Cyberspace Conflict: A New Phenomenon or an Extension of the Enduring Role of Information Warfare?

By Squadron Leader Paul Withers

Biography: Squadron Leader Paul Withers is an Engineer Officer, currently commanding Support Squadron on the Tactical Imagery-Intelligence Wing (TIW) at RAF Marham. He has professional experience and expertise in the Cyber world including a tour at the Joint Cyber Unit (Cheltenham) and was embedded with US Cyber Command in Afghanistan. A CAS' Fellow, Paul is currently undertaking an MSc in Cyberspace Operations.

Abstract: This article sets out a brief history of cyberspace conflict, citing examples that are significant in its evolution. It charts the enduring importance of information as a constituent part of warfare, through the development of the science of cybernetics, and the symbiotic relationship between the development of military systems and advances in computer technology. It examines the advent of Information Warfare and the 'information-age paradox' of opportunities afforded by technology, bringing with them a range of new threats. The article examines the rise of cyberspace as an operating environment, gives examples of operational cyber integration and discusses the development of the United Kingdom's strategic approach. In doing so it attempts to highlight the need for detailed study of cyberspace history to inform strategy, concepts and doctrine.

Introduction[1]

'Cyber conflict is new, but not so new that it has failed to accumulate its own history'[2]

Military history, when appropriately studied and applied, can give great insight to the military profession, by drawing upon the lessons of the past. When a new concept or technology is applied to warfare, the importance of its history may not be immediately apparent, but the need to capture facts and first hand accounts as they occur, for later analysis, should be obvious. Accounts, analyses and theories of war stretch back to Thucydides, Sun Tzu, through the works of Clausewitz, Jomini and Mahan, to the emergence of War Studies as a formal academic discipline. A century ago, the significance of air power started to emerge; it was only a few years after the end of the Great War that the first interpretations of air power history were authored. In 1922, Sir Walter Raleigh published the start of his analysis of the records collected by the Air Ministry's Historical Section with the first volume of *'The War in the Air; Being the Story of the Part Played in the Great War by the Royal Air Force.'*[3] H.A. Jones continued Raleigh's work after his death, and *The War in the Air* eventually ran to six volumes. Raleigh and Jones' work was on the leading edge of an enormous breadth and depth of study of air power over the past one hundred years. At the start of the 21st Century, cyberspace has emerged as an operating environment, and it too must begin to have its history laid down. Much of what has been written about cyberspace is speculative and alarmist, but there is a growing body of empirical study that can aid the broader understanding of conflict in cyberspace.

This article can only give a brief overview of that history. It does not purport to be a history of computer science or information technology in the round, but instead focuses on the history of cyberspace as an operating environment, or in US doctrinal terms, a Domain of War.[4] Determining an appropriate start point for a history of cyberspace is problematic. It could be argued that the start point was the first documented examples of espionage through cyberspace, the invention of the microprocessor, or even back to the emergence of the programmable computer. This paper will argue that cyberspace, though related to 'the interdependent networks of information technology infrastructures… and the data therein,' has a lineage that stretches back before the 'Information Age'.[5] The concept of cyberspace as a war-fighting environment has its antecedence in the historical use of information in war and in the use of communications technology, particularly for Command and Control. It reflects a conceptual debate, which has largely been led by the United States (US) military, but is echoed more broadly around the world. In this paper, the history of the cyberspace environment will be analysed from the historical use of information, through the emergence of communications technology, up to the cyberspace era. The US only formally declared cyberspace as a 'Domain' as late as 2006. However, the declaration of this new domain was not a sudden epiphany of a military role for cyberspace; rather it reflected an age-old reliance on information, coupled with more recent advances in technology.

The article will be presented in six steps. First, it will examine the Early History of cyberspace, giving examples of the use of information from its ancient origins up to the 20th Century and its significance up to and including the Second World War. Second, it will discuss its development during the Cold War, the point at which 'cybernetics', the science of control systems, became embedded in western military concepts and capabilities. Third, the impact of the so-called 'Revolution in Military Affairs' will be considered. The 1991 Persian Gulf War heralded the importance of information and networks in warfare, but it also demonstrated the dangers of technological dependence. Fourth, it will look more broadly at a history of cyber 'conflict' tracking the realisation of the threat, the development of responses and the eventual militarisation of cyberspace as a war-fighting environment. Consideration will then be given to specific historical examples where operations in cyberspace have been integrated with broader military operations. Sixth, the development of the UK's strategic approach to cyberspace will be examined. Finally, the paper will conclude with an overall assessment of the history of conflict in cyberspace. It will argue that, like the other operating environments, we must capture, synthesise and analyse the empirical record in order to develop the history of cyberspace. In advocating the historical study of Air Power, Peter Gray argues for a 'notion of history as an interpretation of the past in which a serious attempt is made to filter out myth and legend.'[6] This applies as much to the study of the history of cyberspace as it does to that of air power. The cyber debate is replete with hyperbole and myth and examples are often used to extrapolate the likely future, without a robust analysis of past events.

Early History

The use of information in support of operations on land has been an enduring theme of warfare and military strategy, with information-based deception and Command and Control (C2) dating back to ancient times. The means of establishing and maintaining C2 across vast distances had been employed by the 13th and 14th Century Mongol Empire through the use of a network of 'Arrow Riders', who ensured that information could be passed in hours or at worst a few days across the breadth of the Empire.[7] The Mongols exploited the technology of bow and arrow to relay messages across the 'network' at a speed far in excess of that achievable by men on horseback alone. This communications network allowed much greater control of the Mongol forces, enabling them to 'first disrupt an enemy's communications, then to strike at his heart'.[8]

The industrial age produced a technological emulation of the Arrow Riders through the military adoption of the telegraph. During the American Civil War, effective C2 was enabled by the use of telegraph communications.[9] However, the reliance on the telegraph led to a new vulnerability, a 'foreshadowing of the information-age paradox that technological advances can simultaneously empower and imperil'.[10] The importance of the telegraph in achieving effective C2 meant that forces had to be diverted to protect the telegraph network. The Union Army used the vulnerability of the telegraph to their advantage by capturing Confederate telegraph stations and using them for deception operations.[11] Earlier innovations of the industrial revolution, such as Joseph-Marie Jacquard's automatic weaving loom and Charles

Babbage's designs for the 'Analytical Engine' are arguably also precursors of the computer technology that led to what we now know as cyberspace.[12] Babbage collaborated with Ada Lovelace, who developed his ideas and is credited with anticipating, in the 19th Century, some of the underpinning concepts of computer software that could not be realised practically until the second half of the 20th Century.[13]

At the turn of the 20th Century, the power of the Royal Navy, with its famous 'Dreadnought' Fleet, was transformed on the initiative of Admiral 'Jacky' Fisher. This transformation included the creation of an Empire-wide intelligence and communications network. Enabled through the use of emerging radio technology, the aim of this network was to track the position of vessels across the vast reaches of the British Empire, and led to Fisher's bold assertion that 'not a dog will wag its tail without being reported'.[14] However, the emergence of wireless telegraphy as a means of communicating over great distances gave rise to what later became known as Signals Intelligence (SIGINT). Another example of foretelling the 'information-age paradox,' wireless telegraphy was extremely vulnerable to eavesdropping and in order to protect the confidentiality of the information, codes and cyphers were developed. The great powers invested significant effort into breaking each other's cyphers to gain 'information advantage' through SIGINT. A notable First World War example was when the British decrypted the 'Zimmerman Telegram', which in many analyses was 'central in bringing the United States into the First World War on the side of Britain and France'.[15] The German Foreign Minister, Arthur Zimmerman, had suggested an alliance with Mexico against the United States. In return, Zimmerman offered the return of lost Mexican 'territories in Texas, New Mexico and Arizona'.[16]

During the Second World War, the crucial role of information in ensuring effective C2 was very much in evidence during the Battle of Britain. The Commander-in-Chief of RAF Fighter Command, Sir High Dowding, 'had created the world's first fully integrated air defence system'.[17] The ability to quickly collect, filter and disseminate information up and down the chain of command enabled the RAF to concentrate its fighter aircraft against incoming bombing raids and therefore overcome the numerical advantage of the German Luftwaffe. Whilst history rightly credits the bravery of the aircrew and the importance of emerging radar technology, the air defence system as a whole allowed aircraft to be concentrated in time and space. Arguably the Dowding System, in enabling the rapid flow of information from the various sensors to the decision makers, gave battle winning advantage. It ensured that Fighter Command aircraft could be efficiently and effectively directed to engage the Luftwaffe.

Perhaps the most important Second World War example of 'information warfare' was the advantage given to the UK and US through 'Ultra' intelligence. The ability to decrypt the various German and Japanese cyphers was so significant that Winston Churchill claimed that 'Ultra had effectively won the war'.[18] Given the numerous other factors that contributed to victory, Churchill might be accused of hyperbole but, although Britain's military forces were inferior in many ways, 'Bletchley Park was the one place where [they] enjoyed a crucial

world lead.'[19] Another crucial legacy of Bletchley Park for the future of cyberspace was the development of the Colossus machine, 'perhaps the first device that might be described as a "computer".[20]

Norbert Wiener's work on *cybernetics* during the Second World War was instrumental in the development of cyberspace. Wiener's work was centred on solving a military problem, controlling anti-aircraft artillery, but had much broader application in the science of control systems.[21] Wiener coined the term cybernetics from the Greek word for 'steersman'.[22] He aimed to solve 'the problem of hitting fast manoeuvrable [sic] bombers with ground-based artillery, [bringing] to bear his own established interest in feedback mechanisms, communication technology, and non-linear processes.'[23] Wiener's development of cybernetics set the scientific, engineering and philosophical basis for information-centric systems that underpinned later developments of cyberspace. Throughout the last century, developments in technology, most notably electrical and electronic engineering (latterly microelectronics) have had a symbiotic relationship with the development of military systems.

The Cold War

The post-Second World War era saw the start of an arms race between the Soviet Union and the West, ostensibly related to achieving nuclear weapons dominance, but underpinned by a scientific, technological, and deep-seated ideological battle that was a dominant force in the history of cyberspace.[24] From the late 1940s, Soviet science journals started to publish information on the early developments of Western computing technology, including a translation of the computer science pioneer Vannevar Bush's paper on the 'Differential Analyzer', an early analogue computer.[25] By 1949 the Soviet intent to bridge the gap with the West in digital computing was clear, and an open-source derived description of an American Stored Program Control digital computer was published.[26] As the Soviets developed their own computing power, it was largely devoted to military applications, with 'the nuclear weapons researchers… and the designers of ballistic missiles and spacecraft… [using] up almost all the resources of the first Soviet digital computer.'[27]

As the Cold War developed, the US scientific and engineering community attempted 'to shape military affairs into a perfectly modelled and controlled closed world.'[28] This was based upon Norbert Weiner's study of cybernetics and control systems, and was enabled by the computerisation of the US military.[29] This approach garnered support from senior military officers, including General William Westmorland who, in 1969, made a prescient speech regarding the integration of cybernetic systems into warfare:

> 'On the battlefield of the future, enemy forces will be located, tracked, and targeted almost instantaneously through the use of data links, computer assisted intelligence evaluation, and automated fire control… In summary, I see an Army built into and around an integrated area control system that exploits the advanced technology of communications, sensors, fire direction, and the required automatic data processing.'[30]

The technological developments of Cold War aircraft meant that decision-making in Air Defence systems became increasingly complex and required decision support calculations that stretched the capacity of human operators. In the late 1950s, the US announced the creation of the Semi Automated Ground Environment (SAGE), 'the first computer-based command, control and communications system for the purpose of constituting a centralized air defence network.'[31] The descendants of the Second World War Dowding System had started to become so complex that a cybernetic solution was required. Arquilla and Ronfeldt point out that 'new technology tends to produce a deluge of information that must be taken in, filtered, and integrated in real time. Informational overload and bottlenecking has long been a vulnerability of centralized, hierarchical structures for command and control.'[32] During the Cold War, and the US conflict in Vietnam, the reliance on computerised control systems did not necessarily lead to an advantage, a reminder that warfare is ultimately still a human endeavour.

Perhaps most notably for the history of cyberspace, during the 1960s, the US government-sponsored research carried out by the Advanced Research Projects Agency (ARPA) and the RAND Corporation led to the development of a distributed network with significant redundancy, able to survive a nuclear attack. In a potential nuclear conflict, the ability to direct and, perhaps more importantly, prevent a launch highlighted both the importance and vulnerability of information in warfare.[33] This gave birth to the packet-switched networks that were the forebears of the Internet.[34] The ARPA Network (ARPANet) had originally started as a government funded science and technology research project. A small number of other academic networks were developed in parallel to ARPANet and in the early 1970s, Vint Cerf and Bob Kahn, members of the ARPA team, proposed interconnecting the various academic networks.[35] The problem Cerf and Kahn faced was that the networks were dissimilar in design. To overcome the differences, they proposed the use of 'a "gateway," a routing computer standing between each of these various networks to hand off messages from one system to the other.'[36] Through building gateways based on 'open' i.e. non-proprietary networking standards, interconnection of dissimilar networks could be achieved, leading to what eventually became the public Internet.

Rapid improvements in microprocessor technology and the benefits of networked computing led to an increasing reliance upon information technology and an emergence of attempts to attack through the technology. Healey argues that conflict in cyberspace 'started in earnest' in 1986 when 'German hackers searched through thousands of US computer files and sold their stolen materials to the KGB.'[37] The lengthy investigation into this attack came from an unusual source, Clifford Stoll, an astronomer working in the Lawrence Berkeley Laboratory, who initially detected a 75-cent discrepancy in billing for computer time.[38] In identifying what he suspected was a software glitch, he actually revealed an ongoing sophisticated hacking campaign that was stealing documents from numerous military and academic networks. His subsequent investigation, lasting nearly two years, tracked down the German hackers who were responsible. Rather than simply preventing the hacker accessing his own network, Stoll traced the hacker's complex path around the US and Germany, until his location could be

identified. Stoll's account of the story, The Cuckoo's Egg, offers important lessons on human online behaviour, and on national and international cooperation in cyberspace, that are as valid today as they were in the 1980s.[39]

Underpinning A Revolution?

The 1991 Persian Gulf War was celebrated as a 'Revolution in Military Affairs', which Lawrence Freedman argues was the 'strategic consequences of the marriage of systems that collect, process and communicate information with those that apply military force'.[40] It is arguable whether this really marked revolutionary change or whether it was simply part of on-going evolutionary development, but crucially it did place information at the centre of the US way of warfare. The post 1991 debate heralded Operation DESERT STORM as the 'technological paradigm for future warfare', establishing the criticality of information technology and 'electronic fire strikes'.[41] The post-Persian Gulf War period saw intense debate on the role of information in warfare, elevating it from a supporting activity secondary to "real" weapons' to a central and crucial role.[42] In the US, the increased use of computers and networks highlighted a number of key vulnerabilities. These included the use of commercial lines for military communications and the sourcing of microchips for military systems from foreign commercial vendors.[43] Whilst celebrating the stunning military success in 1991, it started to become apparent that Information Warfare might present the Achilles Heel for the US military.

In a 1997 paper titled *Cornerstones of Information Warfare*, the US Air Force acknowledged the importance of the Information Age making the distinction between the general effects of the Information Age on aspects of warfare versus the specific concept of 'Information Warfare', which 'views information itself as a separate realm, potent weapon, and lucrative target'.[44] The paper reflects the post-1991 Gulf War optimism in the US military regarding its technological advantage, highlighting the potential for information becoming 'the counter to the fog of war'.[45] Despite the drive to militarize the Information Age, some observers remained sceptical of the potential of Information Warfare. John Rothrock called for 'constructive skepticism *[sic]*' towards the US Government's early approach to Information Warfare.[46] He argued that they were racing towards 'specific "means" issues… with relatively little attention paid to the more general concerns associated with objectives'.[47]

'Realization', 'Takeoff' and 'Militarization'

The US formal adoption of cyberspace as the 'Fifth Domain' of warfare can be traced back to the US National Military Strategy of 2004, which identified a need for the US Armed Forces to 'operate across the air, land, sea, space and cyberspace domains of the battlespace'.[48] More detail regarding the cyberspace domain was added by the 2006 US *National Military Strategy for Cyberspace Operations* (NMS-CO).[49] This strategy aimed to define the *ends, ways and means* for US cyber operations, but in doing so highlighted an evolution of US doctrinal discourse. NMS-CO noted that previous US Joint Doctrine had classified the 'operational environment as consisting of the air, land, maritime, and space domains and the information

environment'.[50] However, it argued that 'treating cyberspace as a domain establishes a foundation to understand and define its place in military operations'.[51]

Jason Healey divides the history of cyberspace up into three distinct phases, which he labels 'realization', 'takeoff' and 'militarization'.[52] Many would argue that attacks in cyberspace are a fairly recent phenomenon and perhaps ignore the relevance of earlier examples. Healey, argues that there is a 'rich cyber history' that is 'not a collection of empty facts, nor trivia for cyber operators to recall for amusement on a long night shift. It yields rich lessons.'[53] He charts this history through a series of 'wake-up calls' for the US Government. In the early 'realization' phase he cites the 1988 Morris Worm as being the first significant attack, both for its impact on the Internet and for the implications of the response for the US Government.

Computer viruses are malicious software, or *'malware'* that can copy themselves to another program and can be passed on through emails or removable media, such as disks.[54] A worm is a particular type of malware that can self-replicate through a network, without the need for a 'host' programme.[55] The Morris Worm was named after its creator, Robert Morris, then a graduate student; the worm spread rapidly across the ARPANet and exploited a number of software flaws that allow a hacker to gain root or Administrator level privileges on a computer system and effectively 'froze' two thousand computers.[56] In an ironic twist to the Morris Worm story, Robert Morris was the son of Bob Morris, who was the director of the US National Security Agency's National Secure Computing Centre, who had collaborated with Cliff Stoll on tracking the Cuckoo's Egg hacker.[57] The Morris Worm led to the establishment of the first Computer Emergency Response Team (CERT), funded by the US Department of Defense (DoD).[58] The ability to monitor networks, share information and coordinate a response to incidents in cyberspace remains a crucial part of cyber defence. CERTs have now been established in most countries and regions and they reflect the collaboration between governments and the IT security industry.

Healey's 'take-off' phase was signalled by President Clinton's 1998 directive on 'Critical Infrastructure Protection, PDP-63'.[59] PDP-63 directed specific responsibilities for the defence of US Critical National Infrastructure (CNI), which underpinned its economic and military power. Although it delegated specific responsibilities to the DoD for defending military systems, it also detailed cross-government responsibilities for the protection of CNI. Despite more recent concerns regarding attempts to militarize cyberspace, PDP-63 placed responsibility broadly across Federal Government departments and the private sector.[60] It was however the policy, coupled with some specific cyber-incidents, which led to the establishment of military units for Computer Network Attack (CNA) and Computer Network Defence (CND); these units eventually transformed into US Cyber Command.[61] Of the incidents that occurred during this time, the most important for the US government became known as SOLAR SUNRISE, which compromised the US DoD Unclassified network in 1998. The attackers exploited a vulnerability that existed in Sun Microsystems' 'Solaris' version of the UNIX operating system, that was widely used across the US DoD.[62] It was a known vulnerability, that could have been mitigated by the

application of software patches and the exploit required only a moderate skill by the hackers.[63] It transpired that the attack was the work of 'two teenagers in California and an Israeli hacker.'[64] However, at the time, in the midst of the geopolitical crisis over Iraq, with attacks seemingly originating from overseas, US officials suspected that another nation state was responsible.[65]

The first decade of the 21st Century led to an increased militarization of cyberspace within the US, and more broadly across the world. Healey cites a 'tremendous string of separate wake-up calls [one] after the other: Chinese espionage, BUCKSHOT YANKEE, Estonia, and Georgia, in addition to Conficker', that led to a response in the US DoD that saw increasing growth and centralisation of cyber forces.[66] BUCKSHOT YANKEE was the name given to the US response to an infection by the 'Agent.btz' malware.[67] The malware was introduced onto the US classified network via an infected USB stick on a base in the Middle East and the subsequent response 'marked a turning point in U.S. cyber defense strategy.'[68] The motivation behind the BUCKSHOT YANKEE intrusion was likely to have been espionage. Although the malware could have allowed attackers to damage or destroy files on the US DoD network, it is most likely that the intent was the exfiltration of information.[69] Similar militarization occurred in other nations, including the UK, albeit on a different scale and under a different framework of authorities. Like the US, the UK military had its share of cyberspace 'wake-up calls', including the costly recovery from the Conficker virus.[70] Conficker is another example of a self-replicating worm, which had the effect of creating an enormous world-wide 'botnet'.[71] A *botnet* is a network of robot programs (abbreviated to *bot*) that 'enslave' affected computers under the control of a 'bot-herder'. By using remote command and control, the *bot-herder* can direct the botnet to attack and overwhelm a particular service, such as a web server, with thousands of simultaneous requests, causing it to be unable to respond and therefore effectively taking it offline. This type of attack is known as Distributed Denial of Service (DDoS).[72] Whilst Conficker highlighted a hitherto complacent attitude to cyber defence and information risk management, and required an expensive recovery operation, its actual effects on military operations and mission critical systems were minimal.[73]

Operational Integration

Arguably one of the most relevant examples of cyberspace operations thus far, was the use of DDoS attacks during the Russian conflict with Georgia over South Ossetia in 2008. These attacks included 'large-scale botnet DDoS attacks, targeting the government, news media, and other sites, along with intrusions and defacements'.[74] The use of a DDoS attack is in itself not remarkable; such attacks are routinely used as instruments of criminal activity. However, in this case, Healey argues that 'Russia was not just ignoring or encouraging its patriotic hackers… but were actively coordinating or directing their actions'.[75] These attacks are not significant for their destructive power or their complexity, they are nonetheless important as an example of a state coordinating a military operation on land and in the air with attacks in cyberspace. The extent to which attacks on the ground were really coordinated with cyber-attacks is debatable. The fact that kinetic attacks on communications infrastructure did not occur suggests that there was some degree of coordination.[76] Moreover, the 'cyber

forces' in this case were allegedly not uniformed combatants, but 'Russian organized criminals, who made no effort to conceal their involvement.'[77] Jeffrey Carr argues that this was not the first coordinated use of cyber operations by the Russian military, citing earlier examples in Chechnya; however Georgia, unlike Chechnya, included close synchronisation.[78] Whilst the DDoS attacks were coincident with military action, they had also been part of the escalating diplomatic crisis prior to the ground and air campaign. The level of coordination allegedly included 'vetted target lists of Georgian government websites', thought to be provided by Russian intelligence'.[79]

Operation ORCHARD, the 2007 Israeli attack on a suspected nuclear weapons processing plant at Dayr az-Zawr in Syria is another important example of the integration of cyberspace operations with conventional military operations. The Israeli Air Force destroyed the reactor site with a conventional air attack, but it is claimed that, prior to the air attack, they defeated the Syrian air defence system with a combination of electronic attack and cyber attack. Fulgham argues that the intelligence gathered about the attack provides 'evidence that a sophisticated network attack and electronic hacking capability is an operational part of the Israeli Defense Forces' arsenal of digital weapons.'[80] This type of attack marks an important historical development for cyberspace conflict. Unlike the often speculative arguments regarding the *potential* for cyber attacks, Geers argues that the 'event demonstrates the clear power of cyber attacks to inflict damage on critical infrastructure.'[81]

In the history of cyberspace, the cyber-attack that has perhaps resulted in the most speculation and hype was 'Stuxnet'. Stuxnet was the name given to an attack on a Siemens Supervisory Control and Data Acquisition (SCADA) system managing the centrifuges at the Iranian nuclear enrichment facility at Natanz. SCADA or Industrial Control Systems (ICS), are software processes that control physical 'real world' devices through sensors and electro-mechanical device controllers. This attack, later attributed to the US and Israeli governments, was not executed as part of a broader military operation, rather it was used to complement diplomatic and economic levers against Iran to deter and prevent a nuclear weapons programme.[82] Healey contends that 'not only was Stuxnet "capable of infecting a fully-patched Windows 7 system"; it was also the first malware to target industrial control systems, in this case, those manufactured by Siemens.'[83] Stuxnet serves as an example of the non-trivial nature and complexity of 'high-end' cyberspace effects. Despite being a relatively small focussed and highly targeted, tactical level attack, Stuxnet earns its place in cyberspace history due to its strategic consequences. Stuxnet is credited as 'the most sophisticated malicious software ever found' and its level of complexity led to the accusations that it must have originated from a nation state actor.[84] It has highlighted the risk that malicious software has the potential to have 'real-world' effects through the disruption of control systems.

A Strategy for the United Kingdom

The majority of the history of cyberspace cited above reflects the strategic approach in the US. This has been mirrored in the UK, with the 2010 National Security Strategy highlighting 'hostile

attacks upon UK cyber space by other states and large scale cyber crime' as one of the 'Tier One' risks to National Security.[85] This was a significant assessment, placing cyberspace alongside international terrorism, a major accident or natural hazard, or an international military crisis.[86] Raising the level of importance of this risk has resulted in substantial investment and a need for a pan-government response.

However, the threats from cyberspace were acknowledged in strategy much earlier. The 1998 Strategic Defence Review (SDR) identified the risk from 'novel forms of attack… [including] the use of information warfare against increasingly vital computer systems.'[87] After the 11 September 2001 attacks in the US, the strategic landscape changed immensely, leading to a review of the 1998 SDR, presented to the UK Parliament in 2003 as 'A New Chapter to the Strategic Defence Review'.[88] The 'New Chapter' highlighted an increasing reliance on computer networks, the concepts of Network Centric Warfare and the increased threat of Computer Network Attack.[89]

In 2009 the Cabinet Office issued the 'Cyber Security Strategy of the United Kingdom.'[90] This strategy acknowledged Britain's reliance on cyberspace and set out the Government intent to tackle the risks related to cyberspace, including the establishment of 'an Office of Cyber Security (OCS) to provide strategic leadership for and coherence across Government… [and the creation of] a Cyber Security Operations Centre (CSOC).'[91] This strategy was reviewed in light of the 2010 Strategic Defence and Security Review (SDSR) and a new strategy was issued in 2011.[92] Written in the context of the recovery from a global economic crisis, the 2011 strategy placed significant focus on the UK's economic dependence on cyberspace, arguing 'the scale of our dependence means that our prosperity, our key infrastructure, our places of work and our homes can all be affected.'[93] Citing the cost of cybercrime to the UK economy at £27 Billion per year, it concentrated on the threat of cybercrime. However, it also detailed the threats from states (via espionage and 'patriotic hackers'), terrorists and hacktivists.[94] The response to these threats was the Cabinet Office-led National Cyber Security Programme (NCSP).[95]

The NCSP was a significant step in the history of the UK military development of cyberspace because it aligned a pan-government response, and the national-level programme also set aside £90 million through the Defence Cyber Security Programme (DCSP).[96] The DCSP established two Joint Cyber Units, one focussing on Cyber Defence and the other, 'hosted by GCHQ at Cheltenham whose role [was] to develop new tactics, techniques and plans to deliver military effects.'[97]

The historic evolution of the UK's strategic approach to cyberspace conflict has perhaps lagged behind that of the US and is understandably at a considerably smaller scale. However, cyberspace has now been accepted in UK concepts and doctrine as an operating environment and that has been reflected in the establishment of cyber forces and associated capabilities.[98] Perhaps as a result of the UK's strategic development of cyber security, coupled

with the lessons of operational integration, such as the Israeli attack on the Syrian Integrated Air Defence System, UK Air Power Doctrine, issued in 2013, acknowledged for the first time the concept of Air-Cyber integration.[99] However, the effective ongoing development of doctrine, tactics and techniques to integrate air power with cyberspace needs to be based on the study and interpretation of the empirical evidence. Peter Gray suggests that the 'distillation of 'what has worked best' is the seed corn of tactical level doctrine';[100] perhaps over time, 'what has worked best' in cyberspace will inform the development of cyberspace doctrine and normalise its relationship with the other environments.

The recently published *National Security Strategy and Strategic Defence and Security Review 2015* has reaffirmed and further developed the UK strategy for cyberspace.[101] In the five years since the previous SDSR established Cyber as a 'Tier One' risk, UK cyber dependence has continued to grow commensurate with ongoing scale and sophistication of the threat, so unsurprisingly, Cyber has retained its 'Tier One' status in the 2015 strategy.[102] The national security context within the strategy acknowledges cyberspace in its own right but also demonstrates how it is interwoven with wider technological developments and energy security.[103]

Perhaps more importantly, the strategy has signalled clear intent to act in cyberspace. It states that 'we will use the full spectrum of our capabilities – armed force including, ultimately, our nuclear deterrent, diplomacy, law enforcement, economic policy, offensive cyber, and covert means – to deter adversaries and to deny them opportunities to attack us.'[104] This explicit avowing of an offensive cyber capability is an important political statement, particularly the establishment of a clear role for the Armed Forces, in the Government's commitment to '… provide the Armed Forces with advanced offensive cyber capabilities.'[105] The commitment is also reflected in a £1.9 billion programme over 5 years, a step-change in investment from the NCSP allotment in the 2010 strategy.[106]

Conclusion

This paper has traced the lineage of cyberspace from the historical importance of information, through the technological developments of the 20th Century to the 'Information Age' of the 21st Century. This short history merely offers a few headlines in what has been a complex and rich history. The development of cyberspace through the Cold War highlights the synergistic relationship between the development of cyber technology and that of weapons systems, underpinned by a battle of ideologies. The post DESERT STORM era highlighted a realisation of the threats and opportunities of cyberspace for military operations. Repeatedly the 'information age paradox' has been apparent. Whenever mastery of information seems to offer an advantage in war, the risk of over-dependence becomes apparent. The more recent history of cyberspace has been underpinned by a series of 'wake up calls' that have led to the US and others developing strategies for cyberspace and developing military cyber capabilities. Perhaps some of the most important lessons may be drawn from the few examples of where cyberspace has been integrated with broader military operations. These cases are arguably the

best examples of cyber conflict or Information Warfare, rather than those that demonstrate the importance of *information in war* or espionage through cyberspace.

The United Kingdom has seen an evolution in cyberspace strategy, reflecting national and global economic and social dependence. The strategic *Ends* set out in the UK Cyber Security Strategy have been matched by a programme of *Ways* and *Means*, through the establishment of National and Defence Cyber Security Programmes. The 2015 SDSR has extended the contribution of cyberspace to National Security and has led to a programme grow capacity both nationally and within the Armed Forces.

If cyberspace is to be truly integrated into military operations, there is a need to expand its study. This is not merely a study of computer science, although like all aspects of warfare, technology is important and requires expertise. The study of cyberspace history needs to include work that, like the Land, Maritime and Air environments, is multidisciplinary and robust. Further historical study from the perspectives of social science, law, international relations and technology will build a body of knowledge that will eliminate the myth and hyperbole that exists surrounding cyber conflict. This will enable a path towards normalisation of operations within cyberspace that will become as routine as those in the other environments.

Notes

[1] This article has been developed from a previously unpublished chapter of a dissertation submitted to the Department of War Studies, King's College London, as partial fulfillment of the requirements for the MA degree Airpower in the Modern World in March 2014.
[2] Healey, Jason (Ed) (2013), *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, (Vienna, VA: Cyber Conflict Studies Association), p.10.
[3] Raleigh, Walter (1922), *The War in the Air; Being the Story of the Part Played in the great War by the Royal Air Force*, (Oxford: The Clarendon Press).
[4] UK doctrinal taxonomy classifies Land, Sea, Air, Space and Cyberspace as 'environments' rather than 'domains' – see Development, Concepts and Doctrine Centre (2014), *Joint Concept Note 1/14: Defence Joint Operating Concept*, (Shrivenham: DCDC), Afterward p.4.
[5] Development, Concepts and Doctrine Centre (2010), *Joint Doctrine Note 3/13: Cyber Operations: The Defence Contribution*, (Shrivenham: DCDC), p.1-1.
[6] Gray, Peter (2001), 'Why Study Air Power History?' *RAF Air Power Review*, Vol 4., No. 3, p.10
[7] Arquilla, John and Douglas A. Borer (2007), *Information Strategy and Warfare*, (New York, NY: Routledge), pp.3-4.
[8] Arquilla, John and David Ronfeldt, eds. (1997) *In Athena's Camp: Preparing for Conflict in the Information Age*, (Santa Monica, CA: RAND), p.36.
[9] Arquilla and Borer (2007), p.5.
[10] Ibid.
[11] Healey (2013), p.27.
[12] Essinger, James (2004), *Jacquard's Web: How a Hand Loom Led to the Birth of the Information*

Age, (Oxford: Oxford University Press), p5 and Naughton, John (1999), *A Brief History of the Future: The Origins of the Internet*, (London: Weidenfeld & Nicolson), p.51.
[13] Essinger (2004), p.122.
[14] Lambert, Nicholas (2004), 'Transformation and Technology in the Fisher Era: the Impact of the Communications Revolution', *Journal of Strategic Studies*, Vol. 27, No.2, p.283.
[15] Aldrich, Richard J. (2010), *GCHQ*, Kindle Edition (London: Harper Collins), p.15.
[16] Ibid.
[17] Holland, James (2010), 'The Battle of Britain', *The RUSI Journal*, Vol. 155, No. 4, p.72.
[18] Aldrich (2010), p.58.
[19] Ibid.
[20] Ibid., p.28.
[21] Naughton (1999), pp.61-62.
[22] Galison, Peter (1994), 'The Ontology of the Enemy: Norbert Wiener and the Cybernetic Vision,' Critical Enquiry, Vol. 21, No. 1 p.232.
[23] Ibid.
[24] Slava Gerovitch, "'Mathematical Machines' of the Cold War: Soviet Computing, American Cybernetics and Ideological Disputes in the Early1950s," *Social Studies of Science, Vol. 31, No. 2*, 2001, **http://blogs.bu.edu/guidedhistory/files/2013/02/MathematicalMachinesoftheColdWar.pdf**., p.253.
[25] Ibid., p.262.
[26] Ibid.
[27] Ibid., p.269.
[28] Bousquet, Antoine (2008), 'Cyberneticizing the American War Machine: Science and Computers in the Cold War', *Cold War History*, Vol. 8, No.1, p.83.
[29] Ibid., p.78.
[30] Ibid., p.84.
[31] Ibid., pp. 85-86.
[32] Arquilla, John & David Ronfeldt (1993), 'Cyberwar is coming!', Comparative Strategy, Vol. 12, No. 2, p.156.
[33] Hafner, Katie and Matthew Lyon (1996), *Where Wizards Stay Up Late: The Origins of Internet*, (New York, NY: Touchstone), pp. 54-55.
[34] Naughton (1999), p.97.
[35] Ibid. p.222.
[36] Ibid., p.223.
[37] Healey (2013), p.10.
[38] Stoll, Clifford (1990), *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage*, (New York, NY: Pocket Books), p.3.
[39] Ibid., pp.397-398.
[40] Freedman, Lawrence (1997), 'War Designed for One,' *The World Today*, Vol. 53, No. 8/9, p.217.
[41] Blank, Stephen J. (1997), 'Preparing for the Next War: Reflections on the Revolution in Military Affairs', in John Arquilla and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age*, (Santa Monica, CA: RAND), p.62.

[42] Berkowitz, Bruce D. (1997), 'Warfare in the Information Age', in John Arquilla and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age*, (Santa Monica, CA: RAND), p.177.
[43] Ibid., p.178.
[44] US Air Force (1997), *Cornerstones of Information Warfare*, http://handle.dtic.mil/100.2/ADA323807, accessed 5 September 2015, p.2.
[45] Ibid.
[46] Rothrock, John (1997), 'Information Warfare: Time for Some Constructive Skepticism', in John Arquilla and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age*, (Santa Monica, CA: RAND), pp. 217-229.
[47] Ibid., pp.219-220.
[48] US Department of Defense (2004), *The National Military Strategy of the United States 2004*, (Washington DC: Department of Defense), http://history.defense.gov/Portals/70/Documents/nms/nms2004.pdf, accessed 29 September 2015, p.18.
[49] US Department of Defense (2006), *National Military Strategy for Cyberspace Operations (NMS-CO)*, (Washington, DC: Department of Defense), http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf, accessed 29 September 2015, p.ix.
[50] Ibid., p.3.
[51] Ibid.
[52] Healey (2013), p.17.
[53] Ibid., p.15.
[54] Hey, Tony and Gyuri Pápay (2015), *The Computing Universe: A Journey Through a Revolution*, (New York, NY: Cambridge University Press), pp.246-247.
[55] Ibid., p.248.
[56] Ibid. pp.248-249.
[57] Stoll (1990) pp.385-392.
[58] Ibid., p.32.
[59] US Government (1998), Presidential Decision Directive/ NSC-63, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm, accessed 5 September 2015
[60] Ibid.
[61] Healey (2013) p.42.
[62] Ibid., p.125.
[63] Ibid.
[64] Ibid., p.122.
[65] Ibid., p.127.
[66] Ibid., p.73.
[67] Ibid., p.205.
[68] Lynn, William (2010), 'Defending a New Domain', *Foreign Affairs*, Vol. 89 Issue 5, pp.97-108.
[69] Healey (2013) p.207.
[70] Harvey, Shaun (2013) 'Unglamorous Awakenings: How the UK Developed Its Approach to Cyber', in Healey, Jason, ed, *A Fierce Domain: Conflict in Cyberspace*, 1986 to 2012, (Vienna, VA: Cyber Conflict Studies Association), p.260.

[71] Singer, P.W. & Allan Friedman (2014), *Cyber Security and Cyberwar*, Kindle Edition (New York, NY: Oxford University Press), p.72.
[72] Hey and Pápay (2015), p.250.
[73] Harvey, Shaun (2013), p.260.
[74] Healey (2013), p.71.
[75] Ibid., p.72.
[76] Shakarian, Paul, Jana Shakarian and Andrew Ruef (2013), *Introduction to Cyber-Warfare: A Multidisciplinary Approach*, (Watham, MA: Syngress), p.27.
[77] Healey (2013), p.72.
[78] Carr, Jeffrey (2010), *Inside Cyber Warfare: Mapping the Cyber Underworld*, (Sebastopol, CA: O'Reilly Media), p.3
[79] Singer & Friedman (2014), p.111.
[80] Fulghum, David A., Wall, Robert, Butler, Amy (2007) 'Cyber-Combat's First Shot', *Aviation Week & Space Technology*, Vol. 167, Issue 21, pp.28-31.
[81] Geers, Kenneth (2009) 'The Cyber Threat to National Critical Infrastructures: Beyond Theory,' Information Security Journal: A Global Perspective 18, No. 1, pp.1–7.
[82] Rid, Thomas (2013), *Cyber War Will Not Take Place*, (London: Hurst), pp.44-46.
[83] Healey (2013), p.75.
[84] Morton, Chris (2013), 'Stuxnet, Flame and Duqu – the OLYMPIC GAMES', in Healey, Jason, ed, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, (Vienna, VA: Cyber Conflict Studies Association), pp.212-222.
[85] UK Government (2010), *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, p.27.
[86] Ibid.
[87] House of Commons (1998), *Research Paper 98/91:The Strategic Defence Review White Paper*, p.16.
[88] UK Government (2003), *A New Chapter to the Strategic Defence Review.*
[89] Ibid., pp.32-36.
[90] Cabinet Office (2009), Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space
[91] Ibid., p.21.
[92] Cabinet Office (2011), *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world.*
[93] Ibid., p.15.
[94] Ibid., pp.15-16.
[95] Ibid., p.21.
[96] 'Defence Select Committee: Written evidence from the Ministry of Defence', **http://www.publications.parliament.uk/pa/cm201012/cmselect/cmdfence/writev/1881/dcs01.htm** , accessed 29 September 2015.
[97] Ibid.
[98] Development, Concepts and Doctrine Centre (2014), Joint Concept Note 1/14 (JCN 1/14): Defence Joint Operating Concept, (Shrivenham: DCDC), p.1-6.
[99] Development, Concepts and Doctrine Centre (2013), Joint Doctrine Publication 0-30 (JDP

0-30): UK Air and Space Doctrine, (Shrivenham: DCDC), p.4-10.
[100] Gray, Peter (2001), 'Why Study Air Power History?' RAF Air Power Review, Vol 4., No. 3, p.2.
[101] UK Government (2015), *National Security Strategy and Strategic Defence and Security Review 2015*.
[102] Ibid., p.85.
[103] Ibid., pp.19-21.
[104] Ibid., p.24.
[105] Ibid., p.41.
[106] Ibid., p.40.