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.

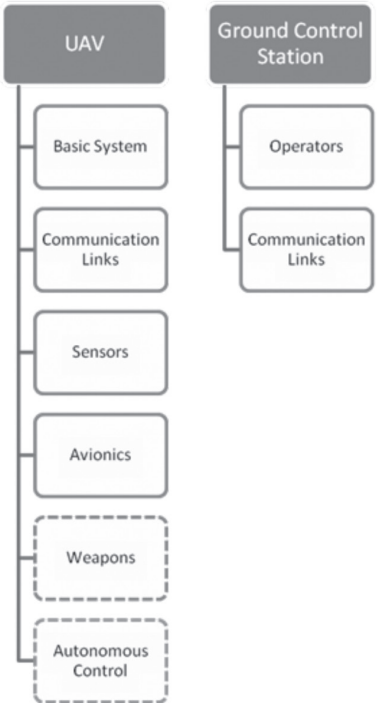
A. Preliminaries

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.