INTEGRATING CYBER WITH AIR POWER IN THE SECOND CENTURY OF THE ROYAL AIR FORCE

By Wing Commander Paul Withers

Biography: Wing Commander Paul Withers is an Engineer Officer, currently serving at the NATO Combined Air Operations Centre at Uedem in Germany. Previously an Officer Career Manager, he also has significant professional experience as a cyber operations planner. As a CAS Fellow, he completed an MA with King's College London and is currently researching for his dissertation for an MSc in Cyberspace Operations.

Abstract: Rapid technological development has been a feature of air power from its inception. More recently, there has been growing recognition that air power is increasingly dependent on the cyber domain. As we try to make sense of the implications of cyberspace, various concepts have been proposed, with United Kingdom Air Power Doctrine developing the principles of Air-Cyber Integration. This article examines Air-Cyber Integration, with an explanation of some general concepts and a study of both defensive and offensive cyber operations and their relationship with air power. It considers technology and process, but most importantly, it reflects upon the need for airmen and women who can operate effectively in both the air and cyberspace domains.

I think most people today understand that cyber clearly underpins the full spectrum of military operations, including planning, employment, monitoring, and assessment capabilities. I can't think of a single military operation that is not enabled by cyber. Every major military weapon system, command and control system, communications path, intelligence sensor, processing and dissemination functions—they all have critical cyber components.

General William L. Shelton, former Commander, US Air Force Space Command[1]

INTRODUCTION

The ubiquity of cyberspace described by General Shelton is perhaps obvious; its implications are arguably less so. As the Royal Air Force (RAF) enters its second century, it will bring its most complex and capable air system into front-line operational service: the fifth-generation F-35B Lightning. This fifth-generation air system comprises not just the air platform itself but an interconnected 'system-of-systems' that is dependent upon cyberspace. Implicit in the delivery of the F-35B Lightning is the requirement for the RAF to adapt more broadly to become a 'fifth-generation air force'. Increased reliance on cyberspace raises questions over the extent to which air operations are resilient in a contested cyberspace. In addition to the direct dependence of air systems on cyberspace, there is increasing interdependence with the other domains for the conduct of operations. This has led to the development of the concept of Air-Cyber Integration[2] which, whilst a relatively recent addition to the lexicon, has in reality been part of warfare since at least the 1990s.[3]

Cyberspace has taken its place as the fifth domain[4] of warfare, a domain[5] that is rapidly changing from a niche area to one which underpins all defence capability. In order for its potential to be realised, the UK Armed Forces must confront the challenges presented by technology and, in doing so, develop the right people and appropriate processes to operate in the cyber domain. The 2016 UK National Cyber Security Strategy makes commitments to defend against cyber threats and to deter aggression in cyberspace.[6] In realising the military elements of this strategy, there are clear roles for UK Defence and the RAF specifically in defending military platforms and capabilities, but also in integrating cyber effects into operations. However, as with any area of military endeavour, hardware and infrastructure have little value on their own; military cyberspace capability relies upon trained personnel, under effective leadership, using tried and tested doctrine and tactics to deliver operational effect.

This article will consider some of the cyberspace challenges for air power. It will take a broad view of people, process, and technology from the perspectives of both threats to air power through cyberspace, and the opportunities that the integration of air and cyber presents to joint operations. The article will be presented in five parts. First, to set the scene for the remainder of the article, it will consider some of the terminology associated with attack through cyberspace. Second, it will discuss some of the

implications of becoming a fifth-generation air force and argue why cyberspace matters for the delivery of air power. In doing so, it will look beyond the threat to networks and platforms and consider air power capabilities as part of interrelated systems, which require a more holistic approach to cyber defence. Third, it will consider the opportunities for offensive Air-Cyber Integration, based on some historical examples since the 1990s. The specifics of offensive cyber operations tend to be closely guarded, but the general principles can be established from past examples that have come into the public domain. Fourth, the article will consider what is arguably the most important part of UK Defence's cyber capability: the skilled and experienced personnel who can defend and attack in cyberspace, and integrate cyber with the other domains. It will consider the challenges of developing and retaining sufficient airmen and women as credible and effective operators in cyberspace. It will argue that there are three types of cyber operator: *all military personnel* who operate information technology and weapon systems; the *cyber specialists* who carry out offensive and defensive cyber operations; and *commanders and staff officers* who plan and integrate cyber effects. Finally, it will conclude that effective Air-Cyber Integration requires a holistic view of defending air platforms and their associated supporting systems, whilst leveraging the ability to exploit weaknesses in those of the adversary. It will argue that the second century of air power, like the first will be characterised by pushing the boundaries of technology; moreover, pushing those boundaries to achieve effective Air-Cyber Integration will continue to rely on the skill, innovation, and character of human operators.

TERMINOLOGY - CYBER VULNERABILITIES AND EXPLOITS

There have been numerous attempts to define cyberspace, with subtle nuances of definition often due to the evolution in understanding of the cyber domain and the particular perspective of the definition. The Development, Concepts and Doctrine Centre (DCDC) Cyber Primer defines cyberspace as consisting of:

> *The interdependent network of digital technology infrastructures (including platforms, the Internet, telecommunications networks, computer systems, as well as embedded processors and controllers), and the data therein spanning the physical, virtual and cognitive domains.*[7]

This particular definition includes some important elements that should influence the manner in which airmen think about cyberspace. First, its scope is significantly greater than the public Internet; in particular for air power, we should consider that modern air platforms exist not just in the physical air domain, but also in cyberspace, and they should be visualised in both domains. Second, it is important to consider the implications of embedded processors and controllers. Increasingly, the systems that support all of our air platforms are controlled through cyberspace. Consequently, any assessment of the resilience of air operations must consider cyber vulnerabilities. Third, cyberspace spans the 'physical, virtual and cognitive.' Often cyberspace is seen

as a purely technical challenge, the realm of Information Technology (IT) professionals, but the threats and opportunities presented by cyberspace have as much to do with human cognition as they do technology. The challenges of cyberspace, therefore, call for a multi-disciplinary approach, building diverse teams of cyber operators.

In order to establish the basic principles of attacking and defending in cyberspace, this section will consider some relevant terminology. Attacks through cyberspace occur as a result of a *threat actor* exploiting a *vulnerability*. A threat actor is a person or group possessing the intent, capability and opportunity to mount an attack.[8] In this paper the terms threat actor and attacker are used interchangeably. Vulnerabilities can be broadly categorised as *flaws*, *features* or *user error*.[9] Flaws come about as a result of errors in the development of a system, primarily software code, and are *unintended.* Features are *intended* functionality that can be misused and exploited by an attacker. Even where design flaws and features have been addressed through good configuration and effective management of measures such as applying software updates, systems can still be vulnerable through user error. User error can be as simple as leaving a computer unattended or choosing a weak password. Some of the most effective cyber attacks come about as a result of users being tricked, or socially engineered, into giving away information to an attacker, or by unwittingly installing malicious software (malware).

In order to deliver an effect, the attacker needs to be able to exploit a vulnerability. To do so, the attacker may use a range of tools and techniques. The UK National Cyber Security Centre categorises these tools and techniques as 'commodity' and 'bespoke' capabilities.[10] Commodity capabilities are available on the Internet and are often easy to operate, whereas, bespoke capabilities are tailored for a particular target and require a much greater degree of skill. Commodity capabilities are generally effective only when cyber security measures have not been implemented effectively. Effective cyber defence would defeat most commodity capabilities, making the exploitation of a system much more difficult for all but the most capable and determined attackers.

Bespoke capabilities tend to be tailored for a specific purpose, and therefore may only be effective against a specific target in a particular configuration. Bespoke capabilities will sometimes take advantage of vulnerabilities that are not yet known to software vendors, carrying out what is known as a 'zero-day' attack.[11] The cyber threat intelligence company, *FireEye* defines zero-day attacks as 'software or hardware vulnerabilities that have been exploited by an attacker where there is no prior knowledge of the flaw in the general information security community, and, therefore, no vendor fix or software patch available for it.'[12] Zero-days are the 'hacking world's prized possession', because initially they cannot be detected by antivirus software, and the absence of software patches makes it very difficult to defend against them.[13] They are highly valued, as once they are known, measures to detect and defeat them are often developed rapidly. Cyber security researchers will often publish their discovery of a new vulnerability and the means of

exploiting it, enabling the antivirus and software companies to release updates and patches in a matter of days.

However, for military offensive cyber operations, governments may choose to retain the knowledge of exploits for future use, rather than reveal them to the cyber security industry.[14] This is extremely controversial, but arguably necessary, if states wish to develop effects in cyberspace that can breach the defences of another state in time of conflict. This implies a responsibility on the state to use the capability responsibly and in accordance with the norms of International Law. In the US, the controversy surrounding government use of zero-days led to a Presidential Directive forcing the US National Security Agency (NSA) to disclose vulnerabilities that it discovers, unless it can demonstrate 'a clear national security or law enforcement need'.[15] Some cyber techniques have been categorised as weapons and are therefore subject to the Wassenaar Agreement which governs the export of conventional armaments.[16] It is of course possible that non-state actors could develop similar knowledge and capabilities, without being subject to the constraints of national or International Law.

The possession of suitable exploit code does not in itself give the attacker the ability to deliver an effect through cyberspace. The attacker needs to develop a process to understand the target and its vulnerabilities, gain access, deploy the exploit and then have the desired effect. A number of models have been developed to describe this process; one popular model is the Lockheed Martin Cyber Kill Chain.[17] This model describes a seven-step process, which is instructive in describing how a cyber attack may occur. Initially, the attacker carries out *reconnaissance* on his target, which may involve online research for basic information about the target organisation or people, and the use of tools to scan for vulnerabilities. During the next stage, known as *weaponization*, the attacker will obtain or develop an exploit and couple it with a means of access. Lockheed Martin refer to the means of access as a 'back door', which could be enabled through technical means or through deceiving a human into granting access. Third, the attacker will *deliver* the weaponized code. Delivery may, for example, take the form of access through a vulnerable web application, through an unwitting user clicking on a link in an email, or through plugging in removable media, such as a USB device. Stage four is *exploiting* a vulnerability on the target system, with stage five being the *installation* of the malware. In the sixth stage, the attacker establishes a *Command and Control (C2)* channel to control the deployed malware. Finally, having established a means of C2, the attacker carries out his '*actions on objectives*', or the execution of his desired effect. It should be noted that the first six stages might be similar if the intent was the exfiltration of data, by espionage, for instance; or if the intent was to disrupt, degrade or destroy the target system. For a military cyber operation, stages one to six might occur well in advance of any requirement to deliver an effect, with the final stage synchronised with action in one or more of the physical domains, such as a pre-planned air operation.

In principle, cyber defence consists of a range of measures aimed at breaking the kill chain. Having established the basic terminology related to attacks in and through cyberspace, the article will turn to the consideration of cyberspace in the context of the second century of air power and some of the implications for a 'fifth-generation' air force.

DEFENSIVE AIR-CYBER INTEGRATION AND THE FIFTH-GENERATION AIR FORCE

Analysis of the 1991 Persian Gulf War led to heated debate about whether a Revolution in Military Affairs (RMA) had occurred. This contributed to a conceptual change in Western air forces, based on a desire to harness 'the quality of the information that can be collected, and its virtually instantaneous transmission, combined with the speed and precision with which force can then be applied.'[18] The RMA concepts evolved and shaped the development of military technology and strategy. The marriage of advanced aircraft and weapon design, with sensor and information processing technology, has led to a step change in capability through the development of a fifth generation of combat air systems. The introduction of the F-35B Lightning presents a transformational challenge for the RAF in integrating the capability into operations. This article will not consider the capabilities of, or means of employing, this highly capable fifth-generation air system, but will focus on some of its broader implications, specifically in cyberspace.

The Australian Air Force Chief defines a *Fifth-Generation Air Force* as 'a fully networked, integrated air force whose systems share battlespace awareness from multiple nodes to increase situational awareness and targeting fidelity to maximise whole force effect'.[19] The implications of fifth-generation capabilities, therefore, extend far beyond the air platform and its associated systems. The RAF Strategy recognises that along with the opportunities afforded by technology, Control of the Air in the future will be challenged in ways that will seek to overcome the advantage of modern platforms:

> *Control of the air and space will remain essential to joint operational success. Our enemies will challenge us for that control, with widely available and highly capable air-defence systems, by exploiting easily accessible commercial off-the-shelf technology, and through an improving offensive cyber capability.*[20]

It is entirely rational that potential adversaries would seek to weaken the advantages of fifth-generation technology, and the RAF Strategy notes that adversaries are likely to aim to lessen the RAF's combat power through exploiting vulnerabilities on the ground.[21] This approach is conceptually as old as air power itself, and Douhet's 'eggs in the nest' analogy retains its validity in the second century of air power: '...in the air his planes may escape; but, like the birds whose nests and eggs have been destroyed, those planes which were still out would have no bases at which to alight when they returned.'[22] Whilst Douhet had physical degradation or destruction of air bases in mind, the reliance of modern air systems on cyberspace offers the adversary opportunities to

deliver a wide range of effects, potentially short-lived and reversible, but with the ability to significantly disrupt operations.

All modern air platforms and systems are reliant on cyberspace to some degree, but the F-35B Lightning aircraft can be visualised as sitting at the centre of a 'system-of-systems', reliant upon people, processes and a wide range of technology, as shown in Figure 1.

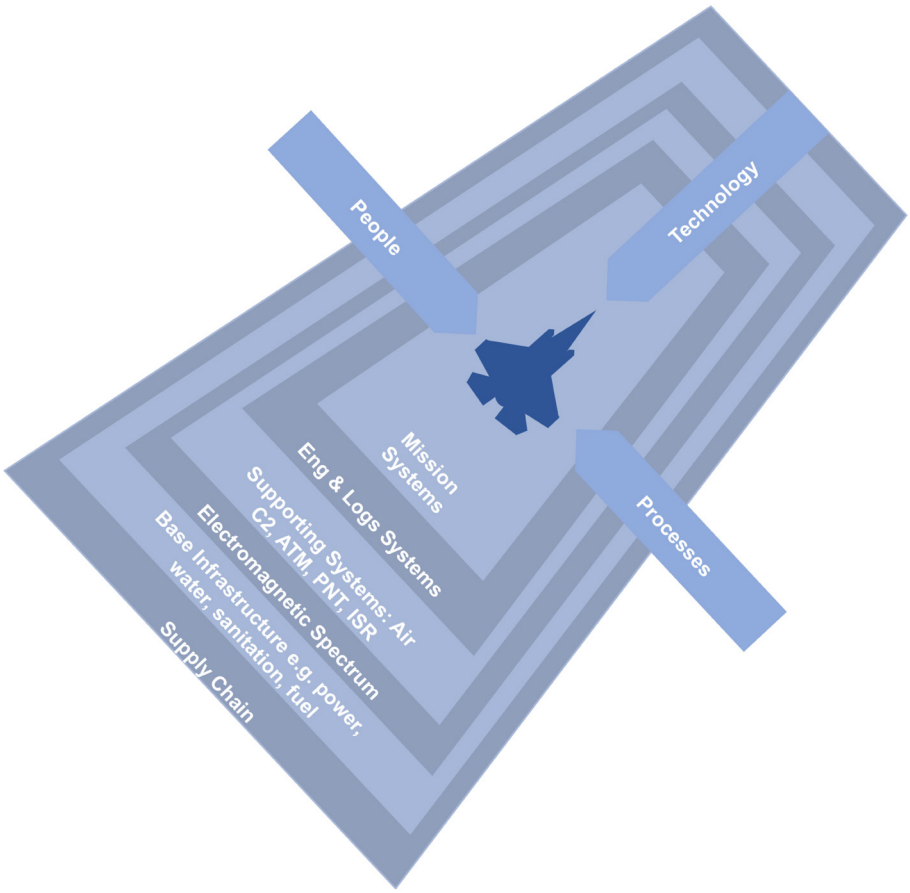

Figure 1-*The F-35B Lightning as part of a system-of-systems*

This discussion focusses on the *potential* for vulnerability and does not consider any specific threat. At any given time, a threat actor with capability, intent and opportunity, may wish to attack air power capabilities through cyberspace; however, this paper makes no assumption about any specific actor, nor the level of capability required.

At the core of the system is the complex air platform itself, with an array of interconnected aircraft and mission systems. For the F-35B Lightning, the term 'mission

system' refers to the air platform's 'operating software, avionics, integrated electronic sensors, displays and communications systems that collect and share data with the pilot and other friendly aircraft, providing unmatched situational awareness.'[23] The increased cyber threat to air platforms comes about as a result of their increased complexity. Cyber security analyst and former RAF fast jet pilot, Pete Cooper, points out that 'aircraft are now digitized and contain millions of lines of code; writing, verifying, and securing it is an increasingly difficult and complex task.'[24] Each generation of combat aircraft brought into service with the RAF has brought with it increased capability, but also complexity, with the manufacturer of the F-35B Lightning stating that 'underpinning the F-35's capabilities is more than 8 million lines of software code.'[25] This level of complexity increases the likelihood that the software code includes vulnerabilities that could potentially be exploited by an adversary. In the commercial IT sector, vendors have developed a level of responsiveness that allows patches to be developed and deployed quickly when software vulnerabilities are discovered. However, in safety-critical aircraft software code, the process is slower and more complex, and 'modifying one line of safety critical software on board an aircraft is currently estimated to take a year and cost around $1 million.'[26] For the F-35B Lightning, potential cyber vulnerabilities and platform airworthiness are inextricably linked.

Post-flight checks on an F-35B Lightning at RAF Marham. © Crown copyright.

Potential vulnerabilities are not limited to the air platform but include the entire 'ecosystem' of which the platform is a component. The F-35B Lightning's mission, engineering, and logistics are supported by the Autonomic Logistics Information System (ALIS), which is 'integral to maintaining and operating F-35s.'[27] ALIS provides

the F-35 fleet with a single management tool that integrates maintenance activity with the supply chain.[28] This system connects the air platform with a global network of support agencies and commercial vendors. Cyber defence of this system is obviously vital; if any cyber vulnerabilities were present, they could be exploited in a manner that could theoretically disrupt the entire Lightning fleet, not just of the UK but of all the allies in the programme. Measures to protect ALIS are as important as protecting the aircraft mission system, as mission support systems *may* provide a bridge for malware to jump from the public Internet to the aircraft platform. *The Times* newspaper reported on speculation that ALIS was indeed vulnerable to cyber attack.[29] This led to an examination by the House of Commons Defence Committee, who acknowledged that the F-35B Lightning had a greater reliance on software than any other defence programme and noted that 'ALIS is of particular importance.'[30] The Committee heard evidence from the Ministry of Defence (MoD) and Lockheed Martin that there had been 'rigorous cyber-testing of ALIS and that software bugs [had] mostly been rectified.'[31] The use of the word 'mostly' implies that perhaps not all known bugs have been resolved, which is perhaps a reflection of the difficulties of assuring air system software. The level of importance attached to the cyber security of ALIS, and the associated parliamentary scrutiny, is commensurate with its level of importance to the overall security and operational effectiveness of the Lightning programme.

In 2009, systems worldwide, including some within the RAF, were hit by a *worm*, a self-propagating piece of malware, known as 'Conficker'. Despite the availability of patches that could have been implemented to prevent the infection, Conficker spread widely. Although it had no specific operational impact beyond the investment of resource to remove it, Conficker 'underlined the potential disruption that could result from even the most simple of infections.'[32] Nearly a decade later, air power's dependence on cyberspace means that there could be significant consequences for operations if malware were to penetrate a system such as ALIS.

Beyond the F-35B Lightning and the systems that directly support it, air operations rely upon Air Traffic Management, Positioning, Navigation and Timing (PNT) and Air Command and Control (C2) systems. Air missions are also routinely supported by a range of Intelligence, Surveillance and Reconnaissance (ISR) platforms and systems. These supporting systems are themselves reliant on space, cyberspace and the electromagnetic spectrum. The importance of the electromagnetic environment and its interdependence with the cyber domain, has seen a doctrinal and organisational shift in the UK Armed Forces towards the synchronisation and coordination of Cyber and Electromagnetic Activity (CEMA).[33]

Air operations also depend upon the fixed infrastructure at Main and Deployed Operating Bases. This includes electrical power, water, sanitation, fuel and other logistics, and the provision of aircraft life support systems such as liquid oxygen.[34]

Increasingly infrastructure systems and processes are managed and controlled by computerised Industrial Control Systems (ICS). If an adversary wished to degrade the combat effectiveness of the air system, he might choose to do so indirectly, through the ICS of one of its service support systems. The ICS sector has spawned its own subset of the cyber security industry. The automation of process control has come about through the use of Programmable Logic Controllers (PLC), which started in the 1960s. PLCs were connected to systems with the intent that processes could easily be updated through remotely changing software code in the PLC. To facilitate maintenance access, they tended to be connected to centralised computer systems, often with remote access via a modem, or other means of indirect connection to the Internet. PLCs came into use at a time before computer hacking became widespread, and even when security started to become a concern, the fact that ICS tended to be isolated from other networks and used arcane proprietary software, was often seen as effective risk mitigation.[35] The threat to ICS was brought to the fore as a result of one of the most high-profile cyber attacks to date, known as Stuxnet. This was an attack on an Iranian nuclear fuel processing plant at Natanz, which has been widely attributed to the US and Israel.[36] Stuxnet was significant for a number of reasons but notably, it provided a 'proof of concept' that a software code-generated attack could be used to disrupt *physical* processes and destroy not only data but also physical components.[37] The attack was able to physically destroy the centrifuges used for uranium enrichment, whilst the system continued to report its status as 'normal' to the operators. The ability to remotely affect, for example, the electrical power of an airbase, or briefly disrupt the function of a number of navigation aids, if synchronised with other effects, might give an adversary an advantage that temporarily undermined the capability advantage of a fifth-generation system.

The F-35 programme consists of a large and immensely complex supply chain network, with 14,000 US suppliers[38] and 300,000 components sourced from 1,500 international suppliers.[39] Whilst the programme provides significant economic benefit for the F-35 partner nations, the level of complexity of the supply chain presents a potential cyber security risk. Collaboration between supply chain partners is a central tenet of supply chain operations, but without effective controls, exploit code could be inserted in the supply chain that could compromise the air system.[40]

This generic system-of-systems model of the F-35B Lightning aims to simply illustrate the potential for system vulnerability in the fifth-generation air force. Detailed vulnerability analysis for each platform and weapons system is now a routine activity in the UK,[41] and is used to inform senior risk owners to enable risk mitigation activity. However, the complex interconnected nature of systems makes effective holistic cyber defence a significant challenge for the fifth-generation air force. Accepting this complexity, there is a need to move on conceptually from the current approaches to cyber defence with a basis in information assurance, to an approach that embraces the concept of

mission assurance. Brad Bigelow highlights that rather than focussing entirely on cyber protection, there is a requirement to be able to still operate effectively in the absence of some cyber capabilities.[42] He notes the difference between 'cyber security, which strives to protect all information systems and assets', versus mission assurance, which 'seeks to ensure that the mission can be carried out even if some systems have failed.'[43] This echoes the view of Air Chief Marshal Sir Andrew Pulford, the former Chief of the Air Staff, who contended that 'we must have sufficient resilience to defend against its use by adversaries and develop our own measures to exploit cyber for gains in the Air environment.'[44] The implications of a 'day without space' have been widely debated[45], and the implications of a day without cyber attracts increasing attention from senior commanders.[46]

The post-1991 RMA debate precipitated a change to Western concepts of warfare, seeking to take advantage of advanced technologies. With a mix of highly capable platforms and systems, modern air forces employ this advantage when fighting against a wide range of adversaries up to and including those that may be considered 'near-peers'. However, the dependence upon space and cyberspace brings a level of risk to mission execution.[47] This necessitates a requirement to train and exercise based on the assumption that cyberspace will be contested, that the systems that contribute to our mission advantage may become unavailable at any point.[48] Exercising reversionary modes of operation in all aspects of air power delivery and Air C2 are vital to maintaining advantage, as noted in the RAF strategy, 'aircraft and systems will need to be able to operate in this increasingly contested and degraded environment and we must combat our adversaries' information and command and control systems.'[49]

OFFENSIVE AIR-CYBER INTEGRATION – HISTORICAL LESSONS

The former Chief of the Air Staff, Air Chief Marshal Sir Andrew Pulford, argued that 'the military importance of cyber, like that of the Air environment just over 100 years ago, is still relatively new and immature, with actors slow to grasp its offensive capability.'[50] The previous section discussed the importance of Air-Cyber Integration from the perspective of defensive cyber operations, but cyberspace also offers opportunities to exploit the vulnerabilities of adversaries through offensive cyber operations. For most nations that declare an offensive cyber capability, the details of that capability remain particularly sensitive. Unlike with conventional weapons technology, exposure of a state's cyber capabilities risks them becoming obsolete almost immediately. Whilst an adversary will always try to develop countermeasures to a kinetic weapon, the difference with specific knowledge of a cyber weapon is that it may allow the immediate nullification of its effects. For example, the adversary may close off network access, reconfigure the system or rapidly develop and deploy a software patch to overcome the vulnerability, thereby countering the capability and opportunity of the threat actor, and breaking the cyber kill chain. Despite the sensitivities around cyber capabilities, historical examples are instructive in understanding how cyber effects

might be employed. Effects delivered through cyberspace are often felt outside of the domain, most notably by impacting on the humans that use technology. However, in general, unlike kinetic effects, cyber effects do not directly have the potential to be violent.[51] Therefore they are likely to be supporting effects, rather than the main effort and may be temporary, be subtle in their impact on the adversary and be reversible.

The integration of cyber operations with air power is often debated conceptually, but there are a number of 'real world' examples that can be studied, with some of the earliest being during the 1999 Kosovo campaign, Operation Allied Force. Often cited as an example where air power was able to bring about victory independently,[52] author Fred Kaplan argues that cyber operations also played their small part in supporting the NATO air campaign.[53] At the strategic level, the US Department of Defense included a cyber line of operations in countering the Serbian strategic communications campaign. They were able to place remotely controlled devices in Serbian television transmitters and then switch off the transmitter and therefore interrupt transmissions at a time of their choosing. The devices were used to impair the ability of Serbian local television news channels to broadcast propaganda aimed at getting Serbian viewers to participate in anti-NATO demonstrations.[54] Kaplan's account does not offer sufficient detail to determine the means of attack with any degree of certainty. It is possible that this operation may have been an example of Electronic Warfare (EW), rather than cyber attack, but this in itself is edifying, in highlighting the conceptual and practical blurring between cyber operations and EW.

Perhaps of more direct relevance to the tactical air campaign was the ability to attack the Serbian air defence system by feeding false track information. This was synchronised specifically on occasions when planned sorties were operating at heights within the range of Serbian ground-based air defences. Kaplan argues that the 'deception had to be subtle, the radar had to be just a bit off, enough to make Serbian officers blame the miss on a mechanical flaw but not enough for them to suspect sabotage.'[55] If the effect had been too obvious there was a risk that the Serbs would switch from 'automatic guidance to manual control.'[56] It is unlikely that malicious code was inserted directly into the Serbian Surface to Air Missile (SAM) systems; the target was more likely to have been computers in the interconnected C2 systems.[57] Nor was it likely that the cyber effects employed were decisive in their own right, given the concomitant high levels of expenditure of anti-radiation missiles against early warning radars and SA-3 and SA-6 batteries.[58] However, it stands as an instructive early example of synchronising a cyber attack with an air attack. It also highlights the importance of understanding adversary systems in great detail in order to understand potential vulnerabilities. In this case, a detailed knowledge of the interconnectivity of the Ground Based Air Defence System needed to be accompanied by knowledge of enemy doctrine and techniques, tactics and procedures to ensure that likely response of the adversary could be assessed.

Kosovo also contributed a great example of a tactical air operation being combined and synchronised with a cyber-enabled information operation, designed to drive a wedge between the regular Yugoslav military, *Vojska Jugoslavije* (VJ), and the Ministry of Internal Affairs militia, *Ministarstvo Unutrasnjih Poslova* (MUP). Kaplan suggests that US intelligence agencies had obtained telephone and fax numbers for the headquarters of both organisations. Immediately prior to simultaneous air attacks on the VJ and MUP headquarters, whilst the aircraft were in flight, messages were sent to the VJ, warning them of the imminent attack. After both buildings were destroyed, the surviving MUP had heard that VJ officers had evacuated their HQ ahead of the attack and 'so began to suspect that VJ was collaborating with NATO.'[59] Whilst this simple example employed very basic cyber technology and techniques, it offers lessons that are particularly relevant to current operations. The ability to directly influence individuals and groups through cyberspace offers a potential supporting effect for air operations. Even if the adversary's C2 systems are difficult to penetrate, cyberspace offers the means to directly target decision makers through their personal online presence that could sow fear, uncertainty, or confusion at a critical moment.

Cyber operations during the Kosovo campaign were not all one-way traffic. Whilst the US was conducting attacks against Serbia, the Serbians were attacking the NATO HQ web and email servers.[60] NATO was subjected to the kind of Distributed Denial of Service (DDoS) attack that has become almost commonplace in more recent times but was relatively novel in 1999. Overall, Kosovo demonstrated the early use of nascent cyber capabilities, with the US European Commander stating 'we did more information warfare in this conflict than we have ever done before, and we proved the potential of it.'[61] It should be noted that US concepts and doctrine have evolved significantly since the late 1990s. During this period, the US used the terms 'information attack' to describe what might now be described as cyber attack. Conceptually, Information Warfare included: psychological operations; physical destruction; military deception; information attack; security measures; and electronic warfare.[62]

When the Israeli Air Force was tasked to destroy a nuclear processing plant under construction at Al Kibar, in Deir-ez-Zor, Syria in 2007, it faced the challenge of safely eluding the highly capable Syrian Integrated Air Defence System. The mission, known as Operation Orchard, was ostensibly a complete success for the Israelis, and despite a heightened level of surveillance by the Syrian air defence system, the attacking aircraft were not observed.[63] The success of the Israelis was reportedly due to the synchronisation of the air operation with both conventional electronic warfare jamming and a cyber operation that 'disrupted the data link connecting the radar with the screens of the radar operators.'[64] The supporting cyber elements of the operations purportedly included 'air-to-ground electronic attack,'[65] using Israeli capabilities 'similar to [a] network invasion capability that was developed by the US.'[66] Additionally, Fulghum

et al reported that 'there also were some higher-level, non-tactical penetrations, either direct or as diversions and spoofs, of the Syrian command-and-control capability, done through network attack.'[67]

Recent Russian military campaigns offer further examples of cyber effects being synchronised with a broader joint campaign. Jeffrey Carr argued that during the 2008 Russian campaign in Georgia, military action was coordinated with large numbers of 'patriotic hackers'. These hacktivists were coordinated through online forums that gave advice and guidance on how to download and use tools to carry out DDoS attacks. Hacktivists were given direction on target lists through the same forums, allegedly from members of groups with close ties to the Russian government.[68] He also highlighted differing levels of skill and sophistication within the hacktivist groups:

> *Those forum members who pinpointed application-level vulnerabilities and published target lists seemed to have moderate/high technical skill sets, whereas those carrying out the actual attacks appeared to have low/medium technical sophistication.*[69]

More recently Carr has argued that things have changed within Russia since 2008. There has been investment in cyber forces and whilst the Russian government could still call upon proxies for action in cyberspace, 'it has invested large sums of money to give its military and security services capabilities that are far beyond what they had in 2008.'[70] Since the crisis over Ukraine started in 2014, those studying the Russian approach have observed that Russia views cyberspace operations as part of a wider concept of Information Warfare, and Russian doctrine does not view cyberspace as a separate domain.[71] Giles notes that rather than cyberspace, Russia refers to 'information space' and 'includes in this space both computer and human information processing, in effect the cognitive domain.'[72] Russian doctrine embraces computer network operations alongside psychological operations and 'intelligence, counterintelligence, maskirovka, disinformation, electronic warfare, debilitation of communications, degradation of navigation support, psychological pressure, and destruction of enemy computer capabilities.'[73] Whilst Western doctrine on cyberspace includes human cognition, it is not central to cyberspace operations in the way it appears to be in Russia. Western doctrine on cyberspace such as Air-Cyber Integration aims to create greater convergence between cyberspace and 'traditional' warfighting. Giles argues that Russia is not faced with the challenge of convergence 'because – thanks to the holistic and integrated approach to information warfare – they never went through a process of divergence in the first place.'[74]

More broadly in the West, integrating cyber effects with other lines of operation has become almost commonplace. Cyber effects have reportedly been employed in Counter Insurgency Operations in Afghanistan, with one US General claiming that:

> *I was able to use my cyber operations against my adversary with great impact… I was able to get inside his nets, infect his command-and-control, and in fact defend myself against his almost constant incursions to get inside my wire, to affect my operations.*[75]

The case studies cited above provide instructive lessons on some of the issues in integrating cyber operations with those in the other domains. They demonstrate the close cooperation and synchronisation required between those planning and executing the cyber lines of operation, with those responsible for air or joint operations. Cyber operations and Electromagnetic Activity (EMA) have a degree of mutual dependence that means they must be planned jointly and closely synchronised. They also form an integral part of Joint Action and can contribute as alternatives to kinetic action, as part of a sequence of actions, or as a combination of actions against a complex target.[76] Planning the integration of cyber effects is in many ways similar to planning air or joint operations, but comes with specific challenges and nuances. Identifying and refining a target in cyberspace requires a similar approach to target systems analysis for employment of a kinetic weapon, although once the generic target set is identified, its refinement may require the support of specialist cyber operators, using a process similar to the generic 'Cyber Kill Chain' process described above. British and NATO targeting methodologies are centred upon the achievement of effects and require that assessment criteria are established as part of the planning process.[77] Assessment requires Measures of Performance (MoP) and Measures of Effectiveness (MoE) to be established as part of the criteria for targeting. For example, MoP might assess whether all the intended targets had been struck at their desired points of impact; a related MoE might be the extent to which striking those targets degraded the enemy's C2 capability. If it is not possible to measure the effectiveness of a particular attack, and its contribution to the Commander's overall objectives, there may be no value in attacking the target and expending resources or exposing crews to risk. The need for MoP and MoE is equally apposite in cyberspace, but arguably the achievement of meaningful measurement can be particularly challenging.[78] Whilst kinetic MoE is normally supported by a range of different sources of intelligence, the primary source is often post-strike imagery, which can give the Commander a reasonable degree of assurance of functional destruction or degradation of an enemy capability, which contributes to his assessment of success criteria. However, the use of imagery is generally meaningless for a cyber target, so other means of supporting assessment are required. In some cases, the process of the 'Cyber Kill Chain' described above might be required to establish both the means of attack and separately, the means of MoE.

The example of Stuxnet, discussed above, highlights another issue of cyber targeting, that of unintended consequences. The possibility of unintended consequences is important in targeting across all the domains, equally so in cyberspace. Stuxnet was aimed at a very specific target and only became known because it spread beyond the

intended target and infected systems around the world.[79] This presents a different collateral damage challenge to that experienced in kinetic targeting, but one that requires careful consideration. A cyber capability whose effects cannot be controlled or contained might risk infecting friendly and neutral systems, as well as those of the enemy. As a consequence, their use might not be acceptable from a legal or policy perspective.

Effects delivered in and through cyberspace may be reversible and ephemeral in nature, although in some case, the resulting outcomes may not be.[80] It may be that a piece of exploit code can be overcome by a system reboot, or as described above, through the application of a patch to remove a vulnerability. In any given set of circumstances this may be an advantage or a disadvantage. The use of a kinetic effect may be preferred if the requirement is to put a target beyond use for a longer period, but a cyber option may be selected if the requirement is for short term disruption, or where there is a desire to avoid physical destruction, such as when collateral damage estimates indicate the likelihood of unacceptable non-combatant casualties.

Debate around attacks in and through cyberspace often turns to the problem of attribution. The degree to which the source of an attack can be attributed may determine the threshold of any response. Considerations of attribution apply equally to both offensive and defensive cyber operations. The ability to determine where a cyber effect comes from, through positive identification of the threat actor, is often seen as a purely technical problem, and one that is both difficult and 'binary' in that it 'can either be solved, or not be solved.'[81] However, Rid and Buchanan argue for a much more nuanced approach that suggests that technical evidence is only one element of the attribution puzzle, which requires interrelated analysis at the technical (or tactical) level and the operational and strategic context of an attack.[82] They also argue that 'attribution is what states make of it.'[83] In some cases during an ongoing conflict, even without technical evidence, attribution may be obvious, although there is clearly scope for intentional deception. However, the strategy of an attacker may be specifically aimed at avoiding attribution and blurring the evidence at the technical, operational and strategic levels. It has been argued that this is a feature of 'hybrid warfare', as seen through the 'unavowed nature of Russian military intervention in Ukraine.'[84] Plausible deniability has the potential to offer an asymmetric advantage; if, for example, an attack on a NATO member might invoke an Article V response, the inability to achieve agreement on attribution may cause discord between NATO members.[85]

Whilst the specific means of conducting offensive cyber operations are likely to remain closely protected, historical examples are instructive in aiding the understanding of how they might be integrated with air power. The article now turns to perhaps the most important element of cyberspace operations and Air-Cyber

Integration, which is that of having sufficient skilled cyber operators to lead, plan and execute cyber operations.

CYBERSPACE OPERATORS

The discussion of Air-Cyber Integration in this article highlights the need for people who can operate credibly and effectively in both the air and cyberspace domains. Despite the fact that cyberspace is associated with technology, successfully integrating it with the other domains is very much a human challenge.

The RAF has always been justifiably proud of its heritage as the most technical of the Services. Lord Trenchard's vision for the RAF was underpinned by detailed technical and operational knowledge and skills imparted in his Cranwell Cadets and Halton Apprentices. In setting out his initial vision for the Independent Air Force in 1919, Trenchard stressed that the future success of the RAF would depend upon recognising the 'extreme importance of training.'[86] He insisted that the officers of the new Service should 'be required to select the particular technical subject they will make their special study during their subsequent career.'[87] Trenchard's legacy of a highly-skilled and technical Service has endured into the RAF's second century, and the need for tactical and operational acumen underpinned by technical expertise extends to cyberspace. Since 2010, the senior leadership of the RAF has recognised that in its second century, the RAF requires 'a highly professional team, staffed by airmen and airwomen who have a deeply specialist expertise in the complexity of the air, space and cyber domains.'[88] Air-Cyber Integration requires a combination of specialist cyber operators along with commanders and staff officers who have a detailed understanding of, and experience of operating within, both the air and the cyberspace domains.

Skilled and experienced cyber operators are required, both to assure the delivery of air power, and to contribute to a range of cyber missions under the Joint Commander. There are arguably three distinct groups of 'cyber operator'. At the most basic level, *all military personnel* operate within the cyber domain, from using networked weapon systems, command and control and information systems, network enabled logistics systems and most forms of communication. Increasingly, all personnel routinely engage with advanced military technology that is vulnerable through cyberspace; however, potential adversaries are subject to similar vulnerabilities, offering a range of potential opportunities in and through cyberspace. All military personnel need an awareness of cyberspace and in particular how their actions can create vulnerabilities that may be exploited by an adversary. Cyberspace also enables information to flow with a speed and reach that was previously unimaginable. The implications are that actions online at an organisational and individual level play a key role in establishing and maintaining the 'strategic narrative'. Small incidents that would have been insignificant in the past can have a strategic effect. Even within their personal lives, military personnel interact

with cyberspace through a range of tools, including social media, opening them up to a range of cyber vulnerabilities. As a consequence, military training and education must include core cyber-specific skills and behaviours throughout the military career. For personnel delivering all aspects of air power, cyber skills are increasingly becoming core military skills.

The second group of 'cyber operator' comprises the *cyber specialists*. Cyberspace has been acknowledged as a domain in its own right and just like in the Maritime, Land and Air domains, but there is clearly not just one 'cyber skill set'. UK doctrine acknowledges four specific cyber operations roles: offensive cyber operations (OCO); defensive cyber operations (DCO) (including active defence); cyber intelligence, surveillance and reconnaissance (cyber ISR); and cyber operational preparation of the environment (cyber OPE).[89] Cyber specialists execute missions across these four roles and are cyber domain experts with skills that are underpinned by deep technical knowledge of the domain, coupled with operational expertise. Cyber ISR specialists can carry out analysis of cyber target systems, or the cyber aspects of a physical system. They may also be responsible for producing cyber threat intelligence to allow assessment of adversary capability and intent in cyberspace. DCO cyber specialists are responsible for operating Security Information and Event Management (SIEM) systems, and carrying out vulnerability analysis, penetration testing, and malware analysis. These operators are required to respond to adversary cyber action and deliver a range of measures to assure the delivery of air power. Additionally, OCO specialists employ capabilities to generate a range of effects, that can be integrated with missions and effects from the Maritime, Land and Air domains. Specialist cyber operators predominately have a technical and/or intelligence analysis background, as the entry level into most specialist cyber roles requires a deep understanding of how the domain functions. However, as specialist cyber operators in both offensive and defensive roles, their development must be focussed on operations; there is a clear distinction between cyber operations and the provision of IT services, even though they are synergistic roles and both might require a detailed fundamental knowledge of cyberspace. The skills of the specialist cadre are highly sought after in the civilian market, adding to the challenges involved in recruitment and retention.

Cyber specialists not only need to operate capabilities that disrupt, degrade, or destroy the physical component of enemy fighting power, but also those that impact upon the moral component. The skills required to attack a network differ from those required for online engagement. It is likely that engaging with target audiences online may become as important as Information Operations through print, radio broadcast and face-to-face Key Leader Engagement. It is as yet unclear if there is a specific mission for airmen in this area of operations, with the mission currently falling predominantly to the Land component in the UK.[90] However, there may be a role for

airmen in planning and synchronising this type of non-kinetic activity with Air effects within the Air Tasking Order (ATO) cycle. In practice, the close interdependence between cyber operations, Information Operations, Psychological Operations, and kinetic operations, requires close synchronisation.[91] In examining the specific information threat to the UK and NATO from Russia, the House of Commons Defence Committee expressed concern over the lack of a UK strategy to counter Russian disinformation.[92] The Committee argued that the weight of effort and resource that Russia applies to its information operations requires a much greater response from the UK and NATO.

The third group of 'cyber operators' are the *commanders and staff officers* that are suitably qualified and experienced to plan and lead cyberspace operations as part of joint operations, and to develop cyber capability, doctrine, and tactics. This group needs an intuitive understanding of the domain and the types of capabilities that could potentially be at the senior commander's disposal. As their careers progress, they need to develop cyber-domain breadth, whilst retaining a degree of depth. Bringing air domain tactical expertise to cyber operations is vital for integration, as is the need for detailed understanding of the cyber domain. If cyber specialist officers are to be successfully employed in the planning and synchronisation of cyber effects as part of a joint operation, they must first possess a knowledge of doctrine and experience of planning at the component and joint level.[93]

Singer and Friedman identify a knowledge gap between the specialists and the commanders that must be bridged due to its significant implications.[94] They highlight that a US General described 'how "understanding cyber is now a command responsibility," as it affects almost every part of modern war.'[95] This view is supported by a former US Cyber Command J3 (Director of Operations), Major General Brett Williams, an F-15C pilot by background, who argues that 'there is too much at stake for our senior leaders not to understand cyberspace operations in the same way they understand operations in the other domains.'[96] In order for airmen and airwomen to enhance their understanding of cyberspace, there is a fundamental requirement to develop a 'feel' for the domain. To dismiss the importance of the technical detail in cyberspace risks those in cyber roles lacking both credibility and effectiveness. Senior Air commanders are no longer the 'tactical experts' that they were in their early careers, but they grow and retain an intuitive understanding of the air domain, capabilities and limitations of air power as an instrument in the joint campaign. Poirier and Lotspeich argue that the same must be true with cyberspace:

> *Just as a pilot must have knowledge of aerodynamic fundamentals to understand the performance and limitations of his weapon system, so must cyber warriors possess a foundational grasp of the cyber domain to employ cyber weapon systems properly.*[97]

Developing this domain expertise is crucial in realising the aim that 'cyber must be "mainstreamed" so that commanders, as well as specialists, understand instinctively how to conduct offensive and defensive cyber at both the strategic and tactical levels.'[98] However, the process of 'mainstreaming' is a conceptual challenge as much as a practical one. It requires an operational mind-set and an ability to understand, but crucially, think *above* the technical details of networks. Williams, argues that 'we have a pressing need to develop cyberspace operators who are credible and effective in the J3 (operations) and J5 (strategic plans and policy)'[99] functional areas. This view is reinforced by the Commanding General of US Army Cyber, who acknowledges the requirement to develop personnel with 'credible backgrounds with degrees in cyber related fields', but also that 'it's just not about being a great computer expert or hacker, this is about your ability to organize these capabilities in time and space against a very specific mission set that is actually in support of the armed forces... and the conduct of their larger mission.'[100]

Developing the appropriate level of expertise takes time and experience and Williams argues that 'cyberspace officers should spend their first 10 years becoming tactically proficient in all aspects of cyberspace operations.'[101] This, however, presents a different challenge in that those tactically proficient cyber operators do not then develop the same level of tactical proficiency in the other domains, such as Air. Arguably, the requirement is a suitable blend of both officers that are deep experts in cyber but retain an underpinning knowledge of air operations, and tactical air power specialists who are also exposed to cyber operations throughout their careers. Developing expertise in airmen, particularly future commanders, requires a combination of relevant Professional Military Education (PME), exposure to cyberspace planning during exercises and in some cases, full tours in cyber roles. Conversely, for those who specialise in cyberspace, the air power aspects of PME, and ongoing exposure to air operations are a necessary part of their development.

The UK National Cyber Security Strategy stresses the need for cyber specialists to work in partnership across government. This is underpinned by financial and organisational investment in the National Offensive Cyber Programme 'the partnership between the Ministry of Defence and GCHQ that is harnessing the skills and talents of both organisations to deliver the tools, techniques and tradecraft required.'[102] This Strategy therefore requires all three of the Armed Services to provide personnel with the attributes to be effective cyber operators, planners and commanders. Fundamentally, the value of cyberspace operations lies in their integration with operations in the other domains through delivering objectives as part of a joint campaign.[103] As a consequence, bringing operational experience of Land, Sea, Air, or Space to Cyberspace is a significant advantage. Although not solely a challenge for airmen, they have their part to play, as a former Chief of the Air Staff, Air Chief Marshal Sir Stephen Dalton highlighted: 'the technological focus and dependency of the RAF

has placed us squarely in the forefront of conceptual as well as technical development for both space and cyberspace arenas.'[104]

Developing sufficient cyber specialists and appropriately skilled cyber leaders, poses a particular challenge. The need to recruit, train, and retain personnel in military cyberspace roles sits in a context of a global cyber security workforce shortage that is predicted to reach 1.8 million by 2022.[105] In mitigating the competition from the civilian cyber security market, the MoD has acknowledged that its cadre of cyber professionals must include reservists.[106] This is consistent with a broader drive to ensure that reductions in regular force numbers are offset by an appropriate mix of the 'Whole Force', regular military, reservist, civil servant and contractor.[107] In generating a sustainable number of cyber professionals, traditional approaches must be adapted, with a need to 'be imaginative in recruiting, managing and retaining the Defence cyber cadre.'[108] Being 'imaginative' arguably requires the application of a range of measures to attract and retain talent. Military cyber operators are often motivated by the challenge, interest and operational relevance of a cyber career and generally have a strong desire to remain in cyber specialist employment.[109] Other nations face similar challenges, with the US Army encouraging transfers from other branches, primarily from those with Science, Technology, Engineering and Maths (STEM) education backgrounds.[110] An issue identified within the US military is that developing deep cyber experience may impose a career disadvantage on individuals in a culture that eschews technical competence in favour of more mainstream attributes. Conti and Surdu cite several examples of this and argue that 'some cyberwarfare soldiers, sailors, and airmen who seek to make a career of the military go to great lengths to mask their technical expertise and assignments from promotion boards by making their personnel evaluations appear as mainstream as possible.'[111] It is clear that appropriately rewarding career development and progression is an important factor in retention, particularly when external opportunities in the civilian employment market abound.

When the UK Secretary of State for Defence made a public announcement regarding the creation of a Joint Cyber Reserves Unit in 2013, there was significant media discussion regarding whether this new Cyber Reserve organisation would include 'convicted hackers' or those that were unable to meet the physical fitness standards of the Armed Forces.[112] This might include recruiting those who have the specific skills required for cyber specialist roles but are limited in the scope of their employment, if for example they suffer from an illness or injury that prevents them carrying out a full range of military duties. The former head of the Defence Cyber Security Programme, General Jonathan Shaw argued for the extensive use of reserves in UK cyber roles:

> *We need a cyber reserve and that reserve should be largely civilian... Don't think camouflage, short-back-and-sides and weapons training. It's ponytails, earrings and thick spectacles – that's what we need.*[113]

Although part of the requirement may be satisfied by civilians and those that do not conform to military norms, there is a danger that this type of pronouncement from a senior officer perpetuates stereotypes that are often more myth than fact. Skill and aptitude for cyber operations and military bearing and ethos are not mutually exclusive. The armed forces attract people with diverse backgrounds and personality types, but the basic requirements beyond technical aptitude remain teamwork and discipline. Some cyber operators, like those from other specialisations, need to deploy on operations and need the underpinning military skills to do so. Despite popular myth, not all cyberspace targets can be reached from 'darkened rooms' in the UK by the stereotypical 'hacker in a hoodie'; integrating and delivering cyber operations will often require a forward presence in the area of operations.[114] There is therefore a requirement for military and civilian, regular and reserve to fill a wide range of cyber roles. Estonia has recruited a Cyber Unit as part of its National Defence League, which provides a reservist force that aims to defend the nation from attack in cyberspace.[115] This reliance on Reserves is arguably an effective way to generate the mass of personnel required in an affordable and achievable manner.

Furthermore, the idea of employing convicted hackers based on their purported advanced technical skill alone is also questionable; trust and reliability are fundamental requirements, as is the requirement to achieve and maintain a security clearance. The US Army Cyber Commander 'views people as the centerpiece *[sic]* to cyberspace characterized by high degrees of competence *and character*' (emphasis added).[116] Whilst some former offenders may be rehabilitated, the recruits likely to be most effective in cyber roles across the Whole Force are arguably those with a strong technical aptitude, coupled with the traditional military attributes of discipline, teamwork, integrity and service.

CONCLUSION

In conclusion, this article has considered some general people, process and technology issues related to the integration of cyberspace with air power. Explanations of the terminology related to attacks in cyberspace enabled the discussion of both defensive and offensive cyber operations. Just as the study and practice of air power has produced a distinct lexicon, so too has cyberspace. For airmen to be credible commanders of cyber operations, and for staff to enable Air-Cyber Integration, they must be equipped to understand the principles of cyberspace, as well as they understand their native air domain.

The twenty-first century is likely to be characterised by a contested cyber domain. The paper uses the cyber defence of the Lightning merely as an example of where threats might arise, beyond the platform, in the interconnected system-of-systems related to its operation and support. The complexity of systems in the twenty-first century requires a holistic examination of cyberspace threats and commensurate

mitigation, with a focus on assuring the delivery of the air mission. However, cyberspace is not solely a domain filled with new threats for air power; it offers the potential to give the commander additional options for delivering effects. By integrating cyber effects with air power, the range of options available to the commander increases, where close synchronisation can enhance air power effects and provide options that may be ephemeral and reversible.

The success of the RAF in capitalising on the opportunities of Air-Cyber Integration is highly dependent upon the skill of its people. Air power missions are underpinned by cyberspace, therefore being competent in operating effectively in cyberspace is a core requirement for all airmen and women. The RAF also has a need to develop and retain sufficient numbers of specialist cyber operators to contribute to Air-Cyber Integration, and to provide a contribution to a range of cyber missions under the Joint Commander. Senior commanders and their staff already have a requirement and a responsibility to be comfortable and competent operating in the cyber domain, therefore developing their successors requires that they gain experience in cyberspace as well as the physical domains. The first century of air power was characterised by pushing the physical and technological boundaries of the air domain. This is likely to continue in its second century, with the added complexity of dependence upon cyberspace. The success of air power at the start of its second hundred years is closely linked to achieving success in the cyber domain.

NOTES

[1] William J Poirier and James Lotspeich, "Air Force Cyber Warfare: Now and the Future," *Air and Space Power Journal* 27, no. 5 (2013): 92.
[2] DCDC, *Joint Doctrine Publication 0-30: UK Air and Space Power*, 2nd Ed. (Shrivenham: Development, Concepts and Doctrine Centre (DCDC), 2017), 54, **https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/668710/doctrine_uk_air_space_power_jdp_0_30.pdf**.
[3] Ronald R Fogleman, "Conerstones of Information Warfare" (Washington, DC: US Air Force, 1997).
[4] UK Ministry of Defence, "Joint Concept Note 1/17: Future Force Concept," 2017, 19.
[5] The UK has undergone some conceptual debate regarding the use of the term 'Domain' and 'Environment'. Joint Concept Note 1/14 referred to maritime, land, air, space and cyber as 'environments', not 'domains'. Joint Concept Note 1/17 returns to the use of 'maritime, land, air, space and cyber domains', underpinned by the information environment, and is consistent with current terminology in Allied concepts and doctrine.
[6] HM Government, "National Cyber Security Strategy 2016-2021," 2016, 15, **https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf**.
[7] DCDC, *Cyber Primer*, 2nd ed. (Shrivenham: Development, Concepts and Doctrine Centre

(DCDC), 2016), 1, **https://www.gov.uk/government/publications/cyber-primer**.
[8] Ibid., 20.
[9] NCSC, "Common Cyber Attacks: Reducing The Impact" (London, 2016), 6, **https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf**.
[10] Ibid., 3.
[11] P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), 115.
[12] Zheng Bu, "Zero-Day Attacks Are Not the Same as Zero-Day Vulnerabilities," FireEye Inc, 2014, **https://www.fireeye.com/blog/executive-perspective/2014/04/zero-day-attacks-are-not-the-same-as-zero-day-vulnerabilities.html**.
[13] Kim Zetter, "Countdown to Zero Day: STUXNET and the Launch of the World's First Digital Weapon" (New York, NY: Crown Publishing, 2014), 6.
[14] Ibid., 221–22.
[15] David E Sanger, "Obama Lets N.S.A. Exploit Some Internet Flaws, Officials Say," New York Times, 2014, **https://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html**.
[16] Wassenaar Arrangement Secretariat, "Public Statement 2013 Plenary Meeting of The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies" (Vienna, Austria, 2013), **http://www.wassenaar.org**.
[17] Lockheed Martin, "Cyber Kill Chain® · Lockheed Martin," 2018, **https://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html**.
[18] Lawrence Freedman, "War Designed for One," *The World Today* 53, no. 8/9 (1997): 217.
[19] Leo Davies, *A Fifth-Generation Air Force: Alliance Structures and Networked Capabilities from an Australian Perspective* (Washington, DC: Center for Strategic & International Studies, 2017), **https://www.csis.org/events/fifth-generation-air-force-alliance-structures-and-networked-capabilities-australian**.
[20] Royal Air Force, "Royal Air Force Strategy: Delivering a World-Class Air Force" (High Wycombe: Headquarters Air Command, 2017), 28.
[21] Ibid.
[22] Giulio Douhet, *Command of the Air*, ed. Trans. Dino Ferrari (Office of Air Force History, 1983), 34.
[23] Lockheed Martin, "F-35 Mission Systems | F-35 Lightning II," 2017, **https://www.f35.com/about/capabilities/missionsystems**.
[24] Pete Cooper, *Aviation Cybersecurity - Finding Lift, Minimizing Drag* (Washington, DC: Atlantic Council, 2017), 23.
[25] Lockheed Martin, "F-35 Software Development," 2017, **https://www.f35.com/about/life-cycle/software**.
[26] Cooper, *Aviation Cybersecurity - Finding Lift, Minimizing Drag*, 23.
[27] Lockheed Martin, "Autonomic Logistics Information System," 2017, **http://www.lockheedmartin.co.uk/us/products/ALIS.html**.

[28] Ibid.
[29] Alexi Mostrous and Deborah Haynes, "F-35 Investigation: Jets Are Overbudget, Unreliable and Vulnerable to Cyberattacks," The Times, 2017, https://www.thetimes.co.uk/article/jets-are-overbudget-unreliable-and-vulnerable-to-cyberattacks-v3gt8dcbb.
[30] HM Government, "Defence Committee Unclear for Take-off? F-35 Procurement" (London, 2017), 18, https://publications.parliament.uk/pa/cm201719/cmselect/cmdfence/326/326.pdf.
[31] Ibid.
[32] Shaun Harvey, "Unglamorous Awakenings: How the UK Developed Its Approach to Cyber," in *A Fierce Domain: Conflict in Cyberspace 1986 to 2012*, ed. Jason Healey (Washington, DC: Atlantic Books, 2013), 260.
[33] DCDC, "Joint Doctrine Note 1/18: Cyber and Electromagnetic Activities" (Shrivenham: Development, Concepts and Doctrine Centre (DCDC), 2018), 19, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf.
[34] PCI Gases, "On-Site LOX/LIN Generator," 2018, https://www.pcigases.com/wp-content/uploads/2015/11/GAMMA_LOX_product_LowRes-0613.pdf.
[35] Zetter, "Countdown to Zero Day: STUXNET and the Launch of the World's First Digital Weapon," 134.
[36] Ibid., 332–33.
[37] Ibid., 164.
[38] Lockheed Martin, "F-35 Economic Impact," 2017, https://www.f35.com/about/economic-impact.
[39] Lockheed Martin, "F-35 Fast Facts," 2017, https://www.f35.com/about/fast-facts.
[40] G. E. Smith et al., "A Critical Balance: Collaboration and Security in the IT-Enabled Supply Chain," *International Journal of Production Research* 45, no. 11 (2007): 2597, https://doi.org/10.1080/00207540601020544.
[41] DCDC, *Joint Doctrine Publication 0-30: UK Air and Space Power*, 2nd Ed (Shrivenham: Development, Concepts and Doctrine Centre (DCDC), 2017), 54, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/668710/doctrine_uk_air_space_power_jdp_0_30.pdf.
[42] Brad Bigelow, "Mission Assurance: Shifting the Focus of Cyber Defence," in *Defending the Core: 2017 9th International Conference on Cyber Conflict*, ed. H. Rõigas et al. (Tallinn: NATO CCD COE, 2017).
[43] Ibid., 48.
[44] Andrew Pulford, "Two Decades at the Chuo Keiba," *Air Commanders' Dialogue Japan*, 2014, 9.
[45] Ed Morris et al., "A Day Without Space: Economic and National Security Ramifications," 2008, http://marshall.org/wp-content/uploads/2013/08/Day-without-Space-Oct-16-2008.pdf.
[46] US Department of Defense, "A Day Without Space And Cyber On The Battlefield,

Operating In Today's Multi Domain Environment" (The Joint Forces Channel, 2016), **https://www.youtube.com/watch?v=0eI_KyO8Vt4**.

[47] For an excellent fictional account underpinned by a detailed understanding of technology and strategic thinking see Singer, P.W. and Cole, A. (2015) *Ghost Fleet: A Novel of the Next World War*, Kindle Edi. Beaconsfield: Canelo Digital Publishing.

[48] Bigelow, "Mission Assurance: Shifting the Focus of Cyber Defence," 49.

[49] Royal Air Force, "Royal Air Force Strategy: Delivering a World-Class Air Force," 28.

[50] Pulford, "Two Decades at the Chuo Keiba," 8.

[51] Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst, 2013), 19–21.

[52] Benjamin S. Lambeth, "NATO's Air War for Kosovo," 2001, 220, **https://www.rand.org/pubs/monograph_reports/MR1365.html**.

[53] Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York, NY: Simon & Schuster, 2016), 107–118.

[54] Ibid., 111–12.

[55] Ibid., 114.

[56] Ibid.

[57] Lambeth, "NATO's Air War for Kosovo," 112.

[58] Ibid., 110.

[59] Kaplan, *Dark Territory: The Secret History of Cyber War*, 114.

[60] Dan Verton, "Serbs Launch Cyberattack on NATO," FCW, 1999, **https://fcw.com/articles/1999/04/04/serbs-launch-cyberattack-on-nato.aspx**.

[61] Lambeth, "NATO's Air War for Kosovo," 112.

[62] Fogleman, "Conerstones of Information Warfare," 4.

[63] Kaplan, *Dark Territory: The Secret History of Cyber War*, 160–61.

[64] Ibid., 161.

[65] Zetter, "Countdown to Zero Day: STUXNET and the Launch of the World's First Digital Weapon," 218.

[66] David A. Fulghum, Robert Wall, and Amy Butler, "Israel Shows Electronic Prowess," Aviation Week, 2007, **https://warsclerotic.com/2010/09/28/israel-shows-electronic-prowess/**.

[67] Fulghum, Wall and Butler (2007)

[68] Jeffrey Carr, *Inside Cyber Warfare*, First (Sebastopol, CA: O'Reilly Media, 2010), 17.

[69] Ibid., 16.

[70] Jeffrey Carr, "Digital Dao: Russian Cyber Warfare Capabilities in 2014 (We Aren't in Georgia Anymore)," accessed May 31, 2015, **http://jeffreycarr.blogspot.co.uk/2014/03/russian-cyber-warfare-capabilities-in.html**.

[71] Keir Giles, "Handbook of Russian Information Warfare," *NATO Defence College NDC Fellowship Monograph Series* 9 (2016): 6–7.

[72] Ibid., 9.

[73] Ibid., 6.

[74] Ibid., 69.

[75] Associated Press, "U.S. General: We Hacked the Enemy in Afghanistan," Politico, 2012,

https://www.politico.com/story/2012/08/us-general-we-hacked-the-enemy-in-afghanistan-080098.
[76] DCDC, "Joint Doctrine Note 1/18: Cyber and Electromagnetic Activities," 43–44.
[77] NATO, "AJP-3.3: Allied Joint Doctrine Publication for Air and Space Operations" (Brussels: NATO Standardization Office (NSO), 2016), 4–8, https://www.japcc.org/wp-content/uploads/AJP-3.3-EDB-V1-E.pdf.
[78] Steven J Anderson, *Airpower Lessons for an Air Force Cyberpower Targeting Theory*, 2016, 120, https://www.hsdl.org/?view&did=797492.
[79] Ibid.
[80] Pulford, "Two Decades at the Chuo Keiba," 14.
[81] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *The Journal of Strategic Studies* 38, no. 1–2 (2014): 6, https://doi.org/10.1080/01402390.2014.977382.
[82] Ibid., 9.
[83] Ibid., 7.
[84] Keir Giles, "Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power" (London, 2016), 49, https://www.chathamhouse.org/sites/files/chathamhouse/publications/2016-03-russia-new-tools-giles.pdf.
[85] Ibid.
[86] Hugh Trenchard, "Memorandum by the Chief of the Air Staff," *Air Power Review, 95th Anniversary Special Edition 2013* (1919), 261, http://airpowerstudies.co.uk/sitebuildercontent/sitebuilderfiles/apr-95th-anniversary.pdf.
[87] Ibid., 263.
[88] Stephen Dalton, "Meeting the Challenge," Air Power Conference 2010, 2010, https://www.raf.mod.uk/rafcms/mediafiles/5E9564D6_5056_A318_A8236B2CB11CCFA4.doc.
[89] DCDC, "Joint Doctrine Note 1/18: Cyber and Electromagnetic Activities," 15.
[90] HM Government, "Russia: Implications for UK Defence and Security" (London, 2016), 36–37, https://publications.parliament.uk/pa/cm201617/cmselect/cmdfence/107/107.pdf.
[91] DCDC, "Joint Doctrine Note 1/18: Cyber and Electromagnetic Activities," 16.
[92] HM Government, "Russia: Implications for UK Defence and Security," 37.
[93] Jason M Bender, "The Cyberspace Operations Planner," Small Wars Journal, 2013, http://smallwarsjournal.com/jrnl/art/the-cyberspace-operations-planner.
[94] Singer and Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, 4–6.
[95] Ibid., 6.
[96] Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Forces Quarterly* 73 (2014): 13.
[97] Poirier and Lotspeich (2013, p.92)
[98] DCDC, *Joint Concept Note 1/14: Defence Joint Operating Concept* (Shrivenham: Development, Concepts and Doctrine Centre (DCDC), 2014), 4–13, http://xtlearn.net/Files/Users/ceri/WO/20140319-dcdc_jcn_1_14_djoc-U.pdf?zoom=80%2525.
[99] Williams, "The Joint Force Commander's Guide to Cyberspace Operations," 14.

[100] Pomerleau, "Army Cyber Chief Outlines Key Challenges, Goals."
[101] Williams, "The Joint Force Commander's Guide to Cyberspace Operations," 13.
[102] HM Government, "National Cyber Security Strategy 2016-2021," 51.
[103] Williams, "The Joint Force Commander's Guide to Cyberspace Operations," 13.
[104] Stephen Dalton, "Air Power in Ages of Austerity," Wilbur & Orville Wright lecture to the Royal Aeronautical Society, 2009, http://www.raf.mod.uk/rafcms/mediafiles/EA27D125_5056_A318_A8289A46DF0DCB91.pdf.
[105] Frost & Sullivan, "2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk," 2017, 2, https://iamcybersafe.org/gisws/.
[106] Sophie Curtis, "UK to Create 'cyber Strike Force' - Telegraph," The Telegraph, 2013, http://www.telegraph.co.uk/technology/internet-security/10343652/UK-to-create-cyber-strike-force.html.
[107] John Louth and Trevor Taylor, "Beyond the Whole Force," *RUSI*, 2015, 14–16, https://rusi.org/sites/default/files/201510_op_beyond_the_whole_force.pdf.
[108] DCDC, *Joint Concept Note 1/14: Defence Joint Operating Concept*, 4–13.
[109] Paul Withers, "How Can the Royal Air Force Sustain and Grow Its Cadre of Cyber Professionals?" (Shrivenham, 2017). (Unpublished study as partial fulfilment of the requirements of the MSc Cyberspace Operations, Cranfield University).
[110] Jim Tice, "Attention Officers: Sign up Soon for Cyber Transfers," Army Times, 2015, https://www.armytimes.com/news/your-army/2015/04/16/attention-officers-sign-up-soon-for-cyber-transfers/.
[111] Gregory Conti and John Surdu, "Army, Navy, Air Force, and Cyber — Is It Time for a Cyberwarfare Branch of Military?," *IA Newsletter* 12, no. 1 (2009): 16, http://iac.dtic.mil/iatac.
[112] BBC, "UK Cyber Defence Unit 'May Include Convicted Hackers,'" 2013, http://www.bbc.co.uk/news/technology-24613376.
[113] David Blair, "Estonia Recruits Volunteer Army of 'Cyber Warriors,'" The Telegraph, 2015, http://www.telegraph.co.uk/news/worldnews/europe/estonia/11564163/Estonia-recruits-volunteer-army-of-cyber-warriors.html.
[114] Nicole Gallucci, "We Need to Talk about All These Absurd Stock Photos of Hackers," Mashable, 2017, https://mashable.com/2017/05/15/horrible-hacker-stock-photos/#3cI_KI_Mcmq0.
[115] Sharon L. Cardash, Frank J. Cilluffo, and Rain Ottis, "Estonia's Cyber Defence League: A Model for the United States?," *Studies in Conflict & Terrorism* 36, no. 9 (September 2013): 777–87, https://doi.org/10.1080/1057610X.2013.813273.
[116] Pomerleau, "Army Cyber Chief Outlines Key Challenges, Goals."