Military Aviation's Cyber Challenge; Are Cyber-Vulnerabilities a Credible Threat to a Modern Air Force?

(Chief of the Air Staff's Henderson Fellowship Dissertation)

By Squadron Leader Daniel Lydiate

Biography: Squadron Leader Daniel Lydiate is a Provost Officer with broad operational experience currently serving within Information Systems and Services (ISS) at MOD Corsham. Having undertaken a MSc with the University of Leicester, and the CAS' Henderson Fellowship to study an MA at the University of Exeter, he is continuing his current focus on cyber-related research by completing an MSc in Cyber Defence with Cranfield University.

Abstract: This article explores military aviation's contemporary cyber challenge by asking whether cyber-vulnerabilities are a credible threat to a modern air force. Following a discussion of the concepts, the question is developed through an analysis of four aspects of air operations: systems, infrastructure, supply chains and personnel. Although cyber-security concerns are identified within all, the article identifies that systems and the supply chain are where considerable cyber-security concern lies. Building on this, the article recommends that the strategic leadership of air forces must invest in reflective in-depth study to understand the problems and identify sources of mitigation. If they do, management of the issues may be possible. If they do not, the strategic relevance of modern air power may be destroyed by the systematic exploitation of military aviation's cyber-vulnerabilities.

Introduction

The article explores military aviation's contemporary cyber challenge by asking whether cyber-vulnerabilities are a credible threat to a modern air force. Beginning with a discussion of the relevant concepts, the article will highlight the requirement to understand cyber-vulnerabilities within the context of air power. To achieve this, the subject will be examined through an analysis of four key aspects of contemporary air operations: systems, infrastructure, supply chains and personnel.

Initially considering systems, it will be noted that within this complex area the human element is being increasingly supplanted by a reliance on the processing of digital information. To address whether this is of concern, the article will consider two key military aviation systems: Unmanned Aerial Vehicles (UAV) and the F-35's Autonomic Logistics Information System (ALIS). Through identifying mounting evidence that systems such as these are susceptible to cyber-attack, it will be concluded that the vulnerability of systems in modern aviation will continue to be of concern.

Moving next to infrastructure, it will be argued that, unlike its sister Services, the impermanence of aviation makes air forces uniquely dependent on infrastructure. Combined with modern Royal Air Force infrastructure's reliance on information systems, the ability of cyber-attack to circumnavigate traditional security will be discussed. Further, examining specific examples, it will be concluded that the cyber-threat to an air force's infrastructure is important but, due to available sources of mitigation, is not the most pressing vulnerability within military aviation's contemporary cyber-challenge.

In the third area of supply chains, the article will identify an issue of greater concern. Commenting on the complexities created by aviation's modern supply chains, the F-35 will be cited as an example before discussing the standards UK Defence is employing to secure its supply chains. Having done so, it will be concluded that with these standards falling short of the contemporary cyber-threat, supply chains are an area that is placing the viability of modern military aviation at risk.

In the final area – an air force's personnel – the article will comment that this 'beating heart' of an organisation plays an important role in security. Entwined with the delivery of air power at every step, it will be noted that people can cause security breaches either maliciously or, more often, non-maliciously. With the latter resulting from mistakes, errors or hostile actors' social engineering, it will be suggested that there is a troubling trend of avoidable security breaches within UK Defence. As a result, the strategic leadership of air forces will be recommended to work towards understanding and managing the problem. If they fail to do so, the article will warn that their own people's non-malicious breaches will inevitably result in incidents which may damage the operational effectiveness of military aviation.

Following this exploration of the four key areas of aviation delivery, the article will, within the final section, review the discussion. Having done so, it will be concluded that whilst significant cyber-security concern exists within all four areas, the strategic leadership of air forces should, on balance, focus their priorities on systems and the supply chain where the most acute contemporary concerns exist.

Building upon this analysis, the article will recommend that the strategic leadership of air forces must invest in reflective in-depth study to understand the problems and identify sources of mitigation. If they do so, management of the issues may be possible. If they do not, the strategic relevance of modern air power may be destroyed by the systematic exploitation of military aviation's cyber-vulnerabilities.

Concepts and the Research Requirement

The meaning of 'cyber' differs depending on perspective. At its source, the term's etymology reaches 'back to the Ancient Greek meaning of governing'.[1] Translated in today's vernacular to an adjective relating to 'the culture of computers, information technology and virtual reality',[2] its contemporary understanding is founded on its employment as a prefix. 'A linguistic tool that technologists aren't shy about using',[3] the approach began with Weiner's 1948 coining of cybernetics.[4] Adopting an 'artificial neo-Greek expression to fill the gap'[5] in communications terminology, this prefixing of cyber to describe a technology related concept is commonplace.

In response, those engaged in securing technology searched for a term that would define their role. Labelled by some as Information Assurance (IA) or Information Security, the popularity of the aforementioned linguistic tool led to the catchall of 'cyber-security'. Noted by Von Solms and Van Niekerk as now used 'in most literature...as an all-inclusive term',[6] it has been broadly accepted as the singular reference point for the protection of electronic systems, networks, data and information.

Concurrent to the adoption of cyber-security, nations also began to recognise the 'rapid technological developments...[which were introducing] unprecedented threats'.[7] Acknowledging the need to protect national assets and information from global threat actors

[1] Jovan Kurbalija, "Different Prefixes, Same Meaning: Cyber, Digital, Net, Online, E-, Virtual", *The World Post* (17 March 2015) **http://www.huffingtonpost.com/jovan-kurbalija/different-prefixes-same-m_b_7073758.html**, accessed 22 December 2017.
[2] Oxford Dictionaries, *Definition of Cyber* (2015).
[3] Paul McFedries, "The (Pre) Fix Is In", *IEEE Spectrum* (1 August 2004) **http://spectrum.ieee.org/at-work/education/the-pre-fix-is-in**, accessed 3 January 2018.
[4] Norbert Weiner, *Cybernetics: or Control and Communication in the Animal and the Machine* (MIT Press,1948) 11.
5 Ibid.
[6] Rossouw Von Solms and Johan Van Niekerk, "From Information Security to Cyber Security", *Computers and Security*, 38, (2013) 97-102: 97.
[7] IT Governance, *What is Cyber Security?* (2015) **http://www.itgovernance.co.uk/what-is-cybersecurity.aspx**, accessed 4 January 2018.

in the digital environment, more than 50 nations had by 2013 created a 'cyber-strategy'.[8] Summarising their cyber-security initiatives, these documents flag the strategic importance cyber has attained.

Although, as demonstrated by these cyber-strategies, governments and industry were comfortable with the catchall of 'cyber-security', it was not prescriptive enough for the military vernacular. Requiring greater clarity of purpose to be incorporated into military strategic planning, the term Defensive Cyber Operations (DCO) was introduced. Recognised by the UK's National Cyber Security Strategy as essential because of the military's dependence 'on information and communications systems',[9] DCO is defined by the UK's Cyber Primer as the 'active and passive measures to preserve the ability to use cyberspace'.[10] Encompassing a broad range of activities, the intent of DCO is to reduce the likelihood of an adversary degrading a nation's military capability through the cyber-domain.

To ensure DCO effectively protects military capabilities, there is a requirement to understand where vulnerabilities in operational delivery may lie. For modern air forces which are committed to operating fifth generation aircraft in a fifth generation environment, this is magnified. To illustrate this, it is necessary to understand the terms and the unique challenges they encompass.

Initially when considering 'fifth generation warfare', scholars view modern warfare as an evolution of five stages. In the first and second stages warfare was defined by technological advances. Whether the smoothbore musket or machine gun, the common theme was an ability to harness greater firepower.[11] Developing into a combination of technology and tactics in the third stage, one epitomised by the concept of 'blitzkrieg', the intent was to embrace manoeuvre over attrition.[12] Enduring throughout the mid-twentieth century, the evolution of a fourth generation was not seen until the 1980s. Characterised as no longer battlefield focused, warfare began to 'take advantage of the political, social, economic, and technical changes since World War II'.[13] Specifically, the approach emphasised 'bypassing an opposing military force and striking directly at cultural, political, or population targets'.[14]

Whilst some argue that today's conflicts continue to be defined by the asymmetric nature of fourth generation warfare, others contend that we are seeing the advent of a fifth generation.

---

[8] Von Solms and Van Niekerk, From Information Security to Cyber Security, 97.
[9] HM Government, *National Cyber Security Strategy, 2016-2021* (2016) 38.
[10] Ministry of Defence, *Cyber Primer 2nd Ed* (2016) 52.
[11] W. S. Nightengale, "The Changing Face of War: Into the Fourth Generation", *Marine Corps Gazette* (October, 1989) 22-26: 22.
[12] Ibid.
[13] Thomas X. Hammes, "Insurgency: Modern Warfare Evolves into a Fourth Generation", *Strategic Forum*, 214 (January 2005) 2.
[14] Jason Vest, "Fourth Generation Warfare", *The Atlantic* (December 2001) **https://www.theatlantic.com/magazine/archive/2001/12/fourth-generation-warfare/302368/**, accessed 9 May 2018.

Defined by Liang and Xiangsui as an unrestricted warfare 'using all means, including armed force or non-armed force',[15] it is ultimately, in Reed's assessment, one that can 'take any form, kinetic or non-kinetic'.[16]

Within this multi-dimensional nature, a key driver has been the concept of cyber and an extensive use of digital networks.[17] With information technologies now unextractable from the modern battle, Layton concludes that this latest generation has in practice created a fifth domain of operations alongside the traditional landscapes of land, sea, air and space.[18]

Though a concern across Defence, the impact of fifth generation warfare is particularly acute for air forces. Reliant in the operation of modern aircraft on protecting the Confidentiality, Integrity and Availability (CIA) of information,[19] it is feasible that a successful non-kinetic attack on an air force through the cyber-domain could impact upon the effective projection of air power. Because of this, air forces must understand areas of delivery within the context of fifth generation conflict and the vulnerabilities which may challenge the provision of effective DCO.

With the introduction of fifth generation aircraft this conclusion has attained increasing relevance. The culmination of a century of aviation development, it builds upon advances including the 'zeroeth' generation's first use of jet engines[20] through to the fourth generation's improvements 'in avionics...and optimised aerodynamics'.[21] Led by the F-35 which first entered service with the US Marine Corps (USMC) in 2015, and soon to be followed by China's J-20[22] and Russia's Su-57,[23] the defining characteristic of the generation is a significant advancement in information systems and associated software.[24]

Offering advantages in 'maintaining the edge against evolving threats',[25] its information-reliant nature presents incredible operational opportunities. In equal measure, however, it also

[15] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America* (Pan American Publishing Company, 2002) xv.
[16] Donald Reed "Beyond the War on Terror: Into the Fifth Generation of War and Conflict", *Studies in Conflict and Terrorism*, 31(8) (2008) 684 – 722: 693.
[17] Peter Layton "Five Fifth Generation Warfare Dilemmas", *The Strategist*, (25 July 2017) **https://www.aspistrategist.org.au/five-fifth-generation-warfare-dilemmas/**, accessed 7 May 2018.
[18] Ibid.
[19] Parker, D. B. *Information Security* (Springer, 1995) 153.
[20] Globalsecurity.org, *Fighter Aircraft Generations* (2018) **https://www.globalsecurity.org/military/world/fighter-aircraft-gen-1.htm**, accessed 20 July 2018.
[21] Fighter World, *Five Generations of Jets* (2018) **http://www.fighterworld.com.au/az-of-fighter-aircraft/five-generations-of-jets**, accessed 22 July 2018.
[22] Franz-Stefan Gady, "China's First Fifth Generation Fighter Jet is Operations", *The Diplomat* (2 October 2017) h**ttps://thediplomat.com/2017/10/chinas-first-5th-generation-fighter-jet-is-operational/**, accessed 9 May 2018.
[23] RT, "First Russian 5th Generation Su-57 Fighter Jets to be put in Service 'Very Soon'", *RT Online* (5 January 2018) **https://www.rt.com/news/415166-su-57-russian-army-soon/**, accessed 10 June 2018.
[24] Fighter World, *Five Generations of Jets*.
[25] Ibid.

introduces vulnerabilities. A concern encompassing fifth generation aircraft from inception to operation, potential attack-vectors can include targeting of the design phase[26] through to the exploitation of long supply chains[27] and the introduction of malicious software (malware) to aircraft systems.[28] Taken collectively, there is credible concern that the targeting of fifth generation aircraft throughout their lifecycle could have serious operational impact.

Considered in the context of vulnerabilities in the delivery of DCO, there is a requirement to explore the areas of threat which fifth generation aircraft operating in a fifth generation environment are exposed to. If such reflective study is not conducted, the strategic leadership of air forces will be unaware of how their adversaries might degrade the advantages assumed to have been gained by technological advancement. It is this research requirement, and more specifically assessing the credibility of the cyber-threat to modern military aviation, that the article will explore and address.

Systems

In discussing military air operations, including their potential cyber-vulnerabilities and other inherent threats, the most intuitive starting point is systems. In broad terms, a system is a combination of hardware and software which can receive inputs, process data and create information for storage and output.[29] Whilst the concept's manifestation can become increasingly complex, the fundamental principles remain unchanged.

Within aviation, as with other industries, bodies have overlaid this basic interpretation with standards that define the roles of specific system types. Aeronautical Radio, Incorporated (ARINC) 811, for example, divides aircraft systems into domains including Aircraft Control and Airline Information.[30] As aviation develops, however, structures will be increasingly difficult to chart.

One manifestation of this increasing complexity is the introduction of Next Generation (NextGen) technologies to aircraft. Entwining multiple systems to create e-enabled aircraft,[31] a shift epitomised by the military concept of fifth generation aircraft,[32] the development is moving aviation away from traditional methods of operation. Evident across the industry,

---

[26] Reuters, "Theft of F-35 Design Data is Helping U.S. Adversaries – Pentagon", *Reuters Market News* (19 June 2013) **https://www.reuters.com/article/usa-fighter-hacking/theft-of-f-35-design-data-is-helping-u-s-adversaries-pentagon-idUSL2N0EV0T320130619**, accessed 10 May 2018.
[27] R. De Cerchio, "Aircraft Systems Cyber Security", *Digital Avionics Systems, Conference (DASC), IEEE/AIAA (2011)* **https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6095969**, accessed 23 June 2018.
[28] Roberto Sabatini, "Cyber Security in an Aviation Context", *Melbourne Cyber Security Conference* (November 2016) *https://www.researchgate.net/publication/312191777_Cyber_Security_in_the_Aviation_Context*, accessed 8 May 2018.
[29] Techopedia, *Computer System* (2018) **https://www.techopedia.com/definition/593/computer-system**, accessed 15 July 2018.
[30] De Cerchio, Aircraft Systems Cyber Security, 1.
[31] Ibid.
[32] Fighter World, *Five Generations of Jets*.

examples include human interaction through voice communication no longer acting as 'the primary means of obtaining information',[33] and Cyber-Physical Systems (CPS) extending beyond the information domain to 'monitor and control physical processes'.[34] Within this new reality operators must acknowledge that the human element is no longer pivotal. Rather, aircraft are becoming reliant on 'timely, accurate and un-tampered information' being processed by both internal and external support systems.[35]

Given this, it is becoming increasingly important 'to protect the CIA of the information processed by those systems'.[36] Extending beyond the aircraft itself, and considering the military context specifically, it is also recognised that systems 'enable almost everything the military does'.[37] This reality has seen information technology evolve in less than a generation 'from an administrative tool...into a national strategic asset'.[38]

Alongside this reliance on systems, the asymmetric threat of cyber,[39] driven by 'the low cost of computing devices, means that operationally essential systems are increasingly vulnerable'.[40] Judged by the United States (US) Operational Test and Evaluation (OTE) agency to be as credible a threat as traditional capabilities, it warns that any data exchange, however brief, is open to compromise.[41]

Though some might characterise these warnings as an overreaction, reporting confirms that 'over the past ten years, the frequency and sophistication of intrusions into western military networks have increased exponentially'.[42] In 2008 for example a USB flash drive infected with malware was placed into a US military laptop in the Middle East. Alleged to have given unknown adversaries the ability to control US Department of Defence (DoD) servers, it represented a troubling window into how an enemy can compromise systems.[43]

---

[33] De Cerchio, Aircraft Systems Cyber Security, 1.
[34] Edward Lee, "Cyber Physical Systems: Design Challenges", *Technical Report No. UCB/EECS-2008-8 - Electrical Engineering and Computer Sciences University of California at Berkeley* (23 January 2008) 1, **http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.156.9348&rep=rep1&type=pdf**, accessed 12 July 2018.
[35] De Cerchio, Aircraft Systems Cyber Security, 2.
[36] Michael Olive, Roy Oishi and Stephen Arentz, "Commercial Aircraft Information Security - An Overview of ARINC Report 811", *25th Digital Avionics Systems Conference*, (15 October 2006) 1-12: 3, **https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4106238**, accessed 4 July 2018.
[37] Willian Lynn, 'Defending a New Domain: The Pentagon's Cyberstrategy', *Foreign Affairs*, 89 (5) (September/October 2010) 97-108: 98.
[38] Ibid.
[39] Ibid.
[40] Ibid.
[41] Operational Test and Evaluation Centre, "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs", *Memorandum for Commander Army Test and Evaluation Command and Air Force Operational Test and Evaluation Centre* (1 August 2014) 1, **www.dote.osd.mil/pub/policies/2014/8-1-14_Procs_for_OTE_of_Cybersec_in_Acq_Progs(7994).pdf**, accessed 1 July 2018.
[42] Lynn, Defending a New Domain: 97.
[43] Clifford Magee, "Awaiting the Cyber 9/11", *Research Paper, USMC University* (11 March 2012) 4.

Not limited to ground systems, media reports also confirmed the compromise of information relating to the F-35. In June 2013, for example, a US Senate Sub-Committee was informed that the systems of the prime-contractor, Lockheed Martin, containing sensitive information had been compromised by an unknown adversary.[44] Reinforced in 2015 through documents leaked by Edward Snowdon, *Der Spiegel* reported that it was Chinese hackers who had compromised Lockheed Martin.[45] This, in the assessment of industry commentators, led to a significant loss of US advantage over a principal adversary.[46]

Though concerning, these losses are not the most dangerous element of system compromise. With exploits 'becoming more sophisticated over time',[47] it is an adversary's ability to impact on current operations which poses the greatest threat. Looking to other industries for examples, automobile research has shown that an attacker can now circumnavigate a car's internal network to compromise 'safety critical elements such as the brakes and engine'.[48] Immensely dangerous, such attacks against operational aircraft could be disastrous. Equally, targeting of the support elements to aviation can also be disruptive. In 2006, for example, a malware attack on the US Federal Aviation Authority's (FAA) Air Traffic Control (ATC) system forced a shutdown of all commercial flights in Alaska.[49] If repeated against critical military support systems, an adversary could prevent the deployment of air power.

It could be argued, however, that with cyber dominating headlines, its elevation to a strategic issue is an over inflation. In Cavelty's opinion, for example, assessments have ignored the 'low probability of a large scale cyber-attack' and placed too much emphasis on the necessity of military cyber-security.[50] This assertion is illustrated by the fact that a large-scale cataclysmic cyber-attack, a potential first warned of in 1991 by Schwartau's predictions of a 'Cyber Pearl

---

[44] Sydney Freeberg, "Top Official Admits F-35 Stealth Fighter Secrets Stolen", *Breaking Defence* (20 June 2013) **https://breakingdefense.com/2013/06/top-official-admits-f-35-stealth-fighter-secrets-stolen/**, accessed 1 July 2018.

[45] Jacob Applebaum, "NSA Preps America for Future Battle", *Das Spiegel* (17 January 2015) **www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409-2.html**, accessed 3 July 2018.

[46] Franz-Stefan Gady, 'New Snowdon Document Reveals China Behind F-35 Hack', *The Diplomat* (27 January 2015) **https://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack/**, accessed 2 July 2018.

[47] De Cerchio, Aircraft Systems Cyber Security, 1.

[48] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner and Tadayoshi Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces", *USENIX Security Symposium* (August 2011) 77-92: 77.

[49] Federal Aviation Administration, *Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems Report Number: FI-2009-049* (4 May 2009) 5, **https://www.oig.dot.gov/sites/default/files/ATC_Web_Report.pdf**, accessed 29 June 2018.

[50] Myriam Cavelty, "The Militarisation of Cyber Security as a Source of Global Tension" in A. Wenger (ed) *Centre for Security Studies – Strategic Trends 2012* (12 March 2012) **https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/153535/1/eth-5788-01.pdf**, accessed 10 July 2018.

Harbour',[51] has not, to date, occurred. Because of this, it is necessary to ask whether the compromise of systems is truly an issue which should concern the strategic leadership of an air force or if it is an over-exaggeration. To address this question, it is informative to consider two contemporary military aviation systems: UAVs and the F-35's ALIS.

Considering the first, UAVs, it has been argued that having harnessed the ability to 'manoeuvre autonomously...[by] relying on on-board computers'[52] they are the future of military aviation and the epitome of systems replacing the human. With the US military having increased its investment in the research and production of UAVs to $4.2 billion by 2012, and their role being extended to include surveillance, reconnaissance, transport and armed attacks, there can be no doubt that they will be an enduring military capability.[53]

Though providing impressive options for military aviation, Hartmann comments that as a flying system they are 'highly exposed...complex pieces of hardware'.[54] A potential weakness to their operation, it was not a concern that had been widely considered prior to 2007. The main reason for this, according to Javaid et al, was that prior to this UAVs were not in widespread use.[55]

Developing this argument, we see that since the operational expansion of UAV usage, their vulnerability to cyber-attack has been increasingly highlighted. In 2009, for example, investigations found that a UAV video feed had been compromised by a terrorist group. Recorded using SkyGrabber software,[56] the events illustrated a widespread problem of unencrypted links between ground stations and UAVs. Allowing an adversary to see the intelligence feeds which guide many modern operations, it reverses the advantage of operating UAVs and potentially places a military's own personnel at an increased threat of harm.

In a second example, a US Sentinel UAV was in 2011 captured by Iranian forces.[57] Confirmed by President Obama in a press conference,[58] it has been suggested that a vulnerability with the

[51] Winn Schwartau quoted in US Congress, *Hearing Before the Subcommittee on Technology and Competitiveness on Computer Security* (27 June 1991) **https://phibetaiota.net/wp-content/uploads/2017/09/Winn-Schwartau-Congressional-Testimony-Digital-Pearl-Harbor-27-June-1991.pdf**, accessed 23 February 2018.
[52] Kim Hartmann and Christoph Steup, "The Vulnerability of UAVs to Cyber-Attacks; An Approach to the Risk Assessment", *Cyber Conflict (CyCon) 5th International Conference* (June 2013) 1-23: 1, **http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.156.9348&rep=rep1&type=pdf**, accessed 10 July 2018.
[53] Ibid.
[54] Ibid.
[55] Ahmad Javaid, Weiqing Sun, Vijay Devabhaktuni and Mansoor Alam, "Cyber Security Threat Analysis and Modelling of an Unmanned Aerial Vehicle System", *IEEE Conference on Technologies in Homeland Security (HST)* (November 2012) 585-590: 586, **https://www.researchgate.net/profile/Ahmad_Javaid/publication/235676360_Cyber_security_threat_analysis_and_mode.pdf**, accessed 27 June 2018.
[56] Ibid.
[57] Hartmann and Steup, The Vulnerability of UAVs to Cyber-Attacks; An Approach to the Risk Assessment, 8.
[58] Barak Obama quoted in Rick Gladstone "Iran is Asked to Return US Drone", *New York Times* (12 December 2011) **https://www.nytimes.com/2011/12/13/world/middleeast/obama-says-us-has-asked-iran-to-return-drone.html**, accessed 1 July 2018.

UAV's navigation system may have been exploited.[59] Specifically, as Humphrey explains, the Iranians could have used 'Global Positioning Satellite (GPS) Spoofing' to exploit the fact that GPS has no built-in protection against counterfeiting.[60] Allowing an adversary to hijack a GPS signal controlling a UAV, it could have allowed Iran to redirect the Sentinel and 'land it safely on an Iranian airfield'.[61]

Given these examples, there is a clear indication that whilst cyber-attacks on UAVs may be difficult to execute,[62] they are nonetheless possible. With both examples illustrating that a comparatively less capable group can affect or deny the projection of a more powerful state's air power, there is reason for concern. Conversely, however, one might argue that, given the UAV's unique nature as a largely autonomous system, a higher level of vulnerability to cyber-attack should be expected. If this is true, then the systems of the manned (and significantly more costly) fifth generation aircraft should be more immune to cyber-threats.

To explore this statement, there is value in examining a second aviation system: the US led alliance's new fifth generation aircraft, the F-35. An immensely complex aircraft, it takes, in Lockheed Martin's own estimation, 'more than steel, advanced electronics and engine thrust to make [it]...take flight'.[63] Specifically, the F-35 relies on ALIS.

Designed to provide 'a comprehensive logistic support environment',[64] ALIS delivers an array of advanced services. These include Prognostics and Health Management (PHM) to enhance aircraft safety and efficiency, automated technical support to reduce specialised maintenance training, digital links between aircraft and Lockheed Martin, and innovative support to deliver sorties at the lowest cost.[65] Taken collectively, the chief F-35 test pilot for Lockheed Martin, Alan Norman, compares ALIS to R2-D2. Referring to the droid that helped Luke Skywalker fly the X-Wing in Star Wars, he asserts that 'right now [ALIS] is the ultimate in human-machine interaction'.[66]

---

[59] Hartmann and Steup, The Vulnerability of UAVs to Cyber-Attacks; An Approach to the Risk Assessment, 8.
[60] Todd Humphrey, "Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing", *Submitted to the Subcommittee on Oversight, Investigations, and Management of the House Committee on Homeland Security* (18 July 2012) 1, **https://homeland.house.gov/files/Testimony-Humphreys.pdf**, accessed 3 July 2018.
[61] Hartmann and Steup, The Vulnerability of UAVs to Cyber-Attacks; An Approach to the Risk Assessment, 8.
[62] David Cenciotti, "Captured Stealth Drone", *The Aviationist* (17 January 2012) **http://theaviationist.com/category/captured-stealth-drone/page/2/**, accessed 5 July 2018.
[63] Lockheed Martin, *Autonomic Logistics Information System (ALIS)* (2018) **https://www.lockheedmartin.com/en-us/products/autonomic-logistics-information-system-alis.html**, accessed 1 July 2018.
[64] Simon Henley, Russ Currer, B. Scheuren, A. Hess and Geoffrey Goodman, "Autonomic Logistics - The Support Concept for the 21st Century", *Aerospace Conference Proceedings, IEEE*, 6 (2000) 417-421: 417, **https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=877915**, accessed 9 July 2018.
[65] Ibid.
[66] Alan Norman quoted in David Martin, "Can the US Military's New Jet Fighter be Hacked?", *CBS News – 60 Minutes* (1 June 2014) **https://www.cbsnews.com/news/can-the-f-35-be-hacked/**, accessed 4 July 2018.

With Version 2.02 of ALIS released in 2017, 'for the first time, [it] integrated the entire F-35 from tip to tail, including the propulsion system'.[67] Given this development which makes ALIS the 'single, secure information environment...for all elements of F-35 operations',[68] and the importance of the aircraft to the defence of the US and its eight partner nations, serious questions must be asked regarding its ability to protect the CIA of information. The implications of this are huge: if an adversary could compromise ALIS 'they've essentially defeated the plane'[69] without 'firing a bullet'.[70]

Though detail on whether ALIS is successfully protecting the CIA of information is classified, consistent open source reporting since its inception have raised concerns. An early example in 2012 related to US Navy penetration testers exploiting Lockheed Martin's failure to separate classified and unclassified data streams.[71] Though a temporary workaround to create an 'air gap' allowed the continued development of ALIS,[72] the events provided an indication of the revelations to come.

In a further circumstance Lockheed Martin, under pressure for its previous failures, acknowledged that 'the company had seen a large increase in the number and sophistication of attacks on its networks'.[73] Accusing unnamed governments 'of targeting and breaking into the networks of its suppliers',[74] it was clear that there was a concerted effort to compromise the cyber-security of the project.

Despite this, events in 2015 showed that elements of ALIS were so deeply flawed that Lockheed Martin were not taking heed of their own concerns. This was illustrated during the USMC Operational Test One (OT-1) which in May 2015 saw seven F-35's embarked on the aircraft carrier *USS Wasp*.[75] Whilst the USMC would 'triumphantly declare its variant of the F-35 combat ready in late July [2015]',[76] the fanfare hid major failings in cyber-security.

---

[67] Wilson Brissett, "ALIS 2.02 Ready to Go'", *Air Force Magazine* (28 March 2017) **http://www.airforcemag.com/Features/Pages/2017/April%202017/ALIS-202-Ready-to-Go.aspx**, accessed 30 June 2018.
[68] Lockheed Martin, *Autonomic Logistics Information System (ALIS)*.
[69] David Martin, "Can the US Military's New Jet Fighter be Hacked?", *CBS News – 60 Minutes* (1 June 2014) **https://www.cbsnews.com/news/can-the-f-35-be-hacked/**, accessed 4 July 2018.
[70] Jeremy Bender, "The New F-35 Fighter Jet Can Be Taken Down Without a Bullet Ever Being Fired", *Business Insider* (18 February 2014) **www.businessinsider.com/f-35-hackers-2014-2?IR=T**, accessed 1 July 2018.
[71] Andrea Shalal-Esa, "Lockheed's F-35 Logistics System Revolutionary but Risky", *Reuters* (16 November 2012) **https://www.reuters.com/article/us-lockheed-fighter-logistics-idUSBRE8AF09L20121116**, accessed 5 July 2018.
[72] Dave Majumdar, "USMC Finds Workaround for Cyber-Vulnerability of F-35 Logistics System", *Flight Global* (21 November 2012) **https://www.flightglobal.com/news/articles/usmc-finds-workaround-for-cyber-vulnerability-on-f-3-379272/**, accessed 2 July 2018.
[73] Shalal-Esa, Lockheed's F-35 Logistics System Revolutionary but Risky.
[74] Ibid.
[75] Operational Test and Evaluation Agency, 'Observations on the Marine Corps F-35B Demonstration on USS Wasp', *Memorandum For Under Secretary of Defense for Acquisition, Technology And Logistics* (22 July 2015) 1, **www.pogoarchives.org/straus/2015-9-1-DoD-FOIA-ocr.pdf**, accessed 5 July 2018.
[76] Dan Grazier and Mandy Smithburger, "Pentagon Testing Office Calls Foul on F-35 Operational Testing", *Project on Government Oversight* (14 September 2015) **www.pogo.org/straus/issues/weapons/2015/pentagon-testing-office-calls-foul.html**, accessed 5 July 2018.

Summarised in a memorandum from the US OTE, it was revealed that the operational limitations of ALIS led to 'extraordinary measures to keep the planes flying'.[77] Specifically, the ALIS Concept of Operation was for data transfer between Squadron Operating Units (SOU) aboard the *USS Wasp* and the Lockheed Martin core logistic node, the Autonomic Logistics Operating Unit (ALOU).[78] Failures in the datalinks, however, led to the support team travelling off base to use commercial wi-fi to download the aircraft files, burn them to CDs and manually upload the data to the *USS Wasp* SOU.[79] A monumental breach of operating procedures, there was no other way to keep the aircraft flying and pass the operational test.

With the *USS Wasp* example also known to have led to 'inconsistencies between home station and deployed files',[80] the lessons are obvious. The USMC, in attempting to operate an aircraft which is entirely reliant on a single system, compromised security to ensure operational delivery. Whilst this risk might be acceptable in a controlled environment, it would be an entirely different prospect in combat.

Going beyond the risk of data compromise, other reports add additional layers of concern. In 2014, for example, it was suggested that ALIS 'disallows the human pilot to take control of the F-35 if it senses there is a problem'.[81] A safety measure to prevent pilots exceeding the capabilities of a malfunctioning aircraft, it is possible that malware introduced to ALIS might allow an adversary through the corruption of the integrity of information to ground an entire fleet.[82]

With Lockheed Martin publicly confirming 'that they are working hard to remove vulnerabilities',[83] and cyber-security recognised as being a strategic issue, it would be expected that both private industry and government agencies alike would be ensuring that the issues do not continue. This direction of travel is supported by the US OTE which asserted that 'as real world cyber adversaries regularly demonstrate their ability to compromise systems...all operational testing must examine system performance in the presence of a realistic cyber threat'.[84]

Despite this public statement, it was reported in 2016 that the US Joint Program Office (JPO) refused to proceed with the required cyber-security tests for ALIS. This was because 'such

[77] Ibid.
[78] Operational Test and Evaluation Agency, Observations on the Marine Corps F-35B Demonstration on USS Wasp, 1.
[79] Ibid.
[80] Ibid.
[81] Cyberwarzone, "New F-35 Jet is Vulnerable to Cyber Attack", *Cyber-Security News* (31 May 2014) **https://cyberwarzone.com/new-f-35-fighter-jet-vulnerable-cyber-attacks/**, accessed 2 July 2018.
[82] Ibid.
[83] Ibid.
[84] Operational Test and Evaluation Agency, Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs, 1.

realistic hacker tests could damage the critical maintenance and logistics software, thereby disrupting flights of the approximately 100 [aircraft] already in service'.[85] Reinforcing concerns over the failure of ALIS and therefore the F-35, media reports responded by raising 'obvious and disturbing questions about what could happen in combat'.[86]

Summarising these concerns, the 2017 US OTE annual report confirmed that cyber-security testing had shown that 'some of the vulnerabilities identified during earlier testing periods still had not been remedied'.[87] When considered against the backdrop of the significant issues already discussed, there is mounting evidence that the cyber-vulnerabilities of the F-35's systems represent a concerning threat to the aircraft's operational effectiveness. Furthermore, with advanced aircraft such as the F-35 and UAVs signalling the future of modern air power, and the systems of both being susceptible to cyber-attack, it is asserted that the cyber-vulnerabilities of military aviation's systems have created a credible threat to air forces which is serious, widespread and persistent.

Infrastructure

A second area for consideration must be infrastructure. Unlike land forces which can operate with limited basing, or navies which can operate for long periods without the support of ports, the impermanence of aviation requires aircraft to frequently return to an established home base environment.[88]

Encompassing a broad array of infrastructure requirements which are essential to the effective projection of air power, this reliance is similar in nature to the civil concept of Critical Infrastructure. Referring to those elements 'necessary for an organisation to function',[89] there are, for aviation, numerous aspects of infrastructure which, if lost or compromised, would prevent the projection of air power. Not limited to the physical elements of runways and hangars, air power is equally reliant on secondary infrastructure including electricity, communications and fuel. With many delivered to air forces by external providers, including foreign states where air power is based overseas, assuring their protection becomes increasingly complex.

A requirement since the advent of air power, air forces have by necessity become world-leaders in layered physical and procedural security measures which combine to deliver

[85] Dan Grazier, '"F-35 Officials Prove Need for Cyber Testing by Cancelling One", *Centre for Defence Information, Project on Government Oversight* (7 December 2015) **http://www.pogo.org/straus/issues/weapons/2015/f-35-officials-prove-need-for-cyber-testing.html**, accessed 3 July 2018.
[86] Ibid.
[87] Operational Test and Evaluation Agency, "F-35 Joint Strike Fighter", *FY 17 Department of Defence Project*s (2018) 31-60: 33, **http://www.dote.osd.mil/pub/reports/FY2017/pdf/dod/2017f35jsf.pdf**, accessed 9 July 2018.
[88] Ministry of Defence, "Joint Doctrine Publication 0-30: UK Air and Space Power", *Development, Doctrine and Concepts Centre*, December (2017) 32, **https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/668710/doctrine_uk_air_space_power_jd p_0_30.pdf**, accessed 9 June 2018.
[89] Centre for the Protection of National Infrastructure, *Critical National Infrastructure* (2018), **https://www.cpni.gov.uk/critical-national-infrastructure-0**, accessed 3 June 2018.

effective defence in depth. These established capabilities can, however, be circumnavigated by the cyber-threat. Considered through the lens of modern operations, this vulnerability has been introduced by a growing dependency on Information and Communications Technology (ICT). A defining feature of the 'interconnected and knowledge-based economy',[90] a situation has emerged in which 'complex physical and cyber based systems'[91] are relied upon to maintain and deliver essential and routine requirements. Making cyber a 'backbone of critical infrastructures...[organisations have reached a place where] a major cyber-security incident could have significant impact' on the continued functioning of key infrastructure.[92]

Recognising this, the UK's National Cyber Security Centre (NCSC) recommends a 'holistic approach to security that encompasses physical and personnel as well as cyber-security'.[93] An expansion of the defence-in-depth principle, the NCSC approach ensures that physical weaknesses are prevented from allowing a hostile actor access to the cyber systems which can, in full circle, impact on the physical delivery of infrastructure.

A high-profile example of where holistic security was not in place, and cyber-vulnerabilities were exploited, was the 2015 attack on the Ukrainian power grid. Initially reported on 24 December 2015 by the Ukrainian news outlet TSN,[94] the 'synchronised and coordinated [cyber-attack], followed extensive reconnaissance of the victim networks'.[95] This in turn is believed to have facilitated the introduction of the BlackEnergy3 malware to the power company systems through phishing emails to their employees.[96] Resulting in a major power outage which disrupted over 50 sub-stations and more than 220,000 consumers,[97] Ukraine was forced to abandon automation and move to manual operations to restore power.[98]

Placed in the context of aviation, an attack on the power supply for an airbase by an adversary intent on degrading operational capability could have significant impact. Though it is expected

---

[90] Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke, "Cyber Security and the UK's Critical National Infrastructure", *A Chatham House Report* (September (2011) viii, **https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r0911cyber.pdf**, accessed 10 June 2018.

[91] Chen-Ching Liu, "Cybersecurity for Critical Infrastructures: Attack and Defense Modelling", *IEEE Transactions on Systems, Man, and Cybernetics*, 40 (4) (July 2010) 853-863: 853.

[92] Ibid.

[93] Cyber Security Centre, *We Work for Government and the Critical National Infrastructure* (2 October 2016) **https://www.ncsc.gov.uk/information/we-work-government-and-critical-national-infrastructure**, accessed 8 June 2018.

[94] TCH, "Due to a Hacker Attack, The Power of Half the Ivano-Frankivsk Region was De-Energised", *TCH Online* (24 December 2015) **https://translate.google.co.uk/translate?hl=en&sl=ru&u=https://ru.tsn.ua/ukrayina/iz-za-hakerskoy-ataki-obestochilo-polovinu-ivano-frankovskoy-oblasti-550406.html&prev=search**, accessed 17 July 2018.

[95] Department of Homeland Defence, "Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure", *International Control Systems Computer Emergency Response Team* (25 February 2016) **https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01**, accessed 21 May 2018.

[96] HM Government, *National Cyber Security Strategy 2016-2021* 2016), 21.

[97] Ibid.

[98] Defense Use Case, "Analysis of the Cyber-Attack on the Ukrainian Power Grid", *Electricity Information Sharing and Analysis Center (E-ISAC)* (18 March 2018) v, **https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf**, accessed 16 July 2018.

that resilience planning in the form of generators would provide a back-up, such options may have limited longevity and reduced capacity. With all aircraft, especially fifth generation aircraft, dependent on electrically powered systems to operate, this impact (even at a limited level) could seriously degrade the delivery of air operations.

Exploring this cyber-vulnerability in more detail, and broadening it to consider other key elements of aviation infrastructure such as fuel supplies, an important area of concern is Supervisory Control and Data Acquisition (SCADA) systems. Integral to the performance of much critical Infrastructure,[99] SCADA systems enable automation and optimisation of industrial processes.[100] Deployed globally in virtually all large industries, they are integral to everything from power generation to transport networks.[101] Prominent in the aforementioned Ukraine attack, it was the disabling of the sub-station's SCADA systems which caused the outages.[102]

Given their role as a keystone of critical infrastructure, SCADA systems are 'increasingly becoming the targets of cyber-attacks'.[103] This interest has been maximised by those with malicious intent recognising the ability for attacks on SCADA systems to have 'physical manifestations in the real world'.[104]

The likelihood of such attacks has also increased as these networks (which were previously located in remote locations and air gapped from other networks)[105] have become interconnected, including through the internet. The result, according to Dell, is a doubling of reported SCADA-based cyber-attacks. This, however, may only be the tip of the iceberg. With companies in most countries 'only required to report data breaches that involve personal or payment information, SCADA attacks often go unreported'.[106]

For military aviation, this increasing trend is one to observe closely. As demonstrated by the infamous Stuxnet attack, which targeted a SCADA system controlling centrifuges in an Iranian nuclear facility, it is an issue which not only affects private industry or manufacturing.

---

[99] Bill Miller and Dale Rowe, "A Survey SCADA of and Critical Infrastructure Incidents", *Proceedings of the 1st Annual conference on Research in Information Technology* (October 2012) 51-56: 52, **https://www.researchgate.net/profile/Bill_Miller5/publication/262315594_A_survey_SCADA_of_and_critical_infrastructure_incidents/links/551ab10f0cf2fdce843695f4.pdf**, accessed 17 May 2018.

[100] Cabinet Office, *The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World* (2011) 13, **https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf**, accessed 22 May 2018.

[101] Andrew Nicholson, Stuart Webber, Shaun Dyer, Tanuja Patel and Helge Janicke, "SCADA Security in the Light of Cyber-Warfare", *Computers and Security*, 31 (4) (2012) 418-436: 419.

[102] Defence Use Case, Analysis of the Cyber-Attack on the Ukrainian Power Grid, 20.

[103] Miller and Rowe, A Survey SCADA of and Critical Infrastructure Incidents, 52.

[104] Ibid.

[105] Vinay Igure, Sean Laughter and Ronald Williams, "Security Issues in SCADA Networks", *Computers and Security*, 25 (7) (2006) 498-506: 500.

[106] Dell, *Dell Annual Threat Report* (2015) **https://software.dell.com/docs/2015-dell-security-annual-threat-report-white-paper-15657.pdf**, accessed 11 May 2018.

Extending to all organisations which operate SCADA systems, it is possible that a hostile actor intent on impacting air operations could disrupt the SCADA systems of an airbase's power supply or fuels infrastructure.

Though aviation-specific examples of SCADA cyber-attacks are not currently in the public domain, successful attacks which could have impacted on air operations have been reported. In 2011, for example, hackers targeted the SCADA system of a pump used by a US water utility company 'after hacking the network of a SCADA vendor and stealing remote access login information'.[107] Causing the pump to constantly turn on and off and finally burn out,[108] similar means could be used to destroy the fuels infrastructure of an airbase or the network supplying an airbase.

Cutting fuel supplies in this way to a military airbase could quickly bring operations to a halt. Though no military examples of such an occurrence are in the public domain, the non-malicious malfunctioning of the fuel pipeline serving Manchester civil airport in 2012 demonstrated the impact on aviation with fuel shortages causing significant disruption to flights.[109] When added to known attacks using similar methodologies in April 2018 against natural gas pipelines in the US,[110] and the signal sent by Russia in 2007 when it allegedly used cyber-operations to target the infrastructure of Estonia,[111] evidence points towards a clear combination of capability and intent which could be directed against air power.

A current and ever growing concern, the cyber-threat to an air force's own and supporting critical infrastructure is therefore one which is likely to persist. This assessment is underlined by a threat warning issued in 2017 by the US Department of Homeland Security (DHS) which cautioned of an 'Advanced Persistent Threat (APT) targeting government entities and organisations in the energy, nuclear, water, aviation, and critical manufacturing sectors'.[112] Issued alongside a Symantec report which warned of the Dragonfly malware[113] targeting European power companies, a claim supported by media reports of hackers targeting the

---

[107] Fahmida Rashid, "Cyber-Attackers Breach SCADA Network, Destroy Pump at Water Utility", *eweek* (18 November 2011) **http://www.eweek.com/c/a/Security/CyberAttackers-Breach-SCADA-Network-Destroy-Pump-at-Water-Utility-614710**, accessed 11 May 2018.

[108] Ibid.

[109] BBC, "Who, what, why: How can an airport run out of fuel?", *BBC News Online* (7 June 2012) **https://www.bbc.co.uk/news/magazine-1835559**2, accessed 18 June 2018.

[110] Haley Zaremba, "U.S. Sees Wave of New Cyber Attacks on Energy Infrastructure" *Oilprice.com* (11 April 2018) **https://oilprice.com/Geopolitics/International/US-Sees-Wave-Of-New-Cyber-Attacks-On-Energy-Infrastructure.html**, accessed 11 July 2018.

[111] Rain Ottis, "Analysis of the 2007 Cyber-Attacks Against Estonia from the Information Warfare Perspective", *Proceedings of the 7th European Conference on Information Warfare* (2004) 151-168: 164.

[112] Simon Sharwood, "US Energy, Nuke and Aviation Sectors Under Sustained Attack", *The Register* (22 October 2017) **https://www.theregister.co.uk/2017/10/22/us_department_of_homeland_security_warns_of_sustained_attacks_on_industry/**, accessed 18 May 2018.

[113] Symantec, *Dragonfly: Western Energy Sector Targeted by Sophisticated Attack Group*, (20 October 2017) **https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks**, accessed 20 May 2018.

EirGrid company in Wales and Northern Ireland,[114] there is mounting evidence that air forces must remain alert to the cyber-vulnerabilities inherent in modern infrastructure.

Notwithstanding the credibility of the threat, the reality is that most of the infrastructure which could be targeted to impact on air operations is beyond the military's control. Whether delivered by commercial or nationalised providers, all of which (under the advisement of organisations including the NCSC) are alive to the threat, there is limited influence an air force's strategic leadership can exert. Furthermore, with most eventualities able to be mitigated through strong resilience planning such as alternate fuel sources or the provision of generators, the ability to impact air operations is lessened. Based on this, it is concluded that though the cyber-vulnerabilities of an air force's infrastructure must be considered, the continuance of current mitigation measures means that infrastructure should not, on balance, be the strategic leaderships principle concern.

Supply Chain

Another significant area for consideration is the securing of an air force's supply chain. With technologically-advanced fifth generation aircraft requiring a complex combination of sub-contractors, commentators have suggested that it is increasingly likely that cyber-attacks will not 'come through the front door...[but via] an attack on the weakest link in their supply chain'.[115]

Considered in general, complex global supply chains have 'transformed the world'[116] with national economies becoming interdependent.[117] In response, supply chains have expanded to achieve reliability and cost-effectiveness. In the delivery of fifth generation air power, the reality is no different. The F-35 project is a prime example, with the main contractor, Lockheed Martin, supported by a myriad of sub-contractors.

Exploring these complexities of the F-35 project is an instructive introduction to discussing the supply chain question. Firstly, to reduce costs, Lockheed Martin optimised its production by contracting-out the manufacture of 60 percent of the 40,000 components required for each aircraft.[118] A divergence from its traditional method of bespoke in-house production and

[114] Cathal McMahon, "State-Sponsored' Hackers Targeted EirGrid Electricity Network in 'Devious Attack", *Irish Independent* (17 July 2018) **https://www.independent.ie/irish-news/statesponsored-hackers-targeted-eirgrid-electricity-network-in-devious-attack-36005921.html**, accessed 17 July 2018.
[115] Omera Khan and Daniel Estay, "Supply Chain Cyber Resilience", *Technology Innovation Management Review* (April 2015) 6-14: 6.
[116] Richard Baldwin, "Global Supply Chains: Why They Emerged, Why They Matter, and Where They are Going", *CERP Discussion Paper* (August 2012), **https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2153484**, accessed 14 June 2018.
[117] Gary Gereffi, John Humphrey, Raphael Kaplinsky and Timothy Sturgeon, "Globalisation, Value Chains and Development", *IDS Bulletin, 32* (3) (2001) 1-8: 1.
[118] Jason Busch, "The F-35 Joint Strike Fighter Supply Chain", *Spendmatters*, (31 July 2006) **http://spendmatters.com/2006/05/31/the-f-35-joint-strike-fighters-supply-chain/**, accessed 18 June 2018.

maintenance,[119] the shift increased efficiency but created a complex supply chain. In the US alone, for example, the F-35 project engages 1,200 small to medium sized suppliers[120] across 46 states.[121]

The international nature of the F-35 project has also created complications. On its commencement, it was agreed that all nine partner countries[122] would share in the economic dividend. To achieve this, companies from each nation were awarded contracts.[123] As a result, even with industry websites publishing comprehensive details of F-35 sub-contractors,[124] it is unlikely that anyone outside of Lockheed Martin could fully chart the supply chain.

Considering the importance of the F-35 project to all nine partner nations, there should be deep concern over the supply chain's complexity and opaqueness. In terms of cyber-security, however, this concern goes deeper. With each company in the chain requiring access to sensitive information, and a proportion granted access to military systems, the potential sources of cyber-compromise grows exponentially.

In exploring this, the concept of the 'weakest link' looms large. As the UK's Computer Emergency Response Team (CERT-UK) highlights, when supply chains become complex, the overall level of cyber-security is only as strong as its weakest member.[125] Determined to exploit this, aggressors will focus on companies with lower levels of cyber-security.

Though a generalisation, it is commonly accepted that these 'weak links' are smaller organisations 'who, due to more limited resources, have the poorest cyber-security arrangements'.[126] This view is supported by the UK Government, which reported that whilst 46 percent of businesses overall identified at least one cyber-security breach in 2017, the number increases to two-thirds among medium businesses.[127] Further underlined by Verizon's research indicating that 92 percent of cyber incidents occurred in small to medium sized

---

[119] Ibid.
[120] K. A. Porter, "A Volatile Supply Chain: What is in Your Future?", *Military Embedded Systems* (7 October 2014) **http://mil-embedded.com/articles/a-supply-chain-is-your-future/**, accessed 17 June 2018.
[121] Lockheed Martin, *F-35 Lightning II; Powering Job Creation for America and its Allies*' (2018) **https://www.f35.com/about/economic-impact**, accessed 11 June 2018.
[122] F-35 project partner countries: Australia, Canada, Denmark, Italy, the Netherlands, Norway, Turkey, the US and the UK.
[123] Lockheed Martin, *F-35 Lightning II – Global Participation* (2018), **https://www.f35.com/global**, accessed 5 June 2018.
[124] Airframer, *Lockheed Martin F-35 Lightning II* (2018), **http://www.airframer.com/aircraft_detail.html?model=F-35_JSF**, accessed 1 July 2018.
[125] CERT-UK, "Cyber Risks in the Supply Chain", *CERT-UK White Paper* (2015) 4, **https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/Cyber-security-risks-in-the-supply-chain.pdf**, accessed 27 May 2018.
[126] Ibid.
[127] Department for Culture, Media and Sport, *Cyber Security Breaches Survey 2017* (April 2017) 3, h**ttps://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf**, accessed 25 May 2018.

businesses,[128] there is a clear requirement when assuring the supply chain to look further than just the prime contractor.

Despite the risk, initiatives to assure cyber-security within supply chains have only recently occurred. Previously favouring traditional security, CERT-UK comments that, when managing supply chains, organisations are adept at mitigating physical vulnerabilities but 'seldom deal with cyber-security risks'.[129] A reversing trend, however, the specialism defined by Oltsik et al as the process of extending 'internal risk management to external parties'[130] is quickly growing. The result has been new methodologies such as Cyber Supply Chain Risk Management (CSCRM) that weave together cyber-security, enterprise risk management and supply chain management.[131]

Having recognised the requirement, increased consideration has been paid to the cyber-vulnerabilities of supply chains. One prevalent example which complex fifth generation aircraft are particularly susceptible to is counterfeit computer chips. A piece of silicon embedded with an electronic circuit,[132] chips are the core component of all modern technology. Though difficult to discern from genuine chips even with close inspection, counterfeits have been found by the US Government to present a greater risk of failure.[133] Endangering the performance of systems they are incorporated into, these counterfeits, especially within the demanding environment of military aviation, present a credible risk to life if they fail during flight.

The scale of counterfeit chips being introduced into the military aviation supply chains is unknown, but it has been proved that US companies knowingly sold counterfeit chips made in China to the US military in 2010[134] and the US nuclear submarine fleet in 2013.[135] With the price of genuine chips rising by 20 percent in 2018,[136] and the US announcing a major review

[128] Verizon, *2018 Data Breach Investigations Report* (2018) 8, **https://www.verizonenterprise.com/verizon-insights-lab/dbir/**, accessed 15 June 2018.
[129] CERT-UK, Cyber Risks in the Supply Chain, 3.
[130] Jon Oltsik, John Gahm, Jennifer McKnight, "Assessing Cyber Supply Chain Security Vulnerabilities Within the U.S. Critical Infrastructure", *Enterprise Strategy Group Research Paper* (28 November 2010) 10, **http://www.nsci-va.org/CyberReferenceLib/2010-11-ESG%20Research%20Report%20Cyber%20Supply%20Chain%20Security.pdf** accessed 1 July 2018.
[131] Sandor Boyson "Cyber Supply Chain Risk Management: Revolutionizing the Strategic Control of Critical IT Systems", *Technovation*, 34 (2014) 342–353: 343.
[132] Tech Terms, "Computer Chip", *Hardware Terms* (2018) **https://techterms.com/definition/chip**, accessed 11 July 2018.
[133] Congressional Committee on the Armed Services, *The Committee's Investigation into Counterfeit Electronic Parts in the Department of Defense Supply Chain*, 8 (November 2011) 36, **https://www.gpo.gov/fdsys/pkg/CHRG-112shrg72702/pdf/CHRG-112shrg72702.pdf**, accessed 1 August 2018.
[134] Robert McMillan, "Woman Helped Sell Fake Chips to US Military", *PC World News* (23 November 2010) **https://www.pcworld.com/article/211428/article.html**, accessed 15 June 2018.
[135] Boyson, Cyber Supply Chain Risk Management: Revolutionizing the Strategic Control of Critical IT Systems, 343.
[136] Matthew Wilson, "Silicon Wafer Makers Plan 20% Increase in Price in 2018", *Kit Guru.net* (5 February 2018) **https://www.kitguru.net/components/graphic-cards/matthew-wilson/silicon-wafer-makers-plan-20-price-increase-for-2018-cpus-gpus-ram-and-nand-to-be-affected/**, accessed 1 July 2018.

of the F-35 project to reduce costs in the supply chain,[137] it is likely that smaller economically squeezed companies might continue the practice of sourcing cheaper counterfeit chips to remain economically viable.

Though the safety issues this practice represents are a major concern for military aviation, it is only one of many problems counterfeit chips represent. Amongst these, a pressing cyber-security consideration is malicious tampering. Whether occurring during their manufacture or added post-production, there is broad opportunity for counterfeit chips or other hardware from untrusted sources to be targeted by hostile actors before they enter the known supply chain.[138]

Discussing this, Borg highlights that altered circuitry containing malicious firmware could 'function in much the same way as malicious software...[allowing hostile actors to access] any network the component is connected to'.[139] This has already been proved to have occurred. In 2007, for example, hard drives produced in Thailand for US company Seagate and bound for the US military were found to contain a virus which facilitated a 'report-back' of all data to a Chinese Internet Protocol (IP) address.[140] Given this, it can be assessed that the risk of a hostile actor targeting a weak link in the supply chain to gain remote access to a fifth generation project is real.

A further related cyber-security concern are logic bombs. A form of malware, logic bombs are programmes designed to remain hidden and dormant until triggered by a pre-defined event or activity.[141] If embedded by a hostile actor into hardware destined for a fifth generation aircraft, it is feasible that a logic bomb could, in response to a certain event (such as entering the airspace of a specified nation), 'shut down the larger information systems'.[142] Alternatively, Borg warns that, in a worst case scenario, a logic bomb could even 'turn the equipment controlled by the information system against those operating it'.[143]

With such malware virtually impossible to detect once installed,[144] there is a credible risk that a hostile actor could, through a supply chain cyber-vulnerability, damage an air force's

[137] Aaron Mehta, "Top Pentagon Official Takes Aim at F-35 Cost, Supply Chain", *Defence News* (23 March 2017) **https://www.defensenews.com/air/2017/03/23/top-pentagon-official-takes-aim-at-f-35-cost-supply-chain/**, accessed 3 June 2018.
[138] Ibid.
[139] S. Borg, "Securing the Supply Chain for Electronic Equipment: A Strategy and Framework", *The Internet Alliance* (2010) 1, **https://obamawhitehouse.archives.gov/files/documents/cyber/ISA%20-%20Securing%20the%20Supply%20Chain%20for%20Electronic%20Equipment.pdf**, accessed 1 July 2018.
[140] Boyson, Cyber Supply Chain Risk Management: Revolutionizing the Strategic Control of Critical IT Systems, 343.
[141] S. Northcutt, "Logic Bombs, Trojan Horses and Trap Doors", *Sans Technology Institute* (June 2018) **https://www.sans.edu/cyber-research/security-laboratory/article/log-bmb-trp-door**, accessed 27 July 2018.
[142] Borg, Securing the Supply Chain for Electronic Equipment: A Strategy and Framework, 1.
[143] Ibid.
[144] Ibid.

operational effectiveness. In the extreme, if targeted correctly, the projection of air power could even be prevented. Based upon this, there is an imperative for air forces to understand and control their supply chains.

A requirement recognised by the UK for not just the Royal Air Force (RAF) but across Defence, the Ministry of Defence (MOD) introduced its own cyber supply chain security initiative in the form of the Defence Cyber Protection Partnership (DCPP). Acknowledging the need to use an existing building block to achieve timely introduction, the DCPP was based on the UK Government's broader Cyber Essentials Scheme (CES). An initiative launched in 2014 to achieve basic cyber security standards for all UK Government suppliers,[145] the programme included a higher level of CES Plus for suppliers assessed to be at a greater risk of cyber-attack.

Recognising the heightened nature of cyber risks to a military supply chain, and the 'baseline' nature of the CES model, in using the CES the MOD also adopted enhanced measures for the DCPP. Designed to protect complex projects including the fifth generation F-35,[146] the standards were formalised in the Cyber Security Model (CSM)'[147] which is detailed in Defence Standard (DEFSTAN) 05-138.[148]

If robust, the DCPP should mitigate the vulnerabilities of Defence's supply chains, including those supporting the RAF's fifth generation aircraft, to a level which removes the area as a credible cyber-threat to military aviation. To assess whether this is achieved, it is necessary to review the DCPP requirements at its strongest level of 'High' risk. As suppliers at this level are also required to meet CES Plus requirements, these standards should be concurrently considered. To do this in a structured manner, five key areas of cyber-security have been examined: boundary firewalls, secure configuration, user access control, malware protection and patch management.

The first – boundary firewalls – focuses on restricting network traffic to authorised connections. Intended to protect internal networks 'against unauthorised access and disclosure from the internet',[149] to meet DCPP and CES Plus requirements suppliers must maintain a network security system.

---

[145] Ministry of Defence, *Defence Cyber Protection Partnership Cyber Security Model Industry Buyer and Supplier Guide* (June 2018) 1, **https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/718566/20180203_Cyber_Industry_Buyer_and_Supplier_Guide_v2_1.pdf**, accessed 5 July 2018.
[146] Gov.UK, *Defence Cyber Protection Partnership* (2 June 2016), **https://www.gov.uk/government/collections/defence-cyber-protection-partnership**, accessed 5 June 2018.
[147] Ibid.
[148] Ibid.
[149] Department for Business, Innovation and Skills, *Cyber Essentials Scheme Requirements for Basic Technical Protection from Cyber Attacks* (June 2014) 5, **http://www.cyberstreetwise.com/cyberessentials/files/requirements.pdf**, accessed 10 June 2018.

Although meeting this requirement is an 'important element in securing data from unauthorised attacks',[150] achieving it in isolation has limited value against a sophisticated attacker. As Mao, Zhe and Li describe, though firewall functions are essential, their effectiveness pivots on the security policy.[151] With neither the DCPP nor CES Plus requiring additional proactive 'management techniques and tools',[152] such as changing of default passwords and updating a devices' operating system,[153] firewalls may be of limited value. With industry standards including the Information Security Forum (ISF) framework clearly articulating this additional requirement,[154] it can be assessed that the DCPP and CES Plus lack of depth fails to mitigate this potential cyber-vulnerability.

Turning next to secure configuration, CES Plus acknowledges that, like firewalls, other 'computers and network devices cannot be considered secure upon installation'.[155] Because of this, both CES Plus and the DCPP require organisations to configure computers and network devices to 'reduce the level of inherent vulnerabilities'.[156] This includes steps such as the removal or disabling of unnecessary user accounts and software.[157]

Though this direction amounts to sound cyber-security practices, they are in reality minimum requirements which do not, without development, provide sufficient protection against a determined attacker. Taking passwords as an example, the DCPP requires suppliers to 'define and implement a policy to maintain the confidentiality of passwords'.[158] Acknowledged as an acceptable baseline, the DCPP should go further and acknowledge that passwords in isolation are no longer an acceptable level of security. As highlighted by Bonneau et al,[159] 'the continued domination of passwords over all other methods of end-user authentication is a major embarrassment'. To be relevant, the DCPP should therefore direct additional authentication

---

[150] Smirti Salarial and Nishi Madaan, "Firewall and Its Policies Management", *International Journal of Computer Science and Mobile Computing*, 3 (4) (April 2014) 359-367: 359.
[151] Huaqing Mao, Li Zhe and Mingbiao Li, "Current State and Future Development Trend of Firewall Technology", *8th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM)* (21-23 September 2012) **http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6478472**, accessed 21 June 2018.
[152] Salarial and Madaan, Firewall and Its Policies Management, 359.
[153] Wes Noonan and Ido Dubrawsky, "Managing Firewalls", *Cisco Press* (27 November 2007) **https://www.networkworld.com/article/2289079/lan-wan/chapter-11--managing-firewalls.html**, accessed 25 July 2018.
[154] Information Security Forum, *The 2011 Standard of Good Practice for Information Security*, (June 2011) **https://www.uninett.no/webfm_send/730**, accessed 22 June 2018.
[155] Department for Business, Innovation and Skills, *Cyber Essentials Scheme Requirements for Basic Technical Protection from Cyber Attacks*, 7.
[156] Ibid.
[157] Ibid.
[158] Ministry of Defence, *Defence Standard 05-138; Cyber Security for Defence Suppliers* (28 September 2017) 6, **https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/652597/20171016-Defence_Standard_05-138_Iss_2.gov.uk.pdf**, accessed 11 June 2018.
[159] Joseph Bonneau, Cormac Herley, Paul Van Oorschot and Frank Stajano, "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes", *2012 IEEE Symposium on Security and Privacy* (2012), 553-567: 553, **http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6234436**, accessed 23 June 2018.

systems including biometrics or access cards. Not revolutionary, this would bring suppliers in line with industry standards such as the ISF Control Framework (CF) on access management.[160]

Acknowledging that passwords are a singular example, it remains evident that the DCPP and CES Plus fall short of contemporary security practices. Given this, secure configuration is again an area within the supply chain which is not being effectively mitigated if baselines are not being exceeded.

Within a third area – user access control – the CES Plus requires organisations to ensure that user accounts are only assigned to employees authorised to hold the relevant levels of access.[161] This is reflected in the DCPP standards to a less specified extent with the requirement to 'define and implement a policy to monitor user account usage and to manage changes of access rights'.[162] In evaluating whether these measures are sufficient, it is instructive to compare them against industry standards. Within ISO 27001,[163] for example, the requirements provide a similar level of assurance. If one were to criticise, it could be argued that all current standards fail to address the importance of the Systems Administrator who 'sets authorisations on the basis of the security policy'[164] and must therefore be 'trusted to conform to procedural and administrative controls'.[165] Because, however, this is a common oversight, it would be fair to conclude that the DCPP and CES Plus do provide a suitable level of assurance.

This trend is not, however, continued in malware protection. Referring to protecting systems that are connected to the internet or have imported software from malware, CES Plus requires dedicated software monitors to detect and disable malware.[166] This is reflected in the DCPP requirement to control the exchanging of information via removable media, use Intrusion Detection Systems (IDS) and control the use of authorised software.[167]

---

[160] Information Security Forum, *The 2011 Standard of Good Practice for Information Security*, CF 8.2.
[161] Department for Business, Innovation and Skills, *Cyber Essentials Scheme Requirements for Basic Technical Protection from Cyber Attacks*, 9.
[162] Ministry of Defence, *Defence Standard 05-138; Cyber Security for Defence Suppliers*, 12.
[163] BSI Standards, 'BS ISO/IEC 27001:2013 - Information Technology Security Techniques Information Security Management Systems Requirements (Incorporating Corrigenda September 2014 and December 2015)', *BSI Standards Publication* (2015) **https://extranet.cranfield.ac.uk/Download/bsol.bsigroup.com,SSL+SubscriptionPdfDocument?materialNumber=0000000**, accessed 22 June 2018.
[164] Ravi Sandhu and Pierangela Samarati, "Access Control: Principle and Practice", *Communications Magazine*, 32 (9) (1994) 40-48: 40.
[165] David Ferraiolo, Dennis Gilbert and Nickilyn Lynch, "An Examination of Federal and Commercial Access Control Policy Needs", *Proceedings of the 6th NIST-NCSC National Computer Security Conference, Baltimore* (20-23 September 1993) 109, **https://books.google.co.uk/ books?hl=en&lr=&id=vQEHUD51YNEC&oi=fnd&pg=PA107&dq=N.+(1993),+%E2%80%98A**, accessed 24 June 2018.
[166] Department for Business, Innovation and Skills, *Cyber Essentials Scheme Requirements for Basic Technical Protection from Cyber Attacks*,10.
[167] Ministry of Defence, *Defence Standard 05-138; Cyber Security for Defence Suppliers*, 10.

Considered to be a baseline requirement, the DCPP and CES Plus direction is essential. With CERT-UK warning, however, that 'attackers continue to evolve',[168] and Stange assessing that organisations must go beyond baselines and 'note the limitations of anti-malware products',[169] there is a requirement for suppliers to exceed DCPP and CES Plus. This is underlined by software company OPSWAT, which comments that 'installing an antivirus product is the first, not last, step to having a safe and secure computer'.[170] As a result, there is again concern that whilst baselines are directed, a robust level of assurance within the supply chain will not be achieved at the specified levels.

Turning to the final area – patch management – we see another example of baseline provision by the DCPP and CES Plus. Discussing a process in which vendors 'try to provide fixes for identified vulnerabilities',[171] CES Plus recognises the requirement directing suppliers to, as a minimum, maintain licences, remove out-of-date software and install security patches. This is reflected by the DCPP's requirement to patch and review risk where patching is not possible.[172]

Acknowledging Gerace and Cavusoglu's[173] assessment that the routine application of security patches would prevent an estimated 95 percent of security breaches, patch management is essential. With the DCPP and CES Plus reflecting this, it is one area where the baseline practices directed meet industry norms and should therefore provide sufficient assurance within the supply chain.

Considering this review of DCPP and CES Plus against the prior discussion of 'weak links' and supply chain cyber-vulnerabilities, a troubling picture emerges. Subject to concerted cyber-attack by hostile actors, air forces face a concerning challenge in securing cyber-elements of their supply chains. Despite acknowledging this through initiatives such as the UK MOD's DCPP, the analysis suggests that, in the UK at least, measures to manage the risk are insufficient. Defined at best as industry baseline standards, and at worst as a failure to meet the contemporary cyber-challenge, the reality is that the supply chain of air forces remains vulnerable to exploitation.

Based upon this analysis, and working on the assumption that the UK example is indicative of all modern air forces, it is concluded that military aviation's supply chains are not adequately

---

[168] CERT-UK, "An Introduction to Malware", *CERT-UK White Paper* (2014) 5, **https://www.cert.gov.uk/wp-content/uploads/2014/08/An-introduction-to-malware.pdf**, accessed 25 June 2018.
[169] Szilard Stange, "Detecting Malware Across Operating Systems", *Network Security*, 6 (2015) 11-14: 11.
[170] John Dunn, "Who Runs an Antivirus Scan These Days? Apparently Almost Nobody", *TechWorld* (28 January 2015) **www.techworld.com/news/security/who-runs-anti-virus-scanthese-days-apparently-almostnobody-3595951/**, accessed 25 June 2018.
[171] Department for Business, Innovation and Skills, *Cyber Essentials Scheme Requirements for Basic Technical Protection from Cyber Attacks*, 11.
[172] *Defence Standard 05-138; Cyber Security for Defence Suppliers*, 10.
[173] Thomas Gerace and Huseyin Cavusoglu, "The Critical Elements of the Patch Management Process", *Communications of the ACM*, 52 (8) (2009) 117-121: 117.

protected against the contemporary cyber-threat. Opening a door for hostile actors to degrade or even remove the ability to operate information-reliant aircraft, air forces should be deeply concerned by the credible cyber-threat to air operations which has been created by their compromised supply chains.

Personnel

Though systems, infrastructure and supply chains represent distinct cyber-security concerns, the final area of discussion, an air force's personnel, holds unique importance. This is because if information is 'the lifeblood of Defence'[174] then its people are the beating heart. As a result, if people act in a way which compromises information, Defence will 'bleed-out' and operational effectiveness will be lost.

This graphic analogy loses none of its relevance when discussing air power in a fifth generation environment. With people, despite advances in technology, still entwined at every step of projecting air power there are no areas which do not rely on people's ability to protect information. Whilst this is an intuitive statement, the integral security role of an organisation's people was only recognised relatively recently.

Research by Briney and Prince, for example, suggests that as long as 15 years ago large private companies were on average spending $6m per annum on information security.[175] With nearly 20 percent of this focused on security products,[176] the driving force within cyber-security was traditionally on protection from external attack. This was mirrored within Defence sectors, including in the UK, which dedicates the majority of its DCO budget on outwardly focused capabilities. The flagship amongst these is the Global Operations Security Control Centre (GOSCC) at MOD Corsham. Leading on the MOD's 'Operate and Defend' mission, it manages the raft of technical solutions which support the delivery of DCO.[177]

Though the external threat managed by these means cannot be underestimated, Herath and Rao identified that an organisation's contemporary security depends on three components: people, processes and technology.[178] Encouraging a shift in mainstream thinking, Leach also suggested that there is an increasingly accepted assessment that the people and process

[174] Ministry of Defence, *JSP 441 – Managing Information in Defence – Part 1: Directive* (January 2017) 1, **https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/618489/JSP441_Part1.pdf**, accessed 1 July 2018.
[175] Andrew Briney and Frank Prince, "Does Size Matter", *Information Security*, 5 (9) (2002) 36-39: 36.
[176] Ibid.
[177] House of Commons Defence Committee, *Defence Committee: Further Written Evidence from the Ministry of Defence – The Global Operations Security Control Centre (GOSCC)* (June 2012) **https://publications.parliament.uk/pa/cm201213/cmselect/cmdfence/106/106we05.htm**, accessed 15 May 2018.
[178] Tejaswini Herath and Raghav Rao, "Encouraging Information Security Behaviours in Organizations: Role of Penalties, Pressures and Perceived Effectiveness", *Decision Support Systems*, 47 (2) (2009) 154-165: 154.

elements, which represent threats internal to an organisation, potentially pose the greatest risk to information.[179] A conclusion supported by cyber-security companies including Symantec (which in 2012 identified the subcategories of 'negligent insiders and malicious [internal] attacks'),[180] academics such as Noonan and Archuleta have suggested that security professionals finally woke up to the internal threat.[181]

A concept which focuses on current employees using 'specialised knowledge...[to gain an] advantage over security efforts',[182] this thinking engendered a growing consensus amongst security professionals. Specifically, it is now accepted that whilst 'an adversary who makes a frontal attack can be anticipated or repulsed...[one who] attacks from within...cannot be readily countered'.[183]

An example of this internal attack and the damage it can cause was the 2013 actions of Edward Snowdon, a US National Security Agency (NSA) contractor, who downloaded an estimated 1.7 million classified documents before leaking some to *The Guardian* newspaper.[184] From a sympathetic perspective, Snowdon is a whistle-blower who provided a necessary 'window into the NSA and its international intelligence partners' secret mass surveillance programs and capabilities'.[185] Conversely, however, the breach is assessed by official sources to have caused extensive damage. A declassified US House of Representative report for example stated that the breach 'caused tremendous damage to national security...[including to] military programmes of great interest to [US] adversaries'.[186]

Placing the Snowdon example in the context of a contemporary air force, it is possible to see how such a breach could cause major damage to the success of a fifth generation project.

---

[179] John Leach, "Improving User Security Behaviour", *Computers and Security*, 22 (8) (2003) 685-692: 685.
[180] Symantec, "2011 Cost of Data Breach Study: Global", *Ponemon Institute*, March (2012) 2, **http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-ofdata-breach-global.en-us.pdf**, accessed 15 May 2018.
[181] Thomas Noonan and Edmund Archuleta, "Final Report and Recommendations on the Insider Threat to Critical Infrastructures", *The National Infrastructure Advisory Council* (8 April 2008) 32, **http://ftp.scadahacker.com/library/Documents/Insider_Threats/NIAC%20%20Insider%20Threat%20to%20Criticail%20Inf**, accessed 15 May 2018.
[182] Department of Homeland Security, "National Risk Estimate: Risks to U.S. Critical Infrastructure from Insider Threat", *National Protection and Programs Directorate Office of Infrastructure Protection*, December (2013) 3, **https://scadahacker.com/library/Documents/Insider_Threats/DHS%20%20Risks%20to%20US%20Critical%20Infrastruct ure%20from%20Insider%20Threat%20%2023%20Dec%2013.pdf**, accessed 17 May 2018.
[183] Nicholas Catrantzos, "No Dark Corners: Defending Against Insider Threats to Critical Infrastructure", *Naval Postgraduate School* (September 2009) 1, **http://calhoun.nps.edu/bitstream/handle/10945/4656/09Sep_Catrantzos.pdf?sequence=1**, accessed 21 May 2018.
[184] Michael Kelley, "NSA: Snowden Stole 1.7 Million Classified Documents and Still has Access to Most of Them", *Business Insider* (13 December 2013) **http://www.businessinsider.com/how-many-docs-did-snowden-take-2013-12?IR=T**, accessed 8 May 2018.
[185] The Courage Foundation, *Who is Edward Snowdon?* (2018) **https://edwardsnowden.com/**, accessed 12 May 2018.
[186] United States House of Representatives, *Review of the Unauthorised Disclosure by Former National Security Agency Contractor Edward Snowden* (15 September 2016) **https://intelligence.house.gov/uploadedfiles/hpsci_snowden_review_declassified.pdf**, accessed 1 July 2018.

Whether leaks pertained to the release of technical details leading to a loss of comparative advantage, or the identification of vulnerabilities reducing operational effectiveness and endangering mission success, the impact could be extensive.

Although such malicious insider breaches are of concern, some argue that the true risk is from non-malicious insiders. This sub-group is defined by Nurse et al as those 'without malicious intent who through action or inaction [cause] harm'.[187] Potentially broad in its manifestation and impact, examples range from the accidental loss of work devices to the publishing of sensitive information on social media.

Given the preventable nature of non-malicious insider events, security professionals quickly adopted clichés including 'behind every computer error, no matter how massive, is one or more humans'.[188] Leading to personnel being treated 'as a security risk to be controlled',[189] this newfound concern has developed into a rut of one-dimensional thinking on punishment being the key to managing non-malicious insiders.

An illustrative example of this persistent issue exists in UK Defence. Whilst the MOD's policies on controlling their personnel's security practices may appear robust, open source reports suggest that the approach is not working. In 2018, for example, the UK Government confirmed that the MOD, including in part the RAF, lost through their personnel's negligence 30 desktop computers, 81 laptops and one tablet in the Financial Year 2017/18.[190] Illustrating the damage such losses can cause, *The Guardian* reported in 2008 that amongst that year's MOD losses of 503 laptops, one contained the personal details of 600,000 applicants to the UK Armed Forces.[191]

When explored further, this example becomes deeply concerning. Not simply a major Data Protection issue, the loss of personal information could be used to identify and target military personnel likely to be employed in sensitive areas. Invaluable to those with hostile intent, Foreign Intelligence Services (FIS) could use this information alongside other open-source information including social media to build personal profiles. Having obtained this information,

---

[187] Jason Nurse, Oliver Buckley, Philip Legg, Michael Goldsmith, Sadie Creese, Gordon Wright and Monica Whitty, "Understanding Insider Threat: A Framework for Characterising Attacks", *Security and Privacy Workshops* (May 2014) 214-228: 214. **http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6957307**, accessed 11 May 2018.
[188] info security, *The User is Not The Enemy: How to Increase Information Security Usability* (3 August 2009) **http://www.infosecurity-magazine.com/magazine-features/the-user-isnot-the-enemy-how-to-increase/**, accessed 20 June 2018.
[189] Ann Adams and Martina Sasse, "Users Are Not the Enemy", *Communications of the ACM*, 42 (12) (1999) 40-46: 40.
[190] T. Ellwood, 'Ministry of Defence Computers: Written Question - 141014', *UK Parliament; Written Questions and Answers* (18 May 2018) **https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2018-05-03/141041/**, accessed 4 June 2018.
[191] James Sturcke, "Laptop Lapses Which Embarrassed Government", *The Guardian* (12 June 2008) **https://www.theguardian.com/politics/2008/jun/12/defence.terrorism**, accessed 3 June 2018.

a FIS could identify how to manipulate an individual to provide information or take actions which would allow a technical attack on a system.[192]

This process, commonly referred to as social engineering, is defined by Gafhir et al as 'an ultimate psychological manipulation technique used by attackers to generate responses from unwilling targets'.[193] The result of this when successful can range from gaining access to a workplace through to obtaining state secrets.[194]

Taking the Stuxnet attack on Iranian nuclear centrifuges as an example, some analysts have suggested that it is exactly this process that led to social engineering in the form of well-targeted 'spear phishing' emails. When received, these emails may have contained convincing personal details which lured insiders to unwittingly run infected programs, allowing the Stuxnet malware to be introduced.[195] Though alternate explanations suggest that Stuxnet may have been caused by an employee 'deliberately loading malware from removable media like a USB memory stick'[196] the foundation remains the same: breaches of information concerning an organisation's people can lead to an adversary socially engineering a target to facilitate a major cyber-related incident.

For a fifth generation air force which relies on interconnected systems, this issue is ever growing. In the modern air force there is a necessity to process an immense amount of data which requires access being granted to not only Service Personnel and Civil Servants but also civilian contractors. With many of these providing often opaque routes into sensitive systems, it is no longer the case that those solely granted high level access can cause significant breaches. Rather, everyone – from the administrative assistant to the intelligence officer – if targeted effectively by a hostile actor, can provide a route into a sensitive system.

Beyond this angle of social engineering, non-malicious insiders can also cause breaches through their day-to-day use of social media. With 62.5 percent of the UK population expected to be active social media users by 2021[197] it is a growing reality that the majority of people will chronicle every aspect of their lives online.

---

[192] Aditya Sood and Richard Enbody, "Targeted Cyber Attacks: A Superset of Advanced Persistent Threats", *IEEE Security and Privacy* (January 2012) 54-61: 55.
[193] Ibrahim Ghafir, "Security Threats to Critical Infrastructure: The Human Factor", *The Journal of Supercomputing* (26 March 2018) 1-17: 2.
[194] Ibid.
[195] Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare", *Security Studies*, 22 (3) (2013) 365-404: 381.
[196] Ibid.
[197] Statista.com, *Forecast of Social Network User Numbers in the United Kingdom (UK) from 2015 to 2022 (in million users)* (2018) **https://www.statista.com/statistics/553530/predicted-number-of-social-network-users-in-the-united-kingdom-uk/**, accessed 14 June 2018.

A trend recognised in the UK by the MOD, guidance for military personnel on the appropriate use of social media has been published.[198] Despite these attempts to educate, media reporting in 2018 indicated that members of the UK Armed Forces continue, through social media, to 'compromise operations and national security'.[199] According to Freedom of Information (FoI) requests published by *The Telegraph*, this has included, amongst a list of other examples, SECRET information being published on LinkedIn and a 10 minute *YouTube* video of personnel and equipment on deployment in Afghanistan.[200]

Even though there is nothing to suggest that such breaches are malicious, their occurrence creates a significant security concern. With academic literature acknowledging 'a rapid and massive growth in cyber-exploitation operations'[201] from states including China, it can be assessed that adversaries are not just attacking systems but are actively monitoring social media for breaches of information. Based upon this, the collective damage of self-induced social media breaches may greatly undermine the security of a nation's sensitive military information.

Taken in the context of a fifth generation air force, the potential areas of damage are significant. From the posting on social media of photos of sensitive information on operations boards and cockpits, through to details of aircraft capabilities, there is broad scope for an adversary to easily collect open-source information which may undermine air operations.

In its totality, the risk posed by an air force's own people to either maliciously or inadvertently cause information breaches is concerning. Understanding and accepting this is the first stage; appreciating how to manage it is an altogether more demanding process. Requiring a focus on the psychology of the individual and how to induce them to follow established policies, an air force's strategic leadership must direct concerted effort towards research and development in this area. If they do not, and their own people continue to pose a cyber-security vulnerability, the operational effectiveness of military aviation will continue to be degraded by security breaches that could have been avoided.

Conclusion

This article explored military aviation's contemporary cyber challenge by asking whether cyber vulnerabilities are a credible threat to a modern air force. Beginning with a discussion of the relevant concepts, the article highlighted the requirement to understand cyber-vulnerabilities within the context of an air force's operational delivery. Specifically considering the modern air

[198] Ministry of Defence, *Social Media Guide* (2012) **https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/34247/social_media_i nfo_card.pdf**, accessed 10 June 2018.
[199] Ben Farmer, "Troops Leaked Confidential Data on Twitter and Facebook", *The Telegraph* (8 July 2018) **https://www.telegraph.co.uk/news/uknews/defence/10948490/Troops-leaked-confidential-data-on-Twitter-and-Facebook.html**, accessed 9 July 2018.
[200] Ibid.
[201] Nigel Inkster, "Chinese Intelligence in the Cyber Age", *Survival*, 55 (1) (2013) 45-66: 58.

force's operation of fifth generation aircraft in a fifth generation environment, it was identified that the issue would be examined through an analysis of four fundamental aspects of aviation: systems, infrastructure, supply chains and personnel.

Turning first to consider the systems which deliver modern military aviation, it was noted that the area has become increasingly complex. Driven by the advent of NextGen e-enabled aircraft, the human element has been reduced by a reliance on the processing of information. With evidence that the information held within these complex systems can be compromised through the cyber-domain, the article warned that as adversaries become increasingly sophisticated, there is a rising chance of cyber-attacks impacting on operations.

To address whether this is a pressing issue for military aviation, the article considered two key systems: UAVs and the F-35. Initially examining UAVs, it was concluded that whilst cyber-attacks on UAVs may be difficult to execute, they are nonetheless possible. Reason enough to be troubled, the conclusion was balanced by an acknowledgment that UAVs' unique autonomous nature makes them more vulnerable to cyber-attack.

Turning next to the F-35, it was identified that ALIS is the aircraft's key system. Exploring open-source reports regarding its security failings, and noting a 2017 US OTE report which confirmed that identified vulnerabilities had not been remedied,[202] it was asserted that there is mounting evidence of a cyber-threat to air forces operating the F-35. Taking this in the context of previous discussions, it was concluded that the cyber-vulnerabilities of those systems which are integral to cutting-edge aircraft represent a persistent and credible threat to modern military aviation.

Moving next to examine the issue of infrastructure, the article identified that unlike other forms of military power, the impermanence of aviation makes air power uniquely dependent on infrastructure. Similar to the civil concept of Critical Infrastructure, this means that the loss or compromise of infrastructure could cause significant disruption to air operations.

Responding to this, it was noted that air forces have become world-leaders in layered physical and procedural security measures. Though robust, with the cyber-threat able to circumnavigate these measures, and modern infrastructure extensively reliant on ICT, examples including the 2015 attack on the Ukrainian power grid were explored to show potential vulnerabilities of aviation. Having extended the discussion to the more specific example of SCADA systems, it was acknowledged that militaries are limited in the level of influence they can exert on a large amount of air power's supporting infrastructure. Due to this, and the ability of resilience planning to mitigate the impact, it was concluded that the cyber-threat to

[202] Operational Test and Evaluation Agency, F-35 Joint Strike Fighter, 33.

an air force's infrastructure is concerning but is not the greatest cyber-vulnerability facing modern military aviation.

A third area highlighted for consideration was the securing of supply chains. Commenting on the complexities created in the modern inter-connected world, it was specifically noted that the delivery of fifth generation aircraft creates a heightened requirement for support.

Citing the F-35 as an example, and exploring the concept of cyber-supply chain security further, it was established that the 'weakest link' often resides within smaller firms with lower cyber-security provision. Increasingly recognised, organisations have begun to regulate their suppliers to ensure cyber-security compliance. Within UK Defence, the article noted that this is being attempted through the DCPP. Aligned to the broader UK Government CES initiative, five key areas of cyber-security provision were examined. Having done so, the article concluded that the DCPP and CES Plus at best require defence suppliers to meet industry baseline standards. At worst, however, they show a concerning failure to meet the contemporary cyber challenge. Based upon this, it was concluded that if the UK example is indicative of all air forces, strategic leaderships should focus on overcoming the cyber-vulnerabilities that supply chains are exposing their organisations to.

The final area considered was an air force's personnel. Developing the well-known phrase of information being 'the lifeblood of Defence',[203] the article likened its people to a beating heart. Expanding this analogy, it was suggested that the causing of cyber-security breaches by its people will lead Defence to 'bleed-out' and operational effectiveness to be lost.

Building upon this, the article discussed how people are entwined at every step of projecting air power. Playing an integral role in security, it was noted that breaches can occur from malicious actors such as Edward Snowdon through to non-malicious personnel who cause incidents through negligence or as a result of manipulation by hostile actors. With media reports showing that UK Defence continues to experience breaches, particularly through non-malicious activity, the article concluded that for a fifth generation air force which relies on interconnected systems, this issue is ever growing. Because of this, it was suggested that air forces must work to understand and manage the issue. If they fail to do so, their own people's mistakes will continue to cause an avoidable degradation of operational effectiveness.

Considered in its totality, the article presented a troubling picture of the cyber challenge for military aviation. Across the four lenses used to explore whether cyber-vulnerabilities represent a credible threat to modern air forces, the analysis found concerning aspects in all. An area where some reassurance can be sought is infrastructure. Here, strong resilience planning aligned with the robust approach of organisations including the NCSC provides a good level

[203] Ministry of Defence, *JSP 441 – Managing Information in Defence – Part 1: Directive*, 1.

of assurance. Through this, an air force's infrastructure is protected from cyber-attack or, where attacks occur, the impact can be mitigated to a level that will prevent any major degradation of air operations.

Further good news can be found in an air force's personnel. Though media reports indicate that UK Defence continues to be troubled by its personnel's non-malicious breaches, and a future 'Snowdon' is difficult to predict, it is an issue which the strategic leadership can manage. With sufficient resource, there is good potential to understand the motivation of its people and, thereafter, develop means to prevent future losses. Such optimism must, however, be cautioned with a requirement to invest. If the strategic leadership does not provide the resources required, or fails to lead by example, its people are likely to continue to falter and, through faltering, cause damaging losses.

Whilst positive assessment can be found, the two other areas explored – systems and the supply chain – are far more concerning. This articles examination of systems identified how, by its very nature, cutting edge air power, through its reliance on information and the systems that process it, is highly susceptible to cyber-attack. Further, the examination of the F-35's ALIS showed long-standing and unresolved problems. From its position as a 'single point of failure', through to the deeply concerning examples of previous breaches, there is a plethora of areas to concern an air force's strategic leadership.

Though limited in their ability to address the information-reliant aspect of modern aviation, and likely restricted in their ability to meaningfully impact on the failures of existing projects led by other nations, the strategic leadership can nonetheless act to manage future failure. With new aircraft under development, the lessons identified by UAVs and the F-35's ALIS must be recognised, reflected upon and fed into future programmes. If this is done robustly, there is hope for enhanced cyber-resilience. If it is not, there will be growing examples of adversaries exploiting system vulnerabilities and impacting on the viability of modern air power.

Leading to the other area of concern – the supply chain – air forces are arguably presented with the most pressing worry. Unlike systems which are, by their nature, unavoidably vulnerable, supply chains have, in response to austerity, been allowed to become immensely complex. Added to this, the means put in place to ensure cyber-resilience in the supply chain have, taking DCPP and CES Plus as an example, fallen disturbingly short of even industry baseline standards for cyber-security. With the Defence sector experiencing an arguably more complex threat from its potential adversaries, it can therefore be assessed that the supply chains of modern air forces are already compromised.

In response to this, air forces must return to the 'drawing board' and reassess the level of cyber-security they are demanding of their suppliers. Taking the UK as an example, the DCPP, though a fair starting point, is not thorough enough. It requires depth with, as a minimum, compliance of industry standards such as the ISO 27001 series. This then needs to be

implemented alongside much simpler supply chains. If this can be achieved, the vulnerabilities presented by the supply chain may be controlled; if it is not, adversaries will continue their infiltration of supply chains which will reduce advantage and, most worryingly, compromise in an unseen manner an air force's ability to project air power.

In conclusion, cyber-vulnerabilities are, based upon the above discussion, a credible threat to modern air forces. Notwithstanding this, the threat is in part controllable. To achieve this control, and proactively manage the cyber-vulnerabilities which threaten military aviation's operational effectiveness, there is a requirement for the strategic leadership of air forces to first acknowledge the scale of the cyber-challenge. Having done so, they must next commit sufficient time and resource to the serious, in-depth and reflective study of the concerns highlighted by this article. If this is achieved, most pressingly within the areas of systems and the supply chain, and subsequent recommendations are followed, it will be possible to ensure that cyber-vulnerabilities do not significantly degrade the effectiveness of modern military aviation. Alternatively, if strategic leaderships ignore the problem, or approach it in an uncoordinated manner, modern air power's relevance to contemporary operations will be systematically destroyed by hostile actors' exploitation of military aviation's cyber-vulnerabilities.