What is the Utility of the Fifth Domain?[1]

By Squadron Leader Paul Withers

The increasing importance of cyberspace for military operations has led to the United States Department of Defense classifying it as the Fifth Domain of Warfare. However, cyberspace lacks the explicit physical properties of land, sea, air and space, and as a consequence its classification as a warfighting domain is controversial. The cyber debate is replete with hyperbole and ambiguous terminology and there are calls to limit the militarization of cyberspace. The critical dependence of Western military forces on microprocessor technology inevitably means that exploiting this domain is viewed from the dual perspectives of opportunity and vulnerability. But does it make any sense to classify cyberspace as a domain? This paper assesses the utility of the Fifth Domain with the aim of understanding what 'domain status' means for military forces, how existing theories of war apply to the new domain, and the practical implications of integrating cyberspace operations into warfare.

Introduction

'Is cyber really a domain? Like everyone else who is or has been in a US military uniform, I think of cyber as a domain. It is now enshrined in doctrine: land, sea, air, space, cyber. It trips off the tongue, and frankly I have found the concept liberating when I think about operationalizing this domain'.

General Michael Hayden[2]

Cyberspace has formed part of the National Security debate for over a decade and the utility of operations in cyberspace continues to be hotly debated. In 2010, cyber security was classified as one of the UK's four 'Tier-One' risks to National Security, reflecting a level of concern regarding the damaging effects of crime, espionage and warfare enacted in and through cyberspace.[3] The US has been developing its pan-government response to the cyber security threat for a number of years and part of that response has included the development of the organisations, concepts and doctrine to define cyberspace as a domain of warfare.

Historically wars were fought in two domains, which corresponded to the physical environments of Land and Sea. At the beginning of the 20th Century powered flight enabled the third environment, Air, to become a domain of warfare from the First World War onwards. In the latter half of the century, the exploration of Space led to the exploitation of the fourth environment for numerous peaceful purposes, but also as a warfighting domain, used for the purpose of supporting, enabling and potentially conducting military operations. More recently a fifth domain has been identified: Cyberspace. Hayden's question, 'is cyber really a domain?' is an important one in furthering the now well-worn debate surrounding 'Cyber War'. Most cogent argument now casts aside alarmist and fanciful ideas of future war being fought solely or even predominantly in cyberspace. What remains is the need to add clarity to the role of cyberspace across the diplomatic, military and economic levers of power.

For the military instrument, cyberspace has found its way into US doctrine as the Fifth Domain of warfare. However, the classification of cyberspace as a domain is in itself steeped in controversy. Cyberspace differs from the other domains in that it is not a physical environment and its physical manifestations arguably exist across the other domains; it is neither wholly physical, nor is it completely virtual. This raises questions regarding the extent to which something that is not entirely tangible can be somewhere where battles are fought and won.

This paper will address the central question 'What is the Utility of the Fifth Domain?' In doing so it will consider both whether the concept of a fifth domain is meaningful in a semantic sense and beyond terminology, it will determine the extent to which cyberspace offers utility as a domain of warfare. It will examine whether or not the fact that the Fifth Domain is 'enshrined' in US doctrine is enough to give credibility to the concept or, even if the doctrinal definition is flawed, whether that is of consequence for the development of cyberspace as a tool of warfare.

The argument is presented in five steps. First, it will define the terminology that bounds the Fifth Domain and the emotive and controversial term 'cyber war.' It will examine academic and US-doctrinal definitions and determine the reasons for treating cyberspace as a domain of warfare. It will argue that there is utility in the terminology of the Fifth Domain and for a number of practical reasons it is sensible to treat cyberspace as a domain of military activity that is separate from land, sea, air and space. It should be noted that UK doctrine now classifies land, sea, air, space and cyberspace as 'environments' rather than 'domains'. This paper accepts the difference in doctrinal approach, but as it is largely based on academic work that refers to cyberspace as a 'domain', the term *domain* will be used.

Second, the importance of cyber defence as a consequence of cyber dependence will be considered. Developed nations and their military forces are particularly dependent upon cyberspace and as a consequence, it is not sufficient to develop effective offensive cyber capabilities. Modern weapons platforms rely upon embedded processors and communications networks and the advanced technology that gives them their advantage may also be their greatest vulnerability.

Third, emerging ideas of war in the Fifth Domain will be considered in the context of some of the theories of war in the traditional domains. It will argue that whilst there is currently a lack of cogent Fifth Domain theory, many of the concepts of existing theorists apply to the new domain. Of equal importance are the lessons that can be learned from the errors in early theory, particularly the parallels with the emergence of air power and the excessive hyperbole of its proponents. Similarly, early claims of wars being fought solely in cyberspace replacing traditional warfare are flawed and detract from the true efficacy of cyber operations as an instrument of power. However, the more recent concepts of 'parallel warfare' offer a possible theoretical basis for cyber operations to complement traditional kinetic operations. Cyberspace cannot offer the lethality or coercive nature of traditional weapons, but its characteristics may give options that can contribute to the overall military aim.

Fourth, consideration will be given to the practical utility of cyberspace operations. The paper will argue that the characteristics of cyberspace and 'weaponised code' offer reversible effects that have significant disruptive potential, despite their lack of destructive potential. The characteristics of 'cyber effects' will be examined with the potential for their use in specific military applications. The argument will balance the advantages and disadvantages of choosing a cyberspace-derived course of action, including the issues of achieving an appropriate degree of assurance of the efficacy of cyber-effects and their legal implications.

Finally, the paper will conclude with an overall assessment of the utility of the Fifth Domain. It will argue that the concept of a warfighting domain is valid as a means of developing cyberspace in the context of 21st Century armed conflict. Future warfare is unlikely to be conducted solely in cyberspace, but Fifth Domain operations are, and will remain an integral

part of warfare. As a consequence, this paper will therefore contend that there is significant utility in the Fifth Domain.

Defining the Fifth Domain

In attempting to make an assessment of its utility, it is first necessary to define the Fifth Domain. Unlike the physical domains, cyberspace is not an entirely tangible entity whose limits can easily be quantified. The acceptance of the term 'Fifth Domain' in US government and military circles does not in itself affirm the existence of a 'cyberspace domain'. In discussing an earlier but related concept, the so-called Revolution in Military Affairs, Colin Gray cautions against the 'nominalist fallacy'; the fact that something is given a captivating name increases the debate that surrounds it, which in itself has a tendency to give substance and credibility to the concept.[4] For the Cyberspace Domain to be more than just fallacious terminology it needs to have real substance and Libicki, whilst arguing against the Fifth Domain, calls for 'the rectification of terms: making the name of the thing match the nature of the thing'.[5] This section examines the terminology of the Fifth Domain and will argue that despite it being a problematic concept, it is appropriate and meaningful for cyberspace to be considered a domain of warfare.

A fundamental problem for applying clarity to the Fifth Domain comes from the use of poorly defined and ambiguous language. Michael Hayden argues: 'Rarely has something been so important and so talked about with less clarity and less apparent understanding than this phenomenon'.[6] The term 'cyber' has been adopted into both popular and military culture with broad and inconsistent meaning. Its origins date back long before the 'information age'; Norbert Wiener's World War II work on predictive characterisation of attacking aircraft profiles, in order to improve the performance of anti-aircraft artillery, led to him coining the term 'cybernetics' in 1947.[7] Wiener 'designated what he hoped would be a new science of control mechanisms in which the exchange of information would play a central role'.[8]

The linguistic origin of 'cyber' as a shortened version of cybernetics, 'from the Greek… meaning good at steering', is far removed from the adoption of cyber into common English usage.[9] The dictionary definition of 'cyber' is 'relating to or characteristic of the culture of computers, information technology, and virtual reality'.[10] The term *cyberspace*, which was originally coined in science fiction by William Gibson, was one which was originally intended to have 'no real semantic meaning'.[11] For cyberspace to have credibility as a domain of warfare, the term requires clear and unequivocal meaning. The dictionary definition of cyberspace is 'the notional environment in which communication over computer networks occurs'.[12] Defining cyberspace as 'notional', i.e. imaginary or hypothetical, does little to enhance its credibility as a place where military operations can occur. However, the US military definition of cyberspace sets a more concrete basis for its case for the existence of a domain:

> 'A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the

> Internet, telecommunications networks, computer systems, and embedded processors and controllers'[13]

This definition contains a number of important elements for setting the bounds of the domain. First, it includes both the infrastructures and the data. It is therefore not simply defined by physical devices but also by the software and data that resides on hardware and transits through it. Second, the domain includes *but is not limited* to the Internet. This is a crucial aspect of defining the domain; the entities that military forces may wish to attack and defend extend beyond the bounds of the Internet. Communication systems, networks, weapons platforms and devices of military interest may be physically or logically isolated from the Internet or connect only fleetingly or indirectly, for example by a human operator using a storage device to transfer files. Arguably the use of the word 'interdependent' in the definition is misleading; isolated networks may not be dependent on other networks, yet still be part of the cyberspace domain. Third, the domain resides in the 'information environment'; this distinction between a cyberspace domain and an information environment is a result of a historical doctrinal and semantic debate within the US military, a debate that is also reflected in the development of UK doctrine. The lack of consistency in terminology is a symptom of the difficulty in articulating a coherent explanation of cyberspace. The US Department of Defense (DoD) has thus far, 'issued at least twelve different definitions of what it thinks of as cyberspace'.[14] The UK Defence Joint Operating Concept classifies land, sea, air, space and cyberspace as 'environments' rather than 'domains', arguing that the word domain 'implies some form of dominion which we would only have fleetingly on operations (sea or air control)'.[15] The dictionary definition of *domain* as 'an area of territory owned or controlled' validates the argument about 'dominion', although the alternative definition of *domain* as 'a specified sphere of activity or knowledge' arguably supports the US terminology.[16] Whilst this semantic difference is acknowledged, this paper prefers the term *domain* simply because most of the published literature about cyberspace is of US origin or reflects US military doctrine.

This leads to the crucial question of whether the US DoD 'domain definition' is little more than an example of Gray's 'nominalist fallacy'.[17] On one level, naming cyberspace as a domain of warfare seems arbitrary; other specialist endeavours within the military might equally have a claim to domain status.[18] In order to assist in countering this possibility, perhaps the most unhelpful and ambiguous term of all, 'cyberwar', needs to be examined. Although the hyperbole around cyberwar has helped generate a healthy debate, the evidence suggests that it is a largely meaningless concept, based on the norms of understanding around the nature of war. Thomas Rid argues that for something to be considered *war* it must meet the Clausewitzian criteria of being violent, instrumental and political.[19] Where 'cyberwar' most notably fails this test is in its capacity to be violent. However, military operations include acts that support warfare and, whilst not being violent *per se*, contribute to military operations, i.e. they support and enable violence or the threat of violence. Examples include intelligence, surveillance and reconnaissance, information operations and numerous other

enabling activities. Cyberspace operations mainly fit into this category of non-violent enablers of warfare. However, the spectrum of cyberspace operations does push up against the boundaries of violence in its ability to cause destruction to equipment and data. The violence inflicted by a cyberspace operation may be indirect and complex; it is often not the easily identifiable 'use of force' apparent with a kinetic weapon.[20] This paper therefore supports Rid's view that due to cyberspace operations' inability to be violent *per se*, 'cyberwar' cannot exist. However, cyberspace operations are, and will remain, an integral part of warfare.

Rid argues against the existence of a Fifth Domain for a number of fairly compelling reasons.[21] The origin of Fifth Domain terminology was originally just a 'US Air Force lobbying gimmick' although he concedes that this fact in itself does not counter its utility.[22] Within the UK, in the context of austerity and significant defence cuts, the Strategic Defence and Security Review of 2010 announced a National Cyber Security Programme, allocating £650 million of 'new' money for cyber security.[23] It is therefore understandable that those in Defence would join the 'moths' around the cyber 'flame'.

Rid also contends that 'code-triggered violence will express itself in the other domains'.[24] However, this in itself is little different to the interdependence of the other domains. 'Aircraft-triggered violence' often has its effect felt in the land domain. Dropping an air launched weapon on a ground target demonstrates the interdependence and synergy between the domains. Indeed, the targeting of a modern precision weapon is also highly dependent on the space domain and may involve a controller on the ground guiding the aircrew. Conversely, whilst Fifth Domain effects must normally be felt in another physical domain, where computer code is used to permanently destroy data rather than a physical device, the effect remains in the cyberspace domain, though it may ultimately be felt in terms of a cognitive effect on the operator of the computer system.[25] The interdependence of cyberspace with the traditional domains, rather than specifically being part of any one of them, strengthens rather than weakens its case for being a separate domain.

Often effects are intended to be cognitive rather than physical in nature. This is true of both kinetic and cyber action. Whilst bombs may be dropped to cause physical harm and damage, they may be used to shatter the will and cohesion of an enemy, to deceive or to sow confusion. Effects in cyberspace arguably have significant utility across what Tibbs calls 'the full spectrum of the information domain [which] runs from hardware, through software to what has been called "wetware", the realm of knowledge in the human brain and mind'.[26]

The use of the term 'cyberspace' is to some extent metaphorical, used in an attempt to describe spatially what otherwise might be a fairly nebulous concept. The physical 'battlespace' can be described and mapped using geographic coordinates, heights and through the description of physical features. In cyberspace, the physical location of hardware is only part of the information required; it is often more meaningful to describe the 'space' in terms of its logical network topology, with Internet Protocol addresses being more important

than geo-coordinates. The language of cyberspace is therefore the means of dealing with the complexity of the 'interdependent networks of information technology infrastructures and resident data'.[27] However, it is possible to take the spatial metaphor too far and therefore undermine its credibility. The US Air Force Mission 'fly, fight and win… in air, space and cyberspace' is a good example of this.[28] The idea applying the flying and fighting analogy to cyberspace has resulted in ridicule that undermines the argument for a Fifth Domain.[29] US airmen are clearly not physically able to 'fly' through cyberspace, but navigating through the network to deliver a 'payload' of software code to a target does seem a reasonable way of simplifying the complexity and 'selling' the mission to 'warfighters' rather than technocrats. The highly technical language of cyberspace that is underpinned by computer science is appropriate for cyber specialists. However, if cyberspace operations are to be truly integrated with the other domains, then the specialist language of cyberspace must be translated into a different specialist language, that of joint military operations. The Fifth Domain metaphor is arguably useful in helping achieve this.

A domain is 'a specified sphere of activity or knowledge'.[30] Therefore, perhaps one of the strongest arguments for designating cyber as a domain of warfare is a pragmatic one; military forces need to organise specialist areas to develop suitably qualified and experienced personnel and to enact effective command and control over those specialist units. Military cyberspace operations require different skills to the traditional physical domains. One hundred years ago, the emergence of the aeroplane over the battlefield gave rise to similar challenges, requiring people both on the ground and in the air who had different skills and who needed to think differently about the conduct of warfare. This led to the creation of separate air arms and eventually, independent Air Forces. An airman's perspective, both literally and figuratively, is very different from that of a soldier or sailor. Like the physical domains, the cyber domain requires operators with a unique perspective, one underpinned by a deep understanding of the nature of cyberspace. In discussing organisations dedicated to operating in the Fourth and Fifth Domains, Colin Gray argues that they are 'likely to advance understanding and capability, not least for joint effectiveness, more rapidly than an arrangement whereby space and cyber concerns are not the primary oci of loyalty and concern'.[31]

Within the US, the distinct nature of cyberspace compared to the other domains has been acknowledged through the establishment of a Cyber Command. There are already calls for the single-service units that make up Cyber Command to evolve into a separate branch of the military.[32] Proponents of a separate branch argue that currently those employed in cyberspace are 'ideologically biased by their operational past—be it on land, at sea, or in the air' and that their single service origins cause 'unhealthy competition' and ultimately 'threaten unity of command'.[33] However, growing a separate service branch poses significant bureaucratic and budgetary challenges; for nations other than the US, scale alone may make the creation and sustainment of separate forces untenable. Another argument to counter the call for a separate cyber-service is the interdependence of cyberspace with the other domains. It may prove that

individuals with both cyber specialist skills and experience in one of the traditional warfighting domains will aid the integration of cyberspace into joint operations.

In defining the Fifth Domain it is equally important to eliminate what is *not* in the military domain. Those writing about 'Cyber War' have often conflated online crime with war. Dealing with crime quite rightly remains the business of law enforcement, not the military. Whilst 'cybercrime' is of concern to governments and needs to be addressed as part of overarching cyber security strategies, it is distinct from using cyberspace in military operations. Similarly, whilst cyber-derived intelligence may be part of military operations, it is distinct from state-sponsored espionage through cyberspace; one state spying on another through cyberspace does not in itself constitute an act of war, nor need it be part of warfare. Tibbs argues that it is now time for 'the more recent convergence of hyperbole and pragmatism', surrounding cyberspace in the business context to extend to the military context.[34] Ultimately, it is the decision of individual governments to determine the extent of the missions delegated to their military forces, underpinned by domestic and international law and their own policy decisions. Many caution against the militarization of the Internet and beyond its military utility and vulnerability, it remains somewhere for business, entertainment, education and numerous other non-warlike human activities. However, the interaction and interdependence between the uses of cyberspace arguably necessitate an overarching governance role within each state 'with topsight responsibility for cyber strategy'.[35]

Singer & Friedman argue that cyberspace is not 'merely a physical place and thus defies measurement in any kind of physical dimension. But [it] isn't purely virtual'.[36] The hardware and software of cyberspace come into contact with both the physical and cognitive world and whilst not part of cyberspace, the interactions and interfaces with the physical and cognitive are important. The maritime domain includes the interface between the land and the sea - the littoral. The littoral acts as the demarcation point between land and sea and is the realm of specialist amphibious forces. Cyberspace also has a number of 'littorals' including: physical infrastructure, cabling and electrical power; the electromagnetic spectrum that data traverses; electro-mechanical processes under computer control; and the senses and cognition of computer users. The 'cyber littorals' may be either the vector through which a cyber-attack is delivered or the intended target of a cyberspace operation.[37] To include the 'cyber littorals' in the domain definition would make the definition so broad it would become meaningless; whilst a human operator interacts with cyberspace, he is not part of it. Despite this, Singer and Friedman do give a broader definition of cyberspace: 'cyberspace is the realm of computer networks (and the users behind them) in which information is stored, shared, and communicated online.'[38] If an effect through cyberspace aims to change the state of something in the physical world or in the realm of human cognition, understanding the interfaces with cyberspace is as important as understanding the software code within it.

Arguably, whether US doctrine writers are correct in labelling cyberspace as the Fifth Domain is not in itself particularly important. As Michael Howard contended:

> 'I am tempted indeed to declare dogmatically that whatever doctrine the armed forces are working on now, that they have got it wrong. I am also tempted to declare that it does not matter that they have got it wrong. What matters is their capacity to get it right quickly when the moment arrives'.[39]

Howard argues that it is the role of military science 'to prevent the doctrines being too badly wrong' and therefore it is important to shape the understanding of cyberspace to ensure that its development is at least on an appropriate intellectual trajectory.[40] Whether or not the Fifth Domain doctrine proves correct and endures over time, it has been adopted much more broadly than the US DoD, most notably across NATO and European nations.[41] However, whilst cyberspace has been accepted as a military domain, it also has significant utility across the other levers of power.[42] Whilst cyberspace is to some extent a metaphor, the Fifth Domain nomenclature does start to aid understanding of the role of cyberspace as part of joint military operations. This paper therefore accepts the utility of the Fifth Domain in a semantic sense and now turns to consider its practical utility.

Cyber Defence and Cyber Dependence

A nation's relative strength in cyberspace is not only related to the efficacy of its offensive capabilities; it is also heavily influenced by its defensive cyber capabilities and its dependence on cyberspace. Admiral Mike McConnell makes a fairly evident observation regarding US reliance on technology which highlights an important aspect of the Fifth Domain:

> 'Because we are the most developed technologically – we have the most bandwidth running through our society and are more dependent on that bandwidth – we are the most vulnerable'.[43]

Clarke and Knake rank the 'overall cyber war strength' of a number of nations by scoring them according to three factors: offense, defence and dependence.[44] Whilst their scoring mechanism is crude, it does illustrate that states with highly developed offensive cyber capabilities are not necessarily the best equipped to win in the Fifth Domain. An actor with a relatively low offensive capability may succeed against a more capable offensive actor if it is less dependent on cyberspace. Below the nation state level this is particularly true of military forces. Tibbs contends that 'the risk for the Pentagon, with its strong reputation as a "technology shop," is that an over-emphasis on technology could become an Achilles heel'.[45]

Any actor considering the utility of integrating cyberspace within joint military operations must weigh options to attack through cyberspace against its ability to block or mitigate the effects of a cyber-response from an adversary. In recent conflicts, the US and its allies have enjoyed a significant advantage because military power has been employed against much weaker adversaries. In cyberspace, the technological advantage enjoyed by Western states may actually be a vulnerability and could potentially allow a technologically inferior adversary to gain asymmetric advantage. Highly advanced platforms and weapons systems are by their

nature highly dependent on cyberspace. Cyber dependence, 'the extent to which a nation is wired, reliant upon networks and systems that could be vulnerable', can only be mitigated with a commensurate focus on defence.[46]

This reliance coupled with the fact that 'security on the Internet has never been anything but a vague intention' means that a broad range of vulnerabilities exist that could potentially be exploited by an adversary.[47] Cyber defence is underpinned by three core principles of information security: confidentiality, integrity and availability.[48] Effective cyber defence addresses all three principles based on the criticality of the information to the organisation. Appropriate defensive measures are put in place based on risk assessment. Where information is assessed as having particular sensitivity, it will be afforded greater protection to assure its confidentiality. Similarly, where the integrity or availability are 'mission critical', measures need to be taken to ensure that system availability cannot be degraded or data cannot be modified by an unauthorised source.

Cyber defence can broadly be divided up into active and passive measures. The passive measures are those associated with 'cyber hygiene', including managing the behaviour of system users, maintaining updates of software and hardware and the use of intrusion detection systems and firewalls.[49] These passive measures are well established and represent the day-to-day activity of protecting a network against an ever-changing threat landscape. More controversially, active defence includes pre-emptively attacking an aggressor, which could include using a cyber-attack to prevent or deter an imminent attack. Whilst the right to self-defence is enshrined in international law, it is unclear how this may apply in practice in cyberspace.[50] An attack in the Fifth Domain may not be apparent in advance; there may not be evidence of 'enemy forces massing on the border' that might occur in the physical domains. Hence, pre-emptive proof of a need to act in self-defence may be problematic until an attack has begun.

Farwell and Rohozinski argue that whilst 'Clausewitz believed that in warfare, the advantage rested with the defence. Cyber reverses that equation'.[51] However, the likelihood of the Fifth Domain marking a return to a doctrine of '*Attaque à outrance*, or "Attack to excess"' seems unlikely.[52] It may be tempting to be seduced by investing predominantly in offensive capabilities in the belief that the 'best defence is attack'. However, highly cyber-dependent states are particularly vulnerable if they do not protect themselves adequately. Singer and Friedman argue that in fact 'the best defense *[sic]* actually is a good defense… any steps that raise the capabilities of the defense make life harder on the offense and limit the incentives for attacks in the first place.'[53] If defensive measures remain effective, only the most capable and determined attacker would be able to breach them.

The reality for highly developed states that wish to carry out offensive acts in cyberspace is that retaliation may not come back directly at the military forces that instigated the attack. Whilst armed forces may choose to harden their systems against a cyber-response, 'the ongoing

cyber sabotage conflict between the United States and Iran demonstrates that Internet commerce provides a soft target for retaliation.'[54]

Ultimately the ability to attack and the requirement to defend in cyberspace comes largely as a result of errors; either errors in the software coding of the systems or of the users not using them in the manner intended.[55] Perfectly written and executed code, operated by perfectly behaved users is unlikely to contain exploitable vulnerabilities. However, code is generally written by humans who are error prone and software is increasingly becoming more complex, increasing the challenge of making it error free. In addition to attacks that exploit software vulnerabilities, some attacks, such as Distributed Denial of Service (DDoS) attacks overwhelm the hardware and software resources of the target system by flooding them with more traffic than they can handle.[56]

The post-1991 US style of Network Centric Warfare is arguably the reason why the US is concerned about warfare in the Fifth Domain.[57] It is clear that the dependence of military forces on advanced technology and network connectivity brings a range of threats and opportunities. 'Fifth generation' weapons platforms may be particularly resilient against conventional threats, but threats in cyberspace may represent a chink in their armour. Countering threats to modern weapons platforms may require a much more holistic approach to cyber defence than simply protecting computer networks. The network-centric weapons platform is surrounded by numerous supporting systems that may represent an attack vector. These may include the component supply chain, engineering and logistics support systems, and power and environmental control systems. The increased reliance on 'on-board computers and network connections' presents the risk that 'equipment does not function as and when expected… [adding] enormously to the fog and friction of any incident.'[58] Vulnerabilities discovered in modern military equipment, such as the new US Littoral Combat Ship, highlight the need to ensure adequate cyber defence through design, development and whilst in operation.[59]

However, the extent of concern over cyber dependence has led to questionable pronouncements by US government officials, such as US Defense Secretary Leon Panetta's warning of the possibility of 'Cyber Pearl Harbour'.[60] Whilst such frightening claims help the US DoD gain support for their mission to 'defend the US nation in cyberspace,' the comparison between the cyber threat and the Second World War attack on Pearl Harbour undermines the credibility of the debate and detracts from the reality of the threat. From the perspective of Fifth Domain, attacks on US infrastructure, whether or not related to actual conflict, become the realm of the US military. Most other western nations have thus far not delegated the responsibility of protecting their critical national infrastructure to military forces. A military cyberspace role outside of conflict raises the question of whether a cyber -attack might elicit an offensive cyber response or a conventional military one if attribution can be proved and it crosses a nation's response threshold. The delegation of responsibility for the task of defending the nation in cyberspace is a significant step in militarizing the Fifth Domain.

Military Theorists and the Fifth Domain

Colin Gray contends that 'one day there will be competent and robust specific general theories of space power and cyber power, but they do not exist as of yet'.[61] Whilst we wait for a Clausewitz, Mahan or Douhet to write a theory appropriate for the Fifth Domain, there are elements of existing theory that have direct relevance to the use of cyberspace in war. Conversely there are dangers in applying false lessons from the theories of war on land, sea and in the air to cyberspace. Analogies have been drawn between the emergence of cyber power at the start of the 21st Century and the emergence of air power a century earlier. However, in the absence of a cyber-power theory Gray highlights the dangers of trying to 'fold space power and cyber power into air power theory and doctrine'.[62] This paper makes no attempt to address the lack of cyber power theory but instead it draws on existing theory to determine its relevance to military operations in an increasingly cyber dependant age.

The basic principles of war retain their applicability in the Information Age. Despite changes to its character, its nature endures: war remains 'an act of force to compel the enemy to do our will'.[63] J.F.C. Fuller argued that in order to defeat an adversary, force must be applied to best effect against the three components of fighting power: the physical, mental and moral.[64] The aim is to apply sufficient force against these three components to achieve the ends. Hence the aim may not be the physical destruction of enemy fighting power, but adequate destruction, coupled with mental disorientation to cause sufficient weakening of the enemy's will to resist.[65] The ability of cyberspace to degrade the physical component may be limited, but there is clear utility in using cyberspace operations to affect the mental and moral components.

The birth of air power brought with it much promise of a new way to fight wars. Early theorist Giulio Douhet saw air power as a means of avoiding the bloody attrition of trench warfare seen during the First World War.[66] Douhet's theories centred on offensive action based on the use of 'bombardment units' that could strike deep into enemy territory.[67] The promise of air power was that it could replace the need for land battle. Hugh Trenchard similarly advocated the use of independent air power and stressed the psychological effects as well as the physical, arguing that 'the moral effect of bombing stands undoubtedly to the material effect in a proportion of 20 to 1'.[68] However, during the Second World War, air power failed to live up to the bold claims made by Douhet and Trenchard. Air power's contribution was significant, both as an independent instrument and when integrated with the land and maritime domain; however, it was not decisive in its own right. Air power neither caused the precisely-targeted destruction required to bring out victory in its own right, nor did it shatter the morale of the civilian populations who were subjected to its effects.

Similarities clearly exist between the early claims for air power and the notions of war in the Fifth Domain. In particular, the hyperbole evident in some of the early air power theorists is evident in some of the discussions regarding cyberspace. Cohen argues that 'Air power is an unusually seductive form of military strength, in part because, like modern courtship, it appears to offer gratification without commitment'.[69] The idea that future wars will be fought

in cyberspace is another example of the seductive nature of new technology, which is unlikely to live up to the hype. Cyberspace operations have some similarities with air power, most notably in their characteristics of speed and reach. Theoretically at least, cyber power, like air power can respond quickly to a crisis and deliver effects at range, without committing ground troops. Where cyber power and air power differ is in their ability to be violent. Beyond the potential for very limited material destruction cyberspace operations do not include violence or the threat of violence.

Douhet firmly held the belief that the best form of defence was offense and as a consequence he dismissed ideas of air defence, convinced that it could not meet its aim.[70] The current debate of cyberspace favouring the offensive is reminiscent of Douhet's claims. Stanley Baldwin's prediction that 'the bomber will always get through' was no more accurate than any ideas of malware always getting through.[71] Effective cyber defence is as important as effective air defence. Douhet advocated attacking enemy airfields and aircraft industry, favouring 'destroying the eggs in their nest' rather than meeting the enemy in aerial combat.[72] This concept of attacking at the point of greatest vulnerability clearly has validity in the Fifth Domain. Rather than attacking military networks whilst deployed on operations, it may be more appropriate to attack the component supply chain.

The 1991 Persian Gulf War was heralded as a Revolution in Military Affairs and marked a change in the American 'way of war'.[73] The manner in which air power was employed has been characterised as 'parallel warfare… based upon achieving specific effects, not absolute destruction of target lists.'[74] The concepts behind 'parallel warfare' are attributed to the US Air Force officer and air power theorist, John Warden. Warden's 'Five Strategic Rings' model was the basis for the 1991 Persian Gulf War air campaign, where instead of sequentially 'rolling back' enemy defences, emerging technologies of stealth and precision guided munitions enabled simultaneous access to the 'leadership... organic essentials, infrastructure, population and fielded forces'.[75] Whilst this approach brought about rapid victory, some of the targets destroyed by air power in Iraq in 1991 and again in 2003 left a legacy of civilian hardship that arguably later fuelled an insurgency. Short-term cyber disruption to infrastructure and organic essentials as an alternative to the long term destruction caused by air power may therefore be preferable in some cases. Warden advocated '… [thinking] of the enemy as a system composed of numerous subsystems' this he argued, would achieve success with the minimum effort'.[76] The application of Warden's 5 Rings Model and systems approach is arguably viable for the conduct of Fifth Domain operations. Cyberspace can give reach into the leadership ring and could potentially complement kinetic effects across the other strategic rings. However, closer examination is required to determine whether cyber effects are a viable alternative or indeed if they are even possible in practice. Leed argues that:

> 'Conceptually, offensive cyber operations offer a source of "fires" whose degree of lethality can be tailored to the situation at hand, be (at least in some instances) reversible, and may prove less costly than alternative methods of pursuing similar effects.'[77]

However, applying ideas of parallel war in cyberspace is reliant upon the character of the war resembling the post-1991 American way of war. Recent history has shown that the state-on-state war may not represent the dominant form of warfare and 'popular theories of the 1990s [have] withered in the cultural realities of the wars that followed 11 September 2001'.[78]

Arguments For and Against Fifth Domain Utility

The military utility of cyberspace is not simply a function of the ability to launch attacks against an adversary. Like the physical domains, military forces require 'freedom of manoeuvre' in cyberspace to ensure that operations can be conducted without an adversary being able to unduly constrain that freedom. This may require the ability to protect networks and platforms using active and passive means. Ensuring freedom of manoeuvre implies that military forces must try to exert some form of control over cyberspace but, unlike the physical domains, the nature of cyberspace means that exerting absolute geographic control is impracticable. Like the air domain, control in cyberspace may be limited in time and space, although the spatial component may relate to logical, rather than physical space.

Exerting some degree of control over cyberspace does not imply that it is possible or even desirable to exert control over the Internet. Whilst some have argued that the Internet is a 'global commons', that cannot or should not be owned or controlled, its physical manifestations are in fact divided up with the same approach to territorial ownership as the artificial lines on a map that define nation states.[79] Some states have configured their portions of the Internet in a manner that would make controlling or limiting access almost impossible, others have intentionally designed network infrastructure to facilitate authoritarian control over access to information. Whilst it is debatable whether exerting control over the public Internet during conflict is a practicable proposition, Libicki contends that 'the ability to command or at least to confound the Internet of foreign countries is likely to be of modest *military* value'.[80] In fact in some circumstances the desired outcome may be to ensure that free and open access to the Internet is maintained, not constrained.

Despite the hype around the risks of 'cyber-attack', it is arguably not a particularly effective means of applying military force in its own right. Tibbs argues that:

> 'Networked digital computers are enormously powerful tools for collaboration, but lack many fundamental properties required to apply hard power with coercive intent. Unlike aircraft, their direct application as a form of warfare is non-obvious. However, their capabilities are extraordinarily well suited to … cyber espionage and cyber sabotage'.[81]

Whilst cyber effects are unlikely to be coercive in their own right, the use of 'cyber sabotage' is likely to increasingly be an important part of warfare, reflecting increasing cyber dependence. The use of 'wartime cyberattacks against military targets and military-related civilian targets' is described by Libicki as 'operational cyberwar'.[82] Operational cyberwar is distinct from any ideas of 'Cyber War' *per se*. Discrete cyber war is problematic, largely due to its lack of potential

for violence, highlighted previously, but also for the difficulty in achieving demonstrable attribution. However, questions of attribution become irrelevant during a conflict in the physical domains, 'it is usually a straightforward matter to determine the nation responsible, since the conflict takes place during an ongoing geo-political crisis'.[83] Cyber effects during a conflict are not independent acts, but are integrated to a greater or lesser degree with the ongoing physical conflict. Betz and Stevens argue that 'while military cyber power is likely to be efficacious, it will not be so in itself.'[84]

In order to assess how cyber operations might usefully be employed, the characteristics of a cyber-attack need to be established, most notably the use of software code as a weapon. Accepting that thus far 'not a single human being has been killed or hurt as a result of a code-triggered cyber attack', the nature of a 'cyber weapon' is clearly different to a conventional kinetic weapon.[85] Kinetic weapons are designed to cause physical damage to humans or property. Whilst kinetic weapon choice can limit scale and severity in order to vary the effect to be delivered, it must result in inflicting some degree of violence on its target. As a consequence, to some extent the effects of the weapon will endure after its use; wounds need time to heal, buildings must be rebuilt and infrastructure must be repaired. In many cases it may be desirable to degrade an enemy's military capability by putting it permanently beyond use. Cyber effects however, are often reversible so where the intention is to permanently deprive an enemy of a military capability, cyber operations may be inappropriate.

Conversely, the non-enduring nature of a cyber-attack may be advantageous. Wars are costly both in terms of human life and in the economic costs of recovery. Where a state's infrastructure is destroyed, it must be rebuilt post-conflict, with a moral responsibility often falling on the victor to support the recovery. This makes reversible cyberspace operations a tempting choice. Leed argues that:

> '…if a cyber weapon could be used instead of a kinetic weapon to cause a temporary and reversible effect as opposed to a permanent one (e.g., raise a bridge instead of blow it up, or temporarily turn off the lights in a local area instead of destroying a local grid), the [US] could theoretically avoid the costs of rebuilding or repairing infrastructure.'[86]

Whilst achieving a reversible cyber effect may not be a trivial undertaking, it may become not only desirable, but necessary, particularly when the target is something that has a dual military and civilian use. Based on the norms of International Law, if a belligerent has the capability to achieve military advantage with a less destructive means, the principle of proportionality may even *require* its use.[87] Moreover, if victory is dependent on gaining and maintaining the support of an indigenous population, levels of destruction that cause suffering and undermine their way of life are unlikely to ensure their support or acquiescence.

Arguably, increasingly effective cyber defence overcomes all but the most capable and determined offensive cyber actor. Whilst a military force may put significant effort into

developing a 'cyber weapon', the 'weaponised code' can quickly become obsolete. Unlike conventional kinetic weapons which often have broad use in a number of different attack scenarios, cyber weapons are generally aimed at exploiting a specific type of vulnerability in a specific configuration. An offensive cyber actor might develop an attack capability, but he is not just fighting against the defensive capabilities of his enemy. In many cases the software target is likely to be a commercially available product and therefore the offensive actor is also fighting against the greatest minds of the software and IT security industry, or potentially the Open Source software movement, who continually aim to identify and remove vulnerabilities in software.

The ability of states and the global IT security industry to react to and mitigate a cyber-attack leads to the argument that a cyber-weapon 'is essentially a "one-shot" capability, [opponents] will patch the target system to prevent further attacks against the same node'.[88] In theory, a well-defended system would need to be attacked by a previously unused software exploit - the so-called 'zero-day' exploit. Once used, its effects become apparent and a patch is developed to counter the exploit. However, in practice networks may not be well defended, allowing attackers to use relatively unsophisticated methods and the evidence suggests that this is often the case: 'Verizon found… the incidents they investigated…did not involve highly sophisticated methods; 96 percent of the intrusions could have been prevented with simple or intermediate controls.'[89]

Types of cyber-weapon can be placed on a spectrum from low impact weapons that can be employed generically to those that deliver a high impact against a very specific target.[90] As for the physical domains, cyberspace weapon choice should be tailored according to the desired effect, including the desired severity and permanence. In the context of an ongoing conflict, cyber-attacks may 'aim to deny, disrupt, or degrade enemy capabilities, either directly or indirectly (e.g., through deception)'.[91] Rosenfield contends that 'the disruptive potential of cyber war is far more significant than its destructive potential'.[92] Short term cyber disruption can be quickly reversed, but if synchronised with other operations, it has the potential to be extremely effective. Farwell and Rohozinski argue that:

> 'It also offers the potential to build the fog of war through the ability to effect disruption, deception, confusion and surprise. We are only beginning to envisage the potential for different forms of malware, or the strategies or tactics employed to use it'.[93]

The 1991 Gulf War Air Campaign offers a historical case study for the potential benefits of cyber operations complementing kinetic weapons. Operation Desert Storm included air strikes to disable the electrical power grid. Despite some claims that attacks on the Iraqi power grid resulted in very limited civilian casualties, 'other critics believe that the loss of electrical power "contributed to" 70-90,000 postwar civilian deaths above normal mortality rates between Apr-Dec 1991 due to the lack of water purification and sewage treatment'.[94] The reversibility of cyber effects compared to the damage incurred by a kinetic effect arguably represents

the major advantage of Fifth Domain warfare, extending the range of effects available to a commander throughout all phases of an operation.[95]

Exploiting vulnerabilities in the software of the target becomes increasingly difficult in a well-defended system, but the system remains vulnerable through its users. In IT security, exploiting the users of a system can result in attacks that are particularly difficult to defend against.[96] Attempts at protecting IT systems have often focussed on technical solutions, access controls, antivirus software, firewalls and other security products.[97] However, it is more difficult to detect and prevent attacks that are prosecuted through exploiting the human weaknesses of legitimate users of a system. Social engineering techniques are based upon exploiting human psychology, abusing basic human traits including the desire to be helpful, a tendency to trust people and the fear of getting into trouble.[98]

Two of the ostensible advantages of attacking through cyberspace are the speed and reach of delivery; cyber effects can travel at 'net speed' and do not suffer from the same constraints of physical distance and speed that apply to a warship or even a jet aircraft. However, despite the ability to deliver a software payload to the target at speed, the desired effect may require a response from the operator of the system to respond and Libicki contends that 'human beings, unlike computers, do not work in nanoseconds. Persuasion and dissuasion in cyberwar take as much time as in wars of any other form.'[99]

UK Air & Space Doctrine argues for a role for 'Air-Cyber integration' in attacking adversary cyber capabilities to enable air operations.[100] It gives the example of attacking computer networks to degrade an adversary's Integrated Air Defence System (IADS).[101] Whilst attacking the enemy IADS may be desirable, it arguably presents a particularly challenging cyber target. The objective would be to disrupt or degrade the IADS at the critical time when a conventional air attack is being prosecuted. There has been one well known example of this when the Israeli Air Force attacked the Syrian nuclear reactor at Dayr ez Zwor in September 2007.[102] During the attack, Israeli aircraft were allegedly able to 'effectively [turn] off the Syrian air defenses *[sic]* for the night' using a cyber-attack.[103] It is claimed that the Israelis were able to do so by inserting data into the IADS; however it is not clear exactly how this was achieved and it highlights speculation regarding the extent to which other nations, such as the US may have similar capabilities.[104] For the utility of the Fifth Domain this cyber-attack, whilst not destructive in its own right was crucial 'as part of an integrated military operation'.[105]

Whilst this attack may offer a tantalising prospect for the use of the Fifth Domain, a note of caution is required. IADS are complex systems and arguably there are no generic cyber weapons to counter them. An attack would require a deep understanding of the system and a means of accessing what is almost certainly not connected to the Internet. However, Warden's systems approach is instructive in targeting such a system. The system includes the weapons, sensors, communication links and Command and Control (computer systems and decision making nodes). Understanding and exploiting the vulnerabilities via cyber-means does not

necessarily require disruption of the sensors or weapons systems that make up the heart of the system. The opportunities that may exist for exploitation may not be the disruption or destruction of computer systems, but may instead be cognitive through sowing doubt or confusion in the mind of the decision maker.

This returns to a key aspect of the Fifth Domain - the understanding of the cyber-littorals. Understanding the manner in which humans behave and interact with technology is of key importance in developing cyberspace operations. Arguably Fifth Domain warfare is as much a human sciences endeavour as it is computer science. As for war in the other domains there remains a need to understand the adversary. Despite an increasing reliance upon automated systems, the adversary is generally not the computer; it is the human who uses these systems. In the event of a system failure, reversionary modes of operation are often well practiced. Isolating a surface-to-air missile battery from its primary communications links might reduce its effectiveness, but the training and ingenuity of its operators are likely to ensure that reversionary modes of operation lessen the impact. Understanding enemy doctrine, tactics, techniques and procedures remains just as important in the Fifth Domain as it has always been in traditional warfighting.

Another challenge for the use of the Fifth Domain is in achieving an appropriate degree of assurance for a cyber-weapon. Kinetic weapons generally leave observable evidence to indicate their effectiveness and this evidence can, over time lead to a reasonable expectation that a particular weapon is likely to have a particular effect on its target. However, cyber weapons leave no visible 'bomb crater' to measure their effectiveness and the smallest change in the software system of the target could render the weapon ineffective. A modern kinetic weapon's effects are broadly predictable and repeatable; a cyber-weapon may not be. Moreover, assurance includes the ability to predict the unintended effects of a cyber-weapon, including its potential to spread to affect systems other than its intended target. Achieving an acceptable degree of assurance may rely upon the use of simulation and target modelling, which is dependent upon an accurate understanding of the configuration of the target system. Without a well-founded means of giving a commander adequate assurance, it is unlikely that he would chose an unpredictable cyber option over a tried-and-tested kinetic one.

Perhaps the greatest potential for cyberspace operations to produce effects in the physical domains, other than through cognitive effects, is through attacks on Supervisory Control and Data Acquisition (SCADA) systems, or Industrial Control Systems (ICS). These systems control numerous physical processes including manufacturing and critical infrastructure, such as electrical power, water and sanitation. ICS have been the focus of much of the hype regarding cyber-attacks, largely due to increasing concerns that they are 'designed with minimal security protection'.[106] ICS attacks have received particular scrutiny as a result of the Stuxnet attack on the Iranian nuclear enrichment facility in Natanz. However, far from setting a precedent for future attacks, Stuxnet has probably driven improvements to the security of control systems.

It also highlights the difficulties of constructing a 'cyber weapon' that can cause damage to a specific physical process. Whilst Stuxnet caused physical damage to a component of the system it was designed to attack, it required a significant intelligence effort both to understand the target system in enough detail to produce the weaponised code and to deliver it to the target.[107] The time and weight of effort required to deliver a cyber-effect may ultimately mean that in some circumstances a kinetic alternative is the cheaper, easier and timelier option.

For many states, the manner in which they plan to utilise the Fifth Domain for military operations remains shrouded in secrecy. Much of the publicly available information comes from the USA, perhaps because the US sees advantage in the general deterrence value of declaring offensive cyber capabilities. Healey cites General James Cartwright, who argues 'we've got to talk about our offensive capabilities and train for them; to make them credible'.[108] The US has published numerous official publications detailing its intention to utilise the Fifth Domain as an integrated part of warfighting, from high-level political intent down to tactical military doctrine.[109] However, other nations are clearly developing similar capabilities and Russia's doctrine reflects broadly similar military doctrine for the Fifth Domain: 'Russia sees information warfare capabilities as including computer network operations, electronic warfare, psychological operations, deception campaigns (maskirovka), and the deployment of malware, back doors and logic bombs'.[110] The UK government has expressed its intent 'to develop new tactics, techniques and plans to deliver military effects' and to '[mainstream] cyber in military operations'.[111]

The novelty of Fifth Domain operations has caused legal experts to debate the implications of their use in conflict. The NATO Cooperative Cyber Defence Centre of Excellence has issued 'The Tallinn Manual on the International Law Applicable to Cyber Warfare'.[112] This manual is the result of the collaboration of international legal and cyber security experts, with the aim of establishing the norms of behaviour in cyberspace, based on extant international law. Crucially, rather than calling for specific laws for dealing with the Fifth Domain, it argues that the Law of Armed Conflict applies to cyber operations in the same manner as other operations within an international or non-international armed conflict.[113] This means that cyberspace belligerents must apply the same principles of necessity, proportionality, distinction and humanity that apply in all forms of conflict.

The Tallinn Manual is less clear on the circumstances where an attack in cyberspace would constitute a 'use of force' that would permit an armed response.[114] The discord between nations on the 'use of force' is reflected in the differing missions delegated to military forces. For example US Cyber Command, beyond protecting military networks and supporting the regional Combatant Commanders, is delegated specific responsibility to 'defend the nation in cyberspace'.[115] This mission probably represents the most problematic use of the Fifth Domain. Unlike the use of cyber effects during conventional combat, defending broader national interest against cyberspace attack requires attribution to be determined in forensic detail and risks escalating non-violent attack into an armed conflict.

Conclusion

This paper has addressed the utility of the Fifth Domain in both a semantic sense and in terms of the practical utility of military operations in cyberspace. The debate around cyberspace is replete with ambiguous terminology and the common usage of the term 'cyber' lacks the precision required for it to be meaningfully applied to military operations. A number of nations have developed doctrine for cyberspace operations, but the US has led the debate in favour of declaring cyberspace as a warfighting domain. This paper has accepted the US DoD definition of cyberspace as broadly appropriate and meaningful in establishing the case for a Fifth Domain of operations.

Various national debates regarding cyber security have led to armed forces in a number of countries staking their claim to new financial resource and for the additional responsibility of cyberspace missions. Cyberspace has both physical and virtual manifestations and it interfaces with all the other domains, rather than being part of one physical domain in particular. These facts strengthen the case for independent domain status. It is necessary to develop personnel with an innate knowledge of cyberspace - just as an airman intuitively understands the principles that underpin operating and fighting military aircraft, cyber operators need an intuitive understanding of their domain.

Despite significant alarmism regarding the threat of cyber-attack, Fifth Domain operations are not solely the preserve of offensive cyber actors. The dependence on cyberspace of technologically-advanced Western states requires that commensurate effort is put into cyber defence. This is particularly true for military forces that gain their military advantage through advanced weapon systems. Armed forces that rely upon their technology without appropriately protecting it from cyber threats, offer their opponents an opportunity to gain asymmetric advantage.

A wealth of literature has appeared arguing for and against cyber power utility, although it lacks the firm theoretical foundations that have been developed in the other warfighting domains. However, there are elements of existing theory which have relevance in the Fifth Domain and the development of cyber-power concepts echoes those of the other domains, particularly the early days of air power. Fallacious arguments of air power being able to remove the requirement for land battle are reflected in similar claims for cyberwar. Cyberspace changes the character of war, but as with all technological change, the basic nature of warfare endures. Many of the extant theories of war retain their validity even when cyberspace effects are integrated into a campaign.

Military operations in the Fifth Domain cannot replace those on land, sea and in the air but they can complement and enhance them. Cyberspace effects in their own right are poor military instruments, they lack the potential to be violent and therefore cannot necessarily be coercive in the same manner that a ground invasion, bombing campaign or port blockade can be. The real potential of the Fifth Domain lies in carefully synchronising cyber operations with

operations in the physical domains to cause disruption, and support deception and confusion. Cyber effects can cause short term, reversible disruption to technology that has the potential to give advantage to an attacker in a way not possible with kinetic effects. Cyberspace has the ability to make elements of warfare potentially less violent, but can only do so if backed up by the potential for violence from the other domains. Beyond reversible disruption, cyberspace offers the potential to sow the seeds of doubt in the mind of an enemy operator or decision maker. It can do so by presenting him with conflicting, ambiguous or incorrect information that plays upon cognitive, rather than physical vulnerabilities.

The particular missions for cyber forces will evolve over time, based upon national and international legal and policy constraints, but equally as a result of practical experience of the effectiveness of choosing cyberspace from the range of military levers. Some of the proposed missions for cyber weapons, such as defeating IADS or ICS, present a tantalising prospect for military commanders. However, it may prove that these 'hard' targets do not represent the norm of future cyber operations. Cyberspace effects may end up being more efficacious when employed against more generic target sets, rather than highly complex bespoke systems.

Arguably a key measure of success for cyberspace as the Fifth Domain of warfare is when it is effectively 'mainstreamed'. When the novelty of cyberspace wears off, discussions of 'cyberwar' will naturally fade away. Cyberspace operations will eventually 'normalise' and the Domain will become an integral part of joint warfare. Whilst there are many aspects to cyberspace in the world of business, entertainment, communication and knowledge sharing, there is a clear military role. The Fifth Domain of warfare has significant utility for 21st Century conflict and the classification of cyberspace as a domain is both entirely appropriate and necessary as a reflection of the reality of technology.

Notes

[1] This article is adapted from 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 Mar 14.
[2] Hayden, Michael V. (2011), 'The Future of Things "Cyber"', *Strategic Studies Quarterly*, Vol. 5, No. 1, p3
[3] HM Government (2010a), *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, (Norwich: The Stationery Office), p27
[4] Gray, Colin S. (2002), *Strategy for Chaos: Revolutions in Military Affairs and the Evidence of History* (London: Frank Cass), p33
[5] Libicki, Martin C. (2011b), 'Cyberspace Is Not a Warfighting Domain,' *I/S: A Journal of Law and Policy for the Information Society*, Vol. 8, No. 2, p322
[6] Hayden (2011), p3
[7] Galison, Peter (1994), 'The Ontology of the Enemy: Norbert Wiener and the Cybernetic Vision,' *Critical Enquiry*, Vol. 21, No. 1 p232
[8] Ibid.

[9] Tibbs, Hardin (2013), *The Global Cyber Game: Achieving Strategic Resilience in the Global Knowledge Society*, (Shrivenham, UK: Defence Academy), p81
[10] Oxford Dictionary of English
[11] Rid, Thomas (2013), *Cyber War Will Not Take Place*, (London: Hurst), p164
[12] Oxford Dictionary of English
[13] US DOD Dictionary of Military Terms http://www.dtic.mil/doctrine/dod_dictionary/index.html?zoom_query=cyberspace&zoom_sort=0&zoom_per_page=10&zoom_and=1, 31 December 2013
[14] Singer, P.W. & Allan Friedman (2014), *Cyber Security and Cyberwar*, Kindle Edition (New York, NY: Oxford University Press), p13
[15] Development, Concepts and Doctrine Centre (2014), *Joint Concept Note 1/14 (JCN 1/14): Defence Joint Operating Concept* (Shrivenham: DCDC), p Afterward-4
[16] Oxford English Dictionary http://www.oxfordreference.com/view/10.1093/acref/9780199571123.001.0001/m_en_gb0237570?rskey=hoSYdy&result=5, 25 January 2015
[17] Gray (2002), p33
[18] Libicki (2011b), p321
[19] Rid (2013), pp. 1-2
[20] Ibid., p3
[21] Ibid., pp.165-166
[22] Ibid., p165
[23] HM Government (2010b), *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*, (Norwich: The Stationery Office), p47
[24] Rid (2013), p166
[25] The US DoD Dictionary of military terms defines an 'effect' as 'the physical or behavioural state of a system that results from an action, a set of actions, or another effect', http://www.dtic.mil/doctrine/dod_dictionary/index.html?zoom_query=effect&zoom_sort=0&zoom_per_page=10&zoom_and=1, 1 March 2014
[26] Tibbs (2013), p29
[27] DOD Dictionary of Military Terms http://www.dtic.mil/doctrine/dod_dictionary/index.html?zoom_query=cyberspace&zoom_sort=0&zoom_per_page=10&zoom_and=1, 31 December 2013
[28] US Air Force, http://www.airforce.com/learn-about/our-mission/, 3 January 2014
[29] Rid (2013), p166
[30] Oxford English Dictionary http://www.oxfordreference.com/view/10.1093/acref/9780199571123.001.0001/m_en_gb0237570?rskey=hoSYdy&result=5, 31 January 2013
[31] Gray, Colin S. (2012), *Airpower for Strategic Effect* (Maxwell Air Force Base, AL: Air University Press), p300
[32] Singer and Friedman (2014), p134
[33] 'Time for a U.S. Cyber Force', http://www.usni.org/magazines/proceedings/2014-01/time-us-cyber-force, 31 January 2014
[34] Tibbs (2013), p63

[35] Ibid., p105
[36] Singer & Friedman (2014), p13
[37] The term 'cyber-littorals' originates from internal UK Ministry of Defence discussions.
[38] Singer and Friedman (2014), p13
[39] Howard, Michael (1974), 'Military Science in the Age of Peace', *The RUSI Journal*, Vol. 119, No.1, p7
[40] Ibid.
[41] Klimburg, Alexander (Ed) (2012), *National Cyber Security Framework Manual*, (Tallinn: NATO CCD COE), p28
[42] Ibid.
[43] Clarke, Richard and Robert Knake (2010), *Cyber War: The Next Threat to National Security and What to Do About It*, (New York, NY: Harper Collins), p145
[44] Ibid., p148
[45] Tibbs (2013), p50
[46] Clarke & Knake (2010), p148
[47] Orman, Valerie (2003), 'The Morris Worm: A Fifteen-Year Perspective', *IEEE Security and Privacy*, September/October 2003, p35
[48] Tipton, Harold F., ed. (2010), *Official (ISC)2 Guide to the CISSP CBK*, (Boca Raton, FL: Auerbach Publications), p4
[49] Farwell, James P. & Rafal Rohozinski (2012), 'The New Reality of Cyber War', *Survival: Global Politics and Strategy*, Vol. 54, No. 4, pp. 107-120, p109
[50] Ibid., p110
[51] Ibid., p114
[52] Singer and Friedman (2014), p153
[53] Ibid., p155
[54] Tibbs (2013), p94
[55] Libicki, Martin C. (2009), *Cyberdeterrence and Cyberwar*, (Santa Monica, CA: RAND), p18
[56] Ibid., p130
[57] Tibbs (2013), p93
[58] Ibid., p72
[59] 'Cyber vulnerabilities found in Navy's newest warship: official', **http://uk.reuters.com/article/2013/04/24/us-usa-cybersecurity-ship-idUSBRE93N02X20130424**, 13 February 2014
[60] 'Panetta Warns of Dire Threat of Cyberattack on U.S.', **http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=0**, 13 February 2014
[61] Gray (2012), p35
[62] Ibid.
[63] Clausewitz, Carl von (1997), *On War*, tr. J.J. Graham (Ware, Hertfordshire: Wordsworth Editions), p5
[64] Fadok, David S. (1997), 'John Boyd and John Warden: Airpower's Quest for Strategic Paralysis', in P. Meilinger, ed, *The Paths of Heaven: The Evolution of Airpower Theory* (Alabama: Air University Press), p359

[65] Ibid.
[66] Meilinger, Philip S. (1997), 'Giulio Douhet and the Origins of Air Power Theory', in P. Meilinger, ed, *The Paths of Heaven: The Evolution of Airpower Theory* (Alabama: Air University Press), p17
[67] Ibid., p14
[68] Budiansky, S. (2005), *Air Power: The Men, the Machines, and Ideas that Revolutionized War, from Kitty Hawk to Iraq* (London: Penguin), p131
[69] 'The Mystique of U.S. Air Power', http://www.foreignaffairs.com/articles/49442/eliot-a-cohen/the-mystique-of-us-air-power, 13 February 2104
[70] Meilinger (1997), p10
[71] Ibid., p20
[72] Ibid., p10
[73] Deptula, David A. (2001), *Effects Based Operations: Change in the Nature of Warfare*, (Arlington, VA: Aerospace Education Foundation), p1
[74] Ibid., p3
[75] Fadok (1997), p372
[76] Warden, John A. (1995), 'The Enemy as a System', *Airpower Journal*, Vol. 9, No. 2, npn
[77] Leed, Maren (2013), *Offensive Cyber Capabilities at the Operational Level: The Way Ahead*, (Washington, DC: Center for Strategic and International Studies), pV
[78] Betz, David and Tim Stevens (2011), *Cyberspace and the State: Towards a Strategy for Cyber-Power*, (Abingdon, Oxon: Routledge), p88
[79] Singer and Friedman (2014), p14
[80] Libicki (2011b), p327
[81] Tibbs (2013), p91
[82] Libicki (2009), p139
[83] Healey, Jason (Ed) (2013), *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, (Vienna, VA: Cyber Conflict Studies Association), p21
[84] Betz and Stevens (2011), p89
[85] Rid (2013), p13
[86] Leed (2013), p8
[87] Murray, Scott F. (2007), *The Moral and Ethical Implications of Precision-Guided Munitions*, (USAF School of Advanced Air and Space Studies thesis), p41
[88] Development, Concepts and Doctrine Centre (2013), *Joint Doctrine Publication 0-30 (JDP 0-30): UK Air and Space Doctrine*, (Shrivenham: DCDC), pp.4-10 – 4-11
[89] Healey (2013), pp. 36-37
[90] Rid, Thomas & Peter McBurney (2012), 'Cyber-Weapons', *The RUSI Journal*, Vol. 157, No. 1, p8
[91] Leed (2013), p3
[92] Rosenfield, Daniel K. (2009), 'Rethinking Cyber War', *Critical Review: A Journal of Politics and Society*, Vol. 21, No. 1, p78
[93] Farwell and Rohozinski (2012), p114
[94] Gingras, Jeffrey L. and Tomislav Z. Ruby (2000), *Morality in Modern Aerial Warfare* (Air Command and Staff College Air University thesis), p25
[95] Leed (2013), p1

[96] Peltier, Thomas (2006), 'Social Engineering: Concepts and Solutions', *Information Systems Security*, Vol. 15, No. 5, p14
[97] Ibid.
[98] Ibid., p13
[99] 'Don't Buy the Cyberhype: How to Prevent Cyberwars from Becoming Real Ones' http://www.foreignaffairs.com/articles/139819/martin-c-libicki/dont-buy-the-cyberhype, 13 February 2014
[100] Development, Concepts and Doctrine Centre (2013), p4-10
[101] Ibid.
[102] Rid (2013), p42
[103] Singer and Friedman (2014), p127
[104] 'The Israeli 'E-tack' on Syria' http://www.airforce-technology.com/features/feature1625/ and http://www.airforce-technology.com/features/feature1669, 13 February 2014
[105] Rid (2103), p42
[106] Trias, Eric D. & Bryan M. Bell (2010), 'Cyber This, Cyber That… So What?', *Air and Space Power Journal*, Vol. 24, No. 1, p93
[107] Rid (2013), p106
[108] Healey (2013), p86
[109] Department of the Army (2014), *FM3-38: Cyber Electromagnetic Activities*, (Washington DC: Department of the Army), pp. v-vi
[110] Tibbs (2013), p59
[111] 'Defence Select Committee: Written evidence from the Ministry of Defence', http://www.publications.parliament.uk/pa/cm201012/cmselect/cmdfence/writev/1881/dcs01.htm, 3 January 2014
[112] Schmitt, Michael N. (2013) *Tallinn Manual on the International Law Applicable to Cyber Warfare*, (New York, NY: Cambridge University Press)
[113] Ibid., p75
[114] Ibid., p48
[115] 'Secretary of Defense Speech', http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1728, 3 March 2014