too are open to cyber or electronic attack.
- Potential future deliberate use of UAVs for terrorist purposes remains a hot topic. In early 2016, a report highlighting the risks led to alarmist headlines in the US and Europe [67], [68]. But even this report focused exclusively on the prospects of terrorist organisations developing their own UAVs, and did not address the potential for cyber hijacking of third party UAVs in order to carry out attacks.

In summary, the rapid development of UAV capabilities is far outstripping concepts and

procedures for ensuring their security. It is commonly repeated that the challenge of ensuring cyber security overall arises largely from the fact that the internet was designed to be fundamentally insecure. By contrast, the current state of development of UAVs presents an opportunity to recognise the problems outlined in this paper, and consequently begin to build in protection against cyber attack as standard.

REFERENCES

[1] Dr Shima Keene. (2015, December) 'Lethal and Legal? The Ethics of Drone Strikes', *U.S. Army War College - Strategic Studies Institute*. [Online]. http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1304.

[2] John Croft. (2016, February) 'Drone Aids TransAsia Flight 222 Accident Investigation', *Aviation Week*. [Online]. http://aviationweek.com/commercial-aviation/drone-aids-transasia-flight-222-accident-investigation.

[3] Kim Hartmann and Christoph Steup, 'The Vulnerability of UAVs to Cyberattacks', in *5th International Conference on Cyber Conflict*, Tallinn, Estonia, 2013.

[4] Matt Bishop, 'Introduction to Computer Security'. Boston, USA: Addison-Wesley, 2004.

[5] Kevin Mitnick, 'The Art of Deception: Controlling the Human Element of Security': John Wiley & Sons, 2003.

[6] Aaron Karp. (2015, October) 'Congress to hold UAV safety hearing Oct. 7', *ATWonline.com*. [Online]. http://atwonline.com/government-affairs/congress-hold-uav-safety-hearing-oct-7.

[7] John Croft. (2015, October) 'DOT: Register Your Drones Or Face FAA Penalties', *Aviation Week*. [Online]. http://aviationweek.com/commercial-aviation/dot-register-your-drones-or-face-faa- penalties.

[8] Cyrus Farivar. (2015, November) 'Drone collides with Seattle Ferris wheel, busts through plastic table', *Ars Technica*. [Online]. http://arstechnica.com/tech-policy/2015/11/drone-collides-with-seattle-ferris-wheel-busts-through-plastic-table/.

[9] Megan Guess. (2015, June) 'Drone flying over forest fire diverts planes, costs US Forest Service $10K', *Ars Technica*.

[10] Cyrus Farivar. (2015, December) 'Toddler loses eyeball after errant drone slices it in half', *Ars Technica*. [Online]. http://arstechnica.com/tech-policy/2015/12/toddler-loses-eyeball-after-errant-drone-slices-it-in-half/.

[11] Aaron Karp. (2015, September) 'FAA Nightmare: A Million Christmas Drones', *Aviation Week*. [Online]. http://aviationweek.com/commercial-aviation/faa-nightmare-million-christmas-drones.

[12] Aviation Week & Space Technology. (2015, September) 'Editorial: Get Data On Risk UAS Pose To Air Traffic', *Aviation Week*. [Online]. http://aviationweek.com/commercial-aviation/editorial-get-data-risk-uas-pose-air-traffic.

[13] Thomas Fox-Brewster. (2016, March) 'Police Drone Can Be Commandeered From Over A Mile Away, Hacker Claims', *Forbes.com*. [Online]. http://www.forbes.com/sites/thomasbrewster/2016/03/02/surveillance-drone-hacked/.

[14] Andrew J. Kerns, Daniel P. Shepard, Jahshan A. Bhatti, and Todd E. Humphreys, 'Unmanned Aircraft Capture and Control Via GPS Spoofing', *Journal of Field Robotics*, vol. 31, no. 4, 2014.

[15] Peter König. (2015, September) 'Hacker starten Stratosphärenballon, um Drohnen-Funk mitzuschneiden' ('Hackers use stratosphere balloon to intercept UAV radio traffic'), *Heise.de*. [Online]. http://www.heise.de/make/meldung/Hacker-starten-Stratosphaerenballon-um-Drohnen-Funk-mitzuschneiden-2823100.html.

[16] Heise Online. (2015, November) 'PhoneDrone Ethos: Drohne nutzt Smartphone als Steuerungsrechner' ('PhoneDrone Ethos: Drone uses Smartphones as Controlunit'), *Heise.de*. [Online]. http://www.heise.de/newsticker/meldung/PhoneDrone-Ethos-Drohne-nutzt-Smartphone-als-Steuerungsrechner-2912422.html.

[17] Hak5. (2014, January) 'Pineapple Drone, Rooftop Packet Sniffing And Offline Archival Backup', *hak5.org*. [Online]. http://hak5.org/episodes/hak5-1520.

[18] Ricky Hill. (2013, March) 'Phantom Network Surveillance UAV / Drone - Defcon', *Defcon.org*. [Online]. https://www.defcon.org/images/defcon-21/dc-21-presentations/Hill/DEFCON-21-Ricky-Hill-Phantom-Drone-Updated.pdf.

[19] Hak5. (2013, December) 'Drones Hacking Drones', *hak5.org*. [Online]. http://hak5.org/episodes/hak5-1518.

[20] Kamkar, Samy. (2013, December) 'SkyJack: autonomous drone hacking'. [Online]. http://samy.pl/skyjack/.

[21] Kamkar, Samy. (2013, December) 'SkyJack', *Github.com*. [Online]. https://github.com/samyk/skyjack.
[22] BBC News. (2009, December) 'Iraq insurgents 'hack into video feeds from US drones'', *BBC.co.uk*. [Online]. http://news.bbc.co.uk/2/hi/middle_east/8419147.stm.
[23] Emy Rivera, Robert Baykov, and Goufei Gu, 'A Study On Unmanned Vehicles and Cyber Security', Texas, USA, 2014.
[24] Dan Lamothe. (2016, January) 'U.S. and Britain hacked into feeds from Israeli drones and fighter jets, according to report', *Washington Post*. [Online]. https://www.washingtonpost.com/news/checkpoint/wp/2016/01/29/u-s-and-britain-hacked-into-feeds-from-israeli-drones-and-fighter-jets-according-to-report/.
[25] Samvartaka blog. (2016, February) 'Cryptanalysis of intercepted Israeli drone feeds', *Github.io*. [Online]. http://samvartaka.github.io/cryptanalysis/2016/02/02/videocrypt-uavs.
[26] Mike Mount and Elaine Quijano. (2009, December) 'Iraqi insurgents hacked Predator drone feeds U.S. official indicates', *CNN.com*. [Online]. http://edition.cnn.com/2009/US/12/17/drone.video.hacked/.
[27] Scott Peterson. (2011, December) 'Exclusive: Iran hijacked US drone, says Iranian engineer', *Christian Science Monitor*. [Online]. http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video.
[28] Raymond Richards. (Undated) 'High-Assurance Cyber Military Systems (HACMS)', *DARPA.mil*. [Online]. http://www.darpa.mil/program/high-assurance-cyber-military-systems.
[29] Joe Gould. (2015, August) 'Electronic Warfare: What US Army Can Learn From Ukraine', *Defense News*. [Online]. http://www.defensenews.com/story/defense/policy-budget/warfare/.um=email&utm_term=%2ASituation%20Report&utm_campaign=SitRep0803.
[30] Dr. Robert J. Bunker. (2015, August) 'Terrorist and Insurgent Unmanned Aerial Vehicles: Use, Potentials, and Military Implications', *U.S. Army War College - Strategic Studies Institute*. [Online]. http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1287.
[31] Patrick Tucker. (2015, March) 'In Ukraine, Tomorrow's Drone War Is Alive Today', *Defence One*. [Online]. http://www.defenseone.com/technology/2015/03/ukraine-tomorrows-drone-war-alive-today/107085/.
[32] Graham Warwick. (2016, January) 'Assisting The Human Central to Pentagon's Third Offset', *Aviation Week*. [Online]. http://aviationweek.com/defense/assisting-human-central-pentagon-s-third-offset.
[33] North Atlantic Treaty Organisation. (2015, August) 'Framework for Future Alliance Operations', *NATO.int*. [Online]. http://www.act.nato.int/images/stories/media/doclibrary/ffao-2015.pdf.
[34] Sydney J. Freedberg. (2015, November) 'Army Fights Culture Gap Between Cyber & Ops: "Dolphin Speak"', *BreakingDefense.com*. [Online]. http://breakingdefense.com/2015/11/army-fights-culture-gap-between-cyber-ops-dolphin-speak/.
[35] Adam Rawnsley. (2015, February) 'War is Boring', *Medium.com*. [Online]. https://medium.com/war-is-boring/ukraine-scrambles-for-uavs-but-russian-drones-own-the-skies-74f5007183a2.
[36] Maksym Bugriy. (2014, June) 'The Rise of Drones in Eurasia (Part One: Ukraine)', *JamesTown.org*. [Online]. http://www.jamestown.org/single/?tx_ttnews%5Btt_news%5D=42536.
[37] Nolan Peterson. (2015, March) 'Ukraine's Grassroots Drone Program Takes Flight', *The Daily Signal*. [Online]. http://dailysignal.com/2015/03/12/ukraines-grassroots-drone-program-takes-flight/.
[38] Christian Borys. (2015, April) 'Crowdfunding a war: Ukraine's DIY drone-makers', *The Guardian*. [Online]. http://www.theguardian.com/technology/2015/apr/24/crowdfunding-war-ukraines-diy-drone-makers.
[39] Nicholas Lazaredes. (2015, April) 'Ukraine's DIY drone war: Self-taught soldiers facing up to Russian-backed war machine', *ABC.net*. [Online]. http://www.abc.net.au/news/2015-04-22/ukraines-diy-drone-war/6401688.
[40] Patrick Tucker. (2015, February) 'How US Technology Could Help Ukraine Without 'Arming' It', *Defense One*. [Online]. http://www.defenseone.com/technology/2015/02/how-us-technology-could-help-ukraine-without-arming-it/104931/.
[41] Sydney J. Freedberg. (2015, October) 'Russian Drone Threat: Army Seeks Ukraine Lessons', *BreakingDefense.com*. [Online]. http://breakingdefense.com/2015/10/russian-drone-threat-army-seeks-ukraine-lessons/.
[42] Andrew Tilghman. (2015, December) 'Advanced Russian air power, jammers are focus of U.S. troops', *Military Times*. [Online]. http://www.militarytimes.com/story/military/pentagon/2015/12/10/advanced-russian-air-power-jammers-focus-us-troops/77090544/.
[43] SC Magazine. (2015, October) 'Russia overtaking US in cyber-warfare capabilities', *SCMagazine.com*. [Online]. http://www.scmagazine.com/russia-overtaking-us-in-cyber-warfare-capabilities/article/450518/.
[44] David Esler. (2015, September) 'What A Business Aviation Flight Department Needs To Know About UAVs', *Aviation Week*. [Online]. http://aviationweek.com/print/business-aviation/what-business-aviation-flight-department-needs-know-about-uavs.

[45] Emily Reynolds. (2015, November) 'DJI update enforces drone no-fly zones across Europe and USA', *Wired*.
[46] Kieren McCarthy. (2016, January) 'Bloke sues dad who shot down his drone – and why it may decide who owns the skies', *The Register*. [Online]. http://www.theregister.co.uk/2016/01/07/drone_lawsuit_who_owns_the_skies/.
[47] Cyrus Farivar. (2015, October) '"Drone Slayer" cleared of charges: "I wish this had never happened"', *Ars Technica*. [Online]. http://arstechnica.com/tech-policy/2015/10/drone-slayer-cleared-of-charges-i-wish-this-had-never-happened/.
[48] Federal Aviation Administration. (2015, December) 'Registration and Marking Requirements for Small Unmanned Aircraft', *FAA.gov*. [Online]. https://www.faa.gov/news/updates/media/20151213_IFR.pdf.
[49] Graham Warwick. (2015, October) 'First Interim Standards For Unmanned Aircraft Unveiled', *Aviation Week*. [Online]. http://aviationweek.com/commercial-aviation/first-interim-standards-unmanned-aircraft-unveiled.
[50] Kieren McCarthy. (2015, December) 'FAA introduces unworkable drone registration rules in time for Christmas', *The Register*. [Online]. http://www.theregister.co.uk/2015/12/14/faa_drone_registration_rules/.
[51] Chatham House. (2015, September) 'Dealing with Drones: A Look at the Regulatory Challenges of Remotely Piloted Aircraft Systems', *Chatham House Seminar*. [Online]. https://www.chathamhouse.org/event/dealing-drones-look-regulatory-challenges-remotely-piloted-aircraft-systems.
[52] David Eshel and John M. Doyle. (2015, November) 'UAV Killers Gain Role Against Growing Threat', *Aviation Week*. [Online]. http://aviationweek.com/defense/uav-killers-gain-role-against-growing-threat.
[53] Daniel Culpan. (2015, August) 'Boeing's latest drone destroyer is the stuff of nightmares', *Wired*.
[54] Graham Warwick. (2016, February) 'Counter-UAS Special Report: The Countermeasures Options', *Aviation Week*. [Online]. http://aviationweek.com/technology/counter-uas-special-report-countermeasures-options.
[55] Graham Warwick. (2015, December) 'Countering Unmanned Defense & Space Technologies To Watch In 2016', *Aviation Week*. [Online]. http://aviationweek.com/defense/defense-space-technologies-watch-2016-0.
[56] Swati Khandelwal. (2015, October) 'First Ever Anti-Drone Weapon that Shoots Down UAVs with Radio Waves', *The Hacker News*. [Online]. http://thehackernews.com/2015/10/drone-defender-gun.html.
[57] Battelle. (2016, April) 'Battelle DroneDefender', *Battelle.org*. [Online]. http://www.battelle.org/our-work/national-security/tactical-systems/battelle-dronedefender.
[58] Kieren McCarthy. (2016, January), 'Beware the terrorist drones! For they are coming! Pass new laws!', *The Register*. [Online]. http://www.theregister.co.uk/2016/01/11/beware_terrorist_drones/.
[59] Jacquelin Foster. (2015, September) 'Report on the safe use of remotely piloted aircraft systems (RPAS), commonly known as unmanned aerial vehicles (UAVs), in the field of civil aviation', *EUROPA.eu*. [Online]. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2015-0261+0+DOC+XML+V0//EN.
[60] Federal Aviation Administration. (2015, December) 'Press Release – FAA Announces Small UAS Registration Rule', *FAA.gov*. [Online]. http://www.faa.gov/news/press_releases/news_story.cfm?newsId=19856.
[61] Jared Ablon, Steve Crocker, Benjamin D. Marcus, and Gregory S. McNeal. (2016, February) 'Robust and Scalable UAS Registration: Key Technology Issues And Recommendations', *SUASNews.com*. [Online]. www.suasnews.com/wp-content/uploads/2016/02/AirMap_White-Paper_UAS-Registration_02042016.pdf.
[62] Graham Warwick and Larry Dickerson. (2015, December) 'Military UAVs Mark Time As Civil Market Advances', *Aviation Week*. [Online]. http://aviationweek.com/print/defense/military-uavs-mark-time-civil-market-advances.
[63] Graham Warwick. (2015, December) '"Swarm Theory", Defense & Space Technologies To Watch In 2016', *Aviation Week*. [Online]. http://aviationweek.com/defense/defense-space-technologies-watch-2016-0.
[64] Tyler Rogoway. (2015, December) 'Here's The First Shot Of The F-15C Pod That Will Change How The Air Force Fights', *Foxtrotalpha*. [Online]. http://foxtrotalpha.jalopnik.com/here-s-the-first-shot-of-the-f-15c-pod-that-will-change-1750314539.
[65] Graham Warwick. (2015, December) '"Team Players", Defense & Space Technologies To Watch In 2016', *Aviation Week*. [Online]. http://aviationweek.com/defense/defense-space-technologies-watch-2016-0.
[66] Graham Warwick. (2016, January) 'Tiny ADS¬B Provides UAV Sense¬-and--avoid', *Aviation Week*. [Online]. http://aviationweek.com/commercial-aviation/week-technology-jan-4-8-2016.
[67] Matt Burges, 'UK at risk from 'simple and effective' terrorist drone attacks', *Wired*, January 2016.
[68] Tony Osborne. (2015, January) 'Terror by Drone', *Aviation Week & Space Technology (print edition)*, pp. 28-29.

[69] Alan Levin. (2015, May) ‘FAA introduces unworkable drone registration rules in time for Christmas’, *Bloomberg.com*. [Online]. http://www.bloomberg.com/news/articles/2015-05-29/google-s-solar-fueled-cyber-drone-crashes-during-new-mexico-test.
[70] Christian Czosseck, ‘State Actors and their Proxies in Cyberspace’, in *Peacetime Regime for State Activities in Cyberspace*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2013.
[71] Kim Hartmann and Christoph Steup, ‘N3P: A Natural Privacy Preserving Protocol for Electronic Mail’, in *4th International Conference on Cyber Conflict*, Tallinn, Estonia, 2012.
[72] Daniel T. Kuehl, ‘From Cyberspace to Cyberpower: Defining the Problem’, in *Cyberpower and National Security*.: Potomac Books Incorporated, 2009.
[73] Heli Tiirmaa-Klaar, ‘Cyber Diplomacy: Agenda, Challenges and Mission’, in *Peacetime Regime for State Activities in Cyberspace*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2013.
[74] Eray Yagdereli, Cemal Gemci, and A. Ziya Aktas, ‘A study on cyber-security of autonomous and unmanned vehicles’, *The Journal of Defense Modelling and Simulation: Applications, Methodology, Technology*, vol. 12, no. 4, 2015.

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

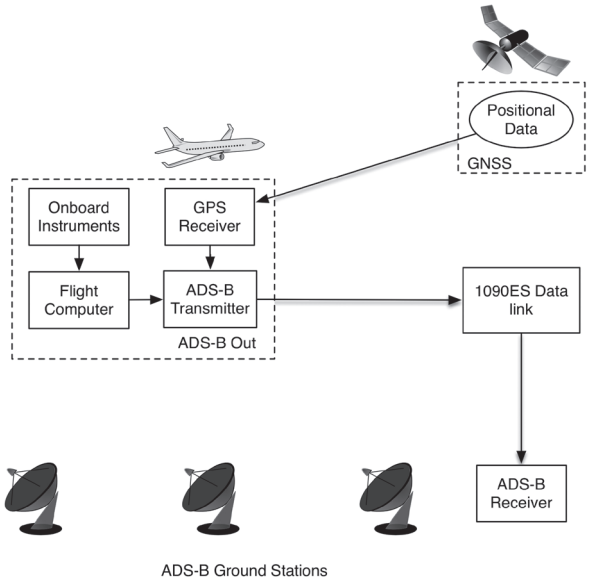
ADS-B is a protocol in which aircraft continually broadcast their own ID, position and velocity as well as further information such as intent or urgency codes. These broadcasts do not require interrogation but independently send the aircraft's position and velocity twice a second and unique identification 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.

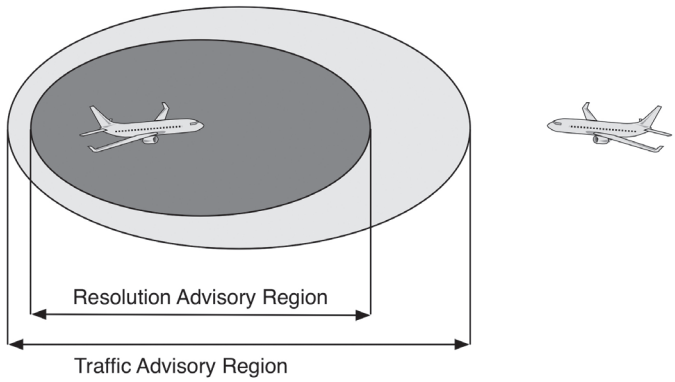
2. TCAS

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.

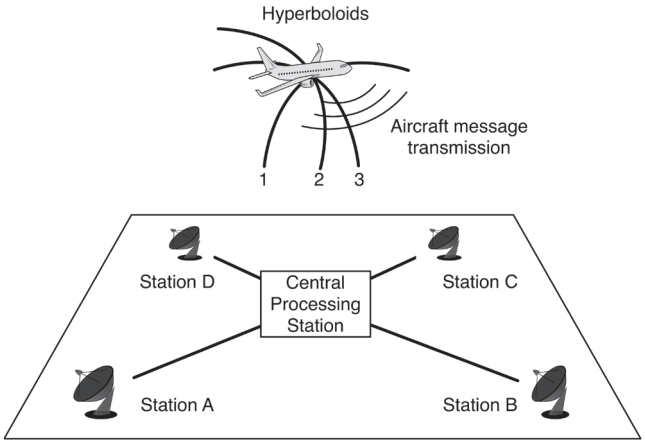
Whilst TCAS is vulnerable due to its design and technologies used, the implications of launching an attack on TCAS are extremely serious. In the best case, ATC may be unable to manage airspace, or aircraft may have a near miss. Jamming the channel or injecting wrong data, however, could cause mid-air 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.

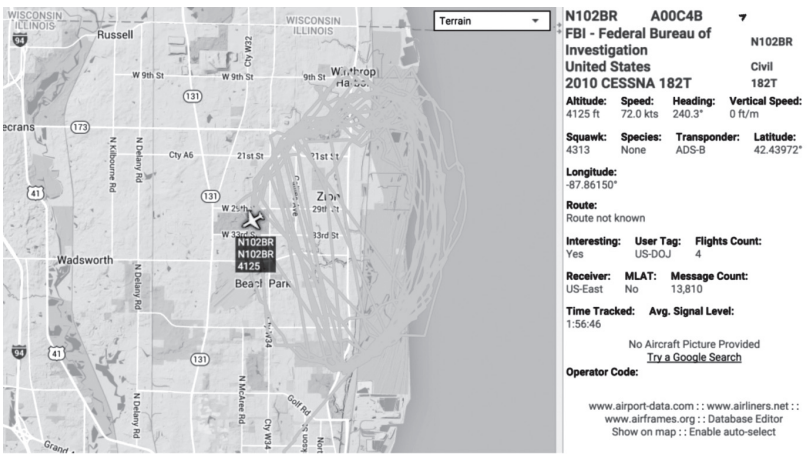
6. AVIATION COMMUNICATIONS SECURITY AS A NEW CYBER POWER ISSUE

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

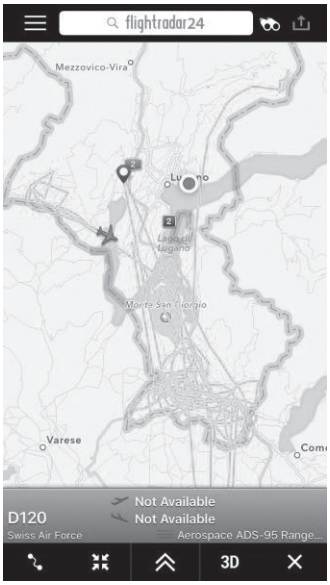


In military settings, this type of open surveillance using data gleaned from Mode S and ADS-B broadcasts has led to similar information leakage through the intentional or unintentional use of transponders during active missions. The diligent tracking of recent airborne engagements in Syria by NATO and 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].