JOINT SERVICES
COMMAND AND STAFF COLLEGE

DEFENCE RESEARCH PAPER

By

WG CDR M G BROCKIE

ADVANCED COMMAND AND
STAFF COURSE

NUMBER 17

SEP 13 – JUL 14

INTENTIONALLY BLANK

Defence Research Paper

Submission Cover Sheet

Student Name:	Wg Cdr M G Brockie
Student PIC Number:	13-02823
DRP Title:	**Cyber: buzzword or instrument of national power?**
Syndicate:	A6
Syndicate DS:	Wg Cdr Rob Gue
DSD DRP Supervisor:	Dr Mark Hilborne
Essay submitted towards <u>psc(j) only</u> *or* <u>MA and psc(j)</u>?	MA and psc(j)

Sponsored/Proposed Topic? Yes/No	No
Word Count:	14,991

I confirm that this Research Paper is all my own work, is properly referenced and in accordance with Standard Operating Procedure T10.

Signature: Date:

INTENTIONALLY BLANK

UK Student Disclaimer

"The views expressed in this paper are those of the author and do not necessarily represent those of the UK Ministry of Defence, or any other department of Her Britannic Majesty's Government of the United Kingdom. Further, such views should not be considered as constituting an official endorsement of factual accuracy, opinion, conclusion or recommendation of the UK Ministry of Defence, or any other department of Her Britannic Majesty's Government of the United Kingdom".

INTENTIONALLY BLANK

CYBER: BUZZWORD OR INSTRUMENT OF NATIONAL POWER?

WG CDR M G BROCKIE RAF

ADVANCED COMMAND AND STAFF COURSE

NUMBER 17

Word Count: 14,991

INTENTIONALLY BLANK

ABSTRACT

The rapid development of information and communications technology has transformed the world to the extent that cyber capabilities now underpin everyday life, which has created both opportunities and vulnerabilities. There is currently no consensus on the importance of cyber capabilities or their consequences on the conduct of the war. At one end of the spectrum, cyber is viewed as hype with no substance. At the opposite end, cyber capabilities are considered to be able to yield devastating effects without the need to put people in harm's way. This paper analyses the field of cyber to determine where cyber sits on the spectrum between the two extremes of buzzword and a new instrument of national power. Using information presented in academic, government and military literature, the paper concludes that cyber is neither a buzzword nor an instrument of national power. Cyber is a vital capability that cannot be ignored due to its importance to civilian and military life. It provides both an enabling function to the diplomatic, economic and military instruments of national power in support of strategic aims, and a means for conducting information operations.

INTENTIONALLY BLANK

INTRODUCTION

> People think of military as land, sea and air. We long ago recognised a fourth – space. Now there's a fifth – cyber.
>
> Cyber is the new frontier of defence. For years, we have been building a defensive capability to protect ourselves against these cyber attacks. That is no longer enough.
>
> You deter people by having an offensive capability. We will build in Britain a cyber strike capability so we can strike back in cyberspace against enemies who attack us, putting cyber alongside land, sea, air and space as a mainstream military activity. Our commanders can use cyber weapons alongside conventional weapons in future conflicts.[1]
>
> Rt Hon Phillip Hammond MP

The exponential development of information and communications technology has transformed the world. It is one of the principal enablers of globalization which has resulted in societies becoming increasingly interconnected to the extent that events in one location have an effect on people and societies in a distant other location.[2] Cyber has become the common word used, either on its own or combined with another, when referring to all aspects of information and communications technology. The adjective cyber originated in the 1980s as an abbreviation of cybernetics and is defined as, "relating to or characteristic of the culture of computers, information technology, and virtual reality".[3] Cyber is also commonly used as a noun[4] to mean "cyberspace or more generally the Internet".[5] Cyberspace, "the notional environment in which communication over computer networks occurs",[6] is credited with stimulating economic growth through engendering open markets and societies.[7] As a consequence, states have embraced cyberspace to exploit the benefits and opportunities it offers but this has also created dependencies with resultant vulnerabilities and threats.[8] Likewise, cyberspace has proved to be a double-edged sword for many armed forces that have taken advantage of information and communications technology to improve their effectiveness in the conventional, physical domains of land, air, maritime and space.

---

[1] United Kingdom. Development, Concepts and Doctrine Centre (DCDC). *Cyber Primer*. (Shrivenham: DCDC, 2013), iii.

[2] John Baylis, Steve Smith and Patricia Owens, *The Globalization of World Politics: An introduction to international relations* (Oxford: Oxford University Press, 2011), 8.

[3] Oxford Dictionary of English, 2nd ed.

[4] Cyber will be used in both noun and adjective form in this paper.

[5] Hardin Tibbs, *The Global Cyber Game: The Defence Academy Cyber Inquiry Report* (Shrivenham: Defence Academy, 2013), 81.

[6] Oxford Dictionary of English, 2nd ed.

[7] United Kingdom. Cabinet Office. *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world.* (London: Cabinet Office, 2011), 7.

[8] Ibid., 15.

This use of technology has made them susceptive to offensive cyber operations that could have a significant impact on their operational effectiveness.[9] The situation was summarised concisely by President Barack Obama, "it's the great irony of our Information Age – the very technologies that empower us to create and to build also empower those who would disrupt and destroy".[10]

In 2013 the UK Secretary of State for Defence, Phillip Hammond, publically announced that cyberspace was recognised as the fifth military domain alongside land, maritime, air and space and, more significantly, that the UK was developing an offensive cyber capability.[11] This was the latest milestone in the UK's development of cyber capabilities which gained momentum in 2010 when the National Security Strategy identified cyber attacks as a tier one risk.[12] To mitigate the risk, the corresponding Strategic Defence and Security Review allocated £650 million of additional funding, over four years, to its National Cyber Security Programme[13] and committed to publishing an updated Cyber Security Strategy in 2011.[14] In parallel to its rapid climb up state policy agendas, an array of literature has been published on cyber. The divergence of opinion within the literature is vast with views on the potential effects of offensive cyber capabilities ranging from the "morally trivial to the absolutely devastating".[15] Despite the public rhetoric, state-based cyber capabilities remain shrouded in secrecy.[16] This lack of transparency combined with little experience and limited knowledge in the field is a major contributing factor to the variety of opinions.

Cyber, as a field with growing budgets in times of austerity, has attracted a lot of attention. There are many public and private organisations 'jumping on the bandwagon' to be involved in cyber-related activities to get their share of the capital being invested or to ensure they remain relevant. This has resulted in an explosion of cyber-related terms.[17] Accordingly, cyber issues are being treated from some quarters with "skepticism and disdain" as cyber terms are considered "jargon and hyped terminology".[18] On the other hand, some authors predict that cyber attacks have the

[9] Edward Barrett, "Warfare in a New Domain: The Ethics of Military Cyber-operations," *Journal of Military Ethics* 12, no. 1 (2013): 4.

[10] Tim Stevens, "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace," *Contemporary Security Policy* 33, no. 1 (2012): 148.

[11] UK. DCDC. *Cyber Primer*, iii.

[12] United Kingdom. Cabinet Office. *A Strong Britain in an Age of Uncertainty: The National Security Strategy.* (London: Cabinet Office, 2010), 27.

[13] United Kingdom. Cabinet Office. *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review.* (London: Cabinet Office, 2010), 47.

[14] Ibid., 49.

[15] Christopher Eberle, "Just War and Cyberwar," *Journal of Military Ethics* 12, no. 1 (2013): 57.

[16] Richard Clarke and Robert Knake, *Cyber War: The next threat to national security and what to do about it* (New York: Ecco, 2012), xi.

[17] To name but a few: cyber war, cyber attack, cyber crime, cyber espionage, cyber bullying, cyber security, cyber terrorism, cyber combatant and cyber weapon.

[18] Gregor Campbell, "Cybersecurity and Reality: What's in a Word?," Info Security, http://www.infosecurity-magazine.com (accessed April 1, 2014).

ability to cripple societies by affecting critical national infrastructure and services such as water, electricity and transport networks.[19] There are also claims that cyber capabilities provide a "revolutionary form of conflict".[20] In their book on Cyber War, Richard Clarke and Robert Knake paint a bleak picture of the devastation that cyber war could entail.[21] They caution that despite no state undertaking such a sophisticated attack to date, there are several advanced nations that have the requisite capability and that an attack could take place without a single solider setting foot in the country.[22] The warning is caveated that, as with nuclear weapons, there would need to be the correct political circumstances for these types of cyber capabilities to be employed.[23] Clarke and Knake conclude with six recommendations that should be undertaken to avoid the cyber disaster they portray.[24] Such publications have led to prominent figures making predictions on potentially devastating outcomes unless action is taken. For example, Leon Panetta, speaking when in office as the US Defence Secretary, cautioned that the US was "facing the possibility of a cyber-Pearl Harbor".[25]

There is currently no consensus on the importance of cyber capabilities or their consequences on the conduct of war. At one end of the spectrum cyber is viewed as a buzzword, "a technical word or phrase that has become fashionable".[26] It is considered to be hype with no substance and often misused by influential people.[27] At the opposite end of the spectrum, cyber capabilities have been described as being potentially able to yield catastrophic effects with no requirement for personnel to be put in harm's way when employed. It is such a ground-breaking capability that cyber could be considered an independent instrument of national power that can directly contribute to national strategic objectives. Instruments of national power are "all of the means available to the government in its pursuit of national objectives".[28] In the UK, the recognised instruments of national power are diplomatic, economic and military with all three underpinned by information.[29] Should cyber be considered the fourth instrument of national power? Or is cyber overhyped and the latest buzzword? The aim of this paper is to analyse the field of cyber to determine where cyber sits on the spectrum between the two extremes of buzzword and instrument of national power.

---

[19] Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst and Company, 2013), viii.

[20] Jean-Loup Samaan, "Cyber Command: The Rift in US Military Cyber-strategy," *RUSI Journal* 155, no. 6 (2010): 16.

[21] Clarke and Knake, *Cyber War*, 64-68.

[22] Ibid., 67.

[23] Ibid., 68.

[24] Ibid., 261.

[25] Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," The New York Times, http://www.nytimes.com (accessed March 31, 2014).

[26] Oxford Dictionary of English, 2nd ed.

[27] Rid, *Cyber War Will Not Take Place*, ix.

[28] United States. Department of Defense. *Dictionary of Military and Associated Terms.* Joint Publication 1-02. (Washington, Department of Defense, 2010), 130.

[29] United Kingdom. Development, Concepts and Doctrine Centre (DCDC). *British Defence Doctrine.* Joint Doctrine Publication 0-01. 4th ed. (Shrivenham: DCDC, 2011), 1-6.

As cyber is a popular, contemporary topic with a wealth of published information, the research methodology used in this paper is qualitative and studies a broad range of material drawn from publically available sources including books; journal articles; papers; dissertations; governmental and military publications; and Internet articles and publications. The sources range from publications from when the field of cyber first emerged into open discourse to the most recent, and also include publications from other relevant fields, such as air power. This approach has been selected as cyber is a relatively new field of study where theories are evolving rapidly and normative understandings and definitions are yet to form. By examining a broad range of sources, it is intended to minimise the impact of any transitory theories in the analysis and to enable comparative analysis with conventional domains where possible. Academic publications form the predominant research evidence; however, due to the field's fast-paced nature, Internet sources have been used as an element of the research base.

The paper's argument is presented in five sections. First, the key cyber terms will be defined and the concept of cyber power will be explored. The characteristics of cyberspace will be analysed, including comparisons with the conventional military domains, and the pertinent legal and ethical issues will be highlighted. It will argue that there is benefit in considering cyberspace as an independent domain. Second, cyber capabilities will be examined. This will include the use of cyber for enabling operations and information operations, as well as the concepts of cyber deterrence and arms control. Reported examples of cyber activity will be used to provide context to the theories debated in the academic literature. State dependency on cyberspace and the strategies developed in response will also be investigated. Third, the notion that cyber is a buzzword will be analysed. It will argue that cyber is not just a buzzword as cyberspace is fundamental to civilian life and, in the military sphere, the opportunities and threats posed cannot be disregarded due to their potential impacts. Fourth, the concept of cyber as an instrument of national power will be tested. It will argue that cyber should not be considered an additional instrument of national power. Instead, cyber should be considered a tool that can support the existing instruments of national power directly though provision of enabling effects or as part of the wider information campaign. Finally, the paper will conclude that cyber is neither a buzzword nor an instrument of national power. It is a vital capability that underpins both civilian life and military effectiveness and, thus, cannot be ignored. Cyber provides an enabling function, similar to how information is considered, to the diplomatic, economic and military instruments of national power. It also provides a means for conducting information operations. It does not, however, change the nature of war such that wars can be fought purely in cyberspace. Hence, it is unable to independently deliver national strategic objectives.

CYBER POWER AND CYBERSPACE

Power is a frequently used term in international relations, yet it is commonly done so without providing a definition for what it means for a state to have power. On the contrary, cyber is littered with definitions of its facets but frustratingly there is a wide divergence between the many definitions. In order to assess the utility of cyber and whether or not it is an instrument of national power, it is first necessary to provide clear definitions of the key terms and concepts relating to power and cyber. The cyberspace domain will also be analysed to determine its characteristics and it will be argued that there is value in considering cyberspace as the fifth military domain alongside the conventional domains of land, maritime, air and space.

Cyber Power

Power is "the capacity or ability to direct or influence the behaviour of others or the course of events".[30] State power is, therefore, the ability of one state to compel or influence another state to do something that it would not otherwise do.[31] The diplomatic, economic and military instruments are considered to be instruments of national power as they have the ability to deliver effects to influence or compel state and non-state actors in order to meet strategic objectives. Thus, it would be logical for a state with a strong economy and military to be considered powerful and able to influence the behaviour of less powerful actors. Power, nevertheless, is not necessarily tangible or measurable.[32] Kenneth Waltz argued that a powerful state needed to score well in the following areas: "size of population and territory, resource endowment, economic capability, military strength, political stability and competence".[33] Joseph Nye recognises that resources are an important factor but highlights a paradox when resources are considered synonymous with power: those with the greatest resources do not always achieve the outcomes they desire.[34] Power also has hard and soft elements. "Hard power is the ability to get others to do what they otherwise would not do through threats or rewards."[35] Whereas, soft power "is the ability to affect others through the co-optive means of framing the agenda, persuading, and eliciting positive attraction in order to obtain preferable outcomes".[36] Put bluntly, hard power is considered 'push' and soft power 'pull'.[37]

---

[30] Oxford Dictionary of English, 2nd ed.

[31] Baylis, Smith and Owens, *Globalization of World Politics*, 157.

[32] Joseph Nye, *The Future of Power* (New York: PublicAffairs, 2011), 82.

[33] Kenneth Waltz, *Theory of International Politics* (Boston, MA: McGraw-Hill, 1979), 131.

[34] Nye, *Future of Power*, 8.

[35] Robert Keohane and Joseph Nye, "Power and Interdependence in the Information Age," *Foreign Affairs* 77, no. 5 (1998): 86.

[36] Nye, *Future of Power*, 21.

[37] Ibid., 20.

Power is employed by a state through its instruments of national power. The diplomatic instrument is used to deliver policy objectives; it relies upon persuasion and influence, reinforced by the threat of coercive power.[38] The economic instrument is empowered by international flows of capital and trade and is realised through "a range of incentives, boycotts, tariffs and sanctions".[39] The military instrument applies power over a range of effects "from coercion through to the deliberate application of force to neutralise a specific threat"[40] and information enables the coherent and effective application of the three instruments.[41] Notably, all of the instruments can be used to deliver soft or hard power effects.

Having established what state power is and how it is applied through the national instruments, it is now worth considering cyber power. A range of cyber power definitions have been articulated in academic publications. Nye defined it in both resource and behavioural terms. In resource terms, it is "a set of resources that relate to the creation, control, and communication of electronic and computer-based information – infrastructure, networks, software, human skills".[42] "Defined behaviourally, cyberpower is the ability to obtain preferred outcomes through the use of the electronically interconnected information resources of the cyberdomain."[43] An alternative definition is one by Daniel Kuehl which defines cyber power as, "the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power".[44] Kuehl's definition is regularly quoted in literature. Indeed, the UK's doctrinal definition, which has not been revised since 2011 despite the recent publication of an updated joint doctrine note[45] and cyber primer,[46] is almost identical.[47]

From the definitions of cyber power two observations can be drawn. The first is that it can be used to enable or support the use of the instruments of national power; effectively an indirect application of power. For the military instrument, cyber power can enable or support operations in the conventional domains. Importantly, cyber power can only be used to apply force indirectly.[48] The second observation is that cyber can be used to influence actors or events directly though the manipulation of information. Before clarifying this paper's definition of cyber power, it is worth

[38] UK. DCDC. *British Defence Doctrine*, 1-6.

[39] Ibid., 1-7.

[40] Ibid.

[41] Ibid., 1-9.

[42] Nye, *Future of Power*, 123.

[43] Ibid.

[44] Daniel Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, eds Franklin Kramer, Stuart Starr and Larry Wentz (Washington, DC: Potomac Books, 2009), 38.

[45] United Kingdom. Development, Concepts and Doctrine Centre (DCDC). *Cyber Operations: The Defence Contribution.* Joint Doctrine Note 3/13. (Shrivenham: DCDC, 2013).

[46] UK. DCDC. *Cyber Primer*.

[47] UK. DCDC. *Cyber Operations*, Lexicon-4.

[48] Shaun Harvey, "Determining the Utility of Cyber Power" (Dissertation, University of Reading, 2012), 57.

reviewing the definitions for air and space power. Air power is defined as "using air capabilities to influence the behaviour of actors and the course of events".[49] Similarly, the definition of space power is "exerting influence in, from, or through space".[50] The simplicity of these definitions is appealing and both are coherent with the definition of state power. A corresponding definition for cyber power could be: using cyber capabilities to influence the behaviour of actors and the course of events in, from or through cyberspace. This, however, does not sufficiently capture cyber power's enabling effects. Hence, a combination of this definition and Kuehl's has been used for the purposes of this paper: using cyber capabilities to create advantages, influence the behaviour of actors and the course of events in, from or through cyberspace. Nye has argued that the arrival of cyber capabilities has caused the diffusion of power from state to non-state actors.[51] The cyberspace domain will now be examined to determine why this is the case.

Cyberspace

The term cyberspace originates from the 1984 novel *Neuromancer* by William Gibson where it was used to describe "a consensual hallucination".[52] Following the novel's publication, the term was adopted by computer scientists before becoming part of mainstream vocabulary with the rise of the Internet in the 1990s. There are now many definitions offered in the literature for cyberspace. Following a detailed examination of the varied definitions, Kuehl proposed the following:

> Cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies.[53]

This definition is significantly different to Gibson's original and the dictionary definition used in the introduction where cyberspace is described as a "notional environment".[54] The UK doctrinal definition, which will be used for the purposes of this paper, is as follows:

> In Defence, cyberspace is the interdependent network of information technology infrastructures, (including the Internet, telecommunications networks, computer systems, as well as embedded processors and controllers), and the data therein within the information environment.[55]

---

[49] United Kingdom. Development, Concepts and Doctrine Centre (DCDC). *UK Air and Space Doctrine.* Joint Doctrine Publication 0-30. (Shrivenham: DCDC, 2013), 1-1.

[50] Ibid., 5-2.

[51] Nye, *Future of Power*, 101.

[52] Kuehl, "From Cyberspace to Cyberpower," 24.

[53] Ibid., 28.

[54] Oxford Dictionary of English, 2nd ed.

[55] UK. DCDC. *Cyber Primer*, 1-1.

Both definitions are broadly similar. The key deduction is that cyberspace is not limited to the Internet or the computers that humans use directly. It includes all computer networks, whether connected to the Internet or part of a discrete network, and computers that support processes or the provision of services. Therefore, cyberspace's scope is massive and is certainly not notional. The one significant difference between both definitions is that Kuehl's includes the electromagnetic spectrum. It is not included in the doctrinal definition as the electromagnetic spectrum is considered to be part of the wider information environment rather than cyberspace.

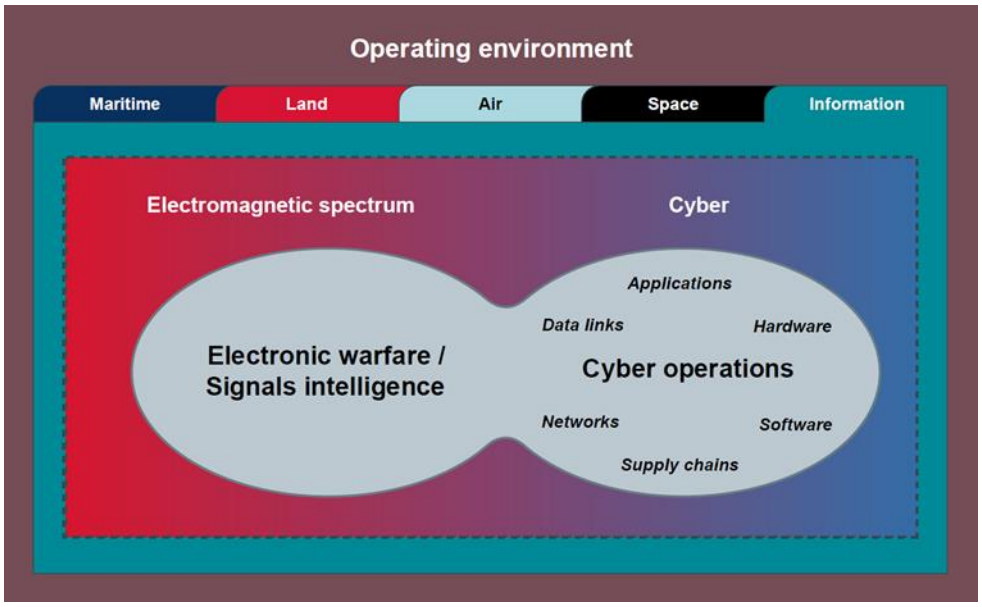

Figure 1 - Cyber operations in context of the operating environment.[56]

The information environment, as depicted in Figure 1, comprises both cyberspace and the electromagnetic spectrum. The electromagnetic spectrum is used for electronic warfare and signals intelligence while cyber operations are conducted within cyberspace. If the meanings are taken literally, it would complicate matters as cyber operations use the electromagnetic spectrum to process and communicate information. Likewise, the data and computer systems used in electronic warfare are considered part of cyberspace. They have been separated conceptually by operational effect delivered and both combine to form the information environment. The information environment is considered part of the wider operating environment which also comprises the conventional domains.[57] This model, however, does not reflect cyberspace's enabling function. Figure 2 is a conceptual model that illustrates both cyberspace and the electromagnetic spectrum intersecting the physical domains. It highlights the conventional

[56] Ibid., 1-22.
[57] Ibid., 1-21.

domains' reliance on cyberspace and the fact that cyber and conventional operations are dependent on the electromagnetic spectrum.[58]

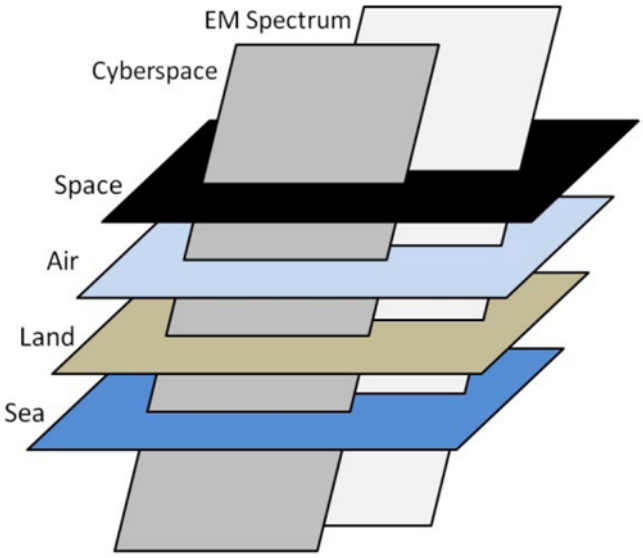

Figure 2 – Conceptual model illustrating the dependency of the physical domains on cyberspace.[59]

Cyberspace, rather than the information environment, is considered to be the fifth military domain. A domain is "a specified sphere of activity or knowledge" [60] and a military domain has several key features: operations can take place within and through it; it has physical attributes; and it has distinctive means and effects.[61] In the UK, each domain has its own doctrine where the distinctive characteristics, roles and operations are defined. Formal UK doctrine for the cyberspace domain has yet to be published. Nonetheless, there have been a number of joint doctrine notes and primers to engender cyber thinking. Within these documents, cyber operations and the characteristics and roles of the domain are described.

Cyber operations are "the employment of capabilities where the primary purpose is to achieve effects in, or through, cyberspace".[62] Offensive operations are "projecting power by applying force in, or through, cyberspace", and defensive operations are "passive and active measures to preserve the ability to use friendly cyber capabilities and protect data networks, net-centric

[58] Gregory Conti, John Nelson and David Raymond, "Towards a Cyber Common Operating Picture," in *2013 5th International Conference on Cyber Conflict,* eds K. Podins, J. Stinissen and M. Maybaum (Tallinn: NATO CCD COE Publications, 2013), 284.

[59] Ibid.

[60] Oxford Dictionary of English, 2nd ed.

[61] Stuart Starr, "Toward a Preliminary Theory of Cyberpower," in *Cyberpower and National Security*, eds Franklin Kramer, Stuart Starr and Larry Wentz (Washington, DC: Potomac Books, 2009), 48.

[62] UK. DCDC. *Cyber Primer*, 1-1.

capabilities and other designated systems".[63] The latest cyber joint doctrine note outlines four cyber roles: control of cyberspace, intelligence and situational awareness, information activity and offensive activity.[64] The four roles are supported by information assurance and data management.[65] These mirror the roles of air power[66] which may be a result of the tendency to compare the emergence of cyberspace with the development of air power in the twentieth century. From these definitions and roles, operations can take place within and through cyberspace and there are particular functions or effects that these operations can deliver, which meet two of the three criteria for a domain.

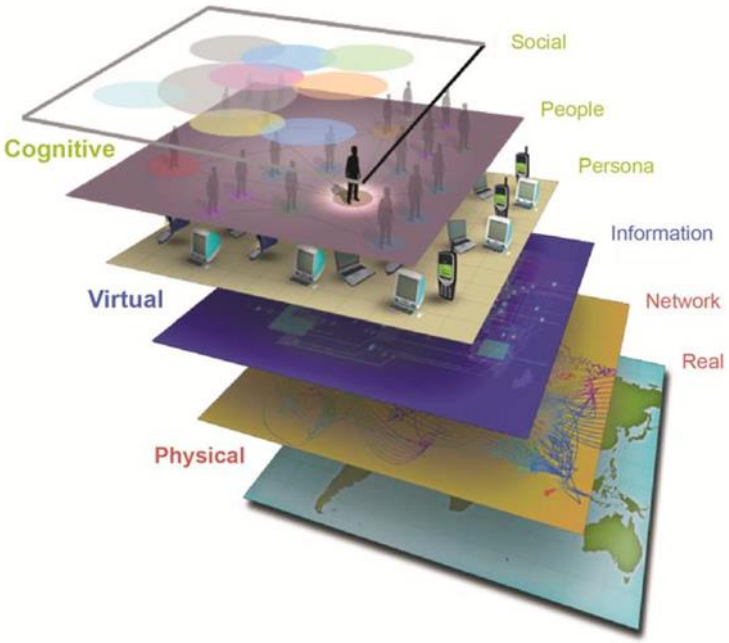

Figure 3 - The layers of cyberspace.[67]

Cyberspace comprises three layers, physical, virtual and cognitive.[68] A visual interpretation is at Figure 3. The physical layer consists of the actual physical components that exist to form cyberspace. The connections between the physical components and the software used to create, manipulate, store and transfer the information over these connections form the virtual layer. The information contained within cyberspace that is manipulated by people and the interaction of

[63] UK. DCDC. *Cyber Operations*, 1-2.
[64] Ibid., 2-1 – 2-2.
[65] Ibid., 2-3.
[66] Control of the air; intelligence and situational awareness; attack; and air mobility. See UK. DCDC. *UK Air and Space Doctrine*, 3-1.
[67] UK. DCDC. *Cyber Primer*, 1-26.
[68] Ibid.

people through cyberspace is the cognitive layer.[69] Notably, the concept of cyberspace is predominantly virtual but it clearly requires physical aspects for it to exist.

The physical domains are both defined and constrained by the established laws of physics and each domain has markedly different characteristics that technology is required to exploit whether aircraft, submarines, tanks or satellites.[70] Conversely, cyberspace is a human-made entity that is continuously changing due to technological developments.[71] Although cyber capabilities exist in the physical world and are subject to the laws of physics, the way it operates is subject to human intervention.[72] For example, the ongoing transition from Internet protocol version four to six is altering cyberspace's fundamental terrain.[73] Hence, cyberspace's future parameters may be different from those of today.[74] This potentially creates an issue for the prosecution of cyber operations as it may not be possible to accurately predict effects or outcomes. Moreover, the interdependencies of cyberspace are difficult to identify, interpret and predict,[75] and the effect caused by a particular cyber weapon may change from one use to the next.[76] In addition, cyber effects are difficult to repeat as once an attack has been detected, the victim is likely to determine how its system was breached and take action to close the vulnerability.[77] This is in contrast to the physical domains, such as the dropping of a bomb from an aircraft, where the first order effects can be readily predicted using established laws of physics and repeated on multiple occasions.

The equipment required to exploit the physical domains for military purposes present a fiscal and technological barrier to entry for states and non-state actors. For instance, there are a limited number of states that possess the wherewithal and technological industrial base to build submarines. In contrast, the tools needed to operate in cyberspace are more freely accessible. As a result, there is a vast range of potential actors which includes states, non-state actors and individuals.[78] This low barrier to entry also means cyber capabilities are ubiquitous as "any computer is a potential cyberweapon and anyone with advanced knowledge of information systems

[69] Ibid.

[70] Kuehl, "From Cyberspace to Cyberpower," 25.

[71] Nye, *Future of Power*, 124.

[72] Franklin Kramer, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework," in *Cyberpower and National Security*, eds by Franklin Kramer, Stuart Starr and Larry Wentz (Washington, DC: Potomac Books, 2009), 5.

[73] For more detail see World Telecommunication/ICT Policy Forum, "IPv4 and IPv6 issues," International Telecommunication Union, https://www.itu.int (accessed April 6, 2014).

[74] Kramer, "Cyberpower and National Security," 5.

[75] Terrence Kelly and Jeffrey Hunker, "Cyber Policy: Institutional Struggle in a Transformed World," *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (2012): 215.

[76] Barrett, "Warfare in a New Domain," 10.

[77] Martin Libicki, "Cyberspace Is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (2012): 331.

[78] Randall Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics* 9, no. 4 (2010): 401.

is a potential cybercombatant".[79] This ubiquitous aspect, combined with the numerous actors and an ability to mask identities, creates the attribution characteristic of cyberspace. In the physical domains, it is normally relatively straightforward to attribute an act to an agent.[80] In cyberspace, it is possible for actors to hide their identity and location through various means.[81] Consequently, it is not always possible for victims of a cyber attack to identify their attacker beyond reasonable doubt.

Cyberspace is also frequently classed as a global commons and likened to the high seas and space.[82] This is due to the Internet being an anarchic domain, as there is no global governing organisation, and it being designed for ease of access.[83] As a consequence of its open design, there are no intellectual property constraints or licensing requirements for technology or services using the Internet.[84] Despite its lack of central governance, the Internet is not free from regulation as standards need to be maintained and observed. The level of regulation, however, is minimal compared to that of the traditional telecommunications sector.[85] Furthermore, the open standards were designed without security as a driving consideration. Accordingly, the standards are being used in both scale and ways not anticipated by the designers; they were not intended to support the vast amounts of sensitive data and economic and social activities that they currently do.[86] The reference to cyberspace as a global commons fails to recognise that the majority of cyberspace infrastructure is privately owned.[87] The physical infrastructure is also located within sovereign territory. Thus, cyberspace should not be considered a global commons in the same sense as the high seas as there are significant elements within sovereign or private control.[88] Crucially, as military and civilian networks utilise common underlying physical infrastructure, cyber operations have the potential to affect combatants and non-combatants.[89]

As identified, cyberspace has distinguishing physical and virtual attributes which meet the final criteria for a military domain. Therefore, cyberspace is regarded as the fifth domain by many nations. Martin Libicki questions the utility of conceptualising cyberspace as a separate domain.

---

[79] Ibid., 385.

[80] Eberle, "Just War and Cyberwar," 56.

[81] Barrett, "Warfare in a New Domain," 8.

[82] Gregory Rattray, "An Environmental Approach to Understanding Cyberpower," in *Cyberpower and National Security*, eds Franklin Kramer, Stuart Starr and Larry Wentz (Washington, DC: Potomac Books, 2009), 254.

[83] Timothy Neal-Hopes, "Preventing a Cyber Dresden: How the Evolution of Air Power can Guide the Evolution of Cyber Power" (Biblioscholar Dissertation, School of Advanced Air and Space Studies, 2011), 12.

[84] Marjory Blumenthal and David Clark, "The Future of the Internet and Cyberpower," in *Cyberpower and National Security*, eds Franklin Kramer, Stuart Starr and Larry Wentz (Washington, DC: Potomac Books, 2009), 233.

[85] Ibid., 236.

[86] Edward Skoudis, "Information Security Issues in Cyberspace," in *Cyberpower and National Security*, eds Franklin Kramer, Stuart Starr and Larry Wentz (Washington, DC: Potomac Books, 2009), 204.

[87] John Arquilla, "Twenty Years of Cyberwar," *Journal of Military Ethics* 12, no. 1 (2013): 84.

[88] Nye, *Future of Power*, 143.

[89] Joelien Pretorius, "Ethics and international security in the information age," *Defence & Security Analysis* 19, no. 2 (2003): 169.

He agrees that cyberspace is fundamental to the prosecution of operations in the physical domains, but argues that defining it as an equivalent leads to presumptions and overly constrains intellectual discussion and theories. He reasons that as cyberspace is so different, there is no point in defining it as a domain.[90] His main contention is based on the malleable nature of cyberspace that allows its features to be transformed rather than its artificiality.[91] Libicki raises some pertinent points. It is, however, assessed that there is utility in defining cyberspace as the fifth military domain due to its interdependence with the physical domains and its ability to influence the behaviour of actors and the course of events. Libicki's argument should be regarded and care taken not to constrain understanding of the opportunities and vulnerabilities presented. The similarity of the roles of air power and cyber is perhaps evidence of such constrained thinking.

Cyberspace's distinctive characteristics have created a number of ethical and legal issues. Questions have been raised relating to the just use of cyber power. For example, would it ever be right to respond to a cyber attack using conventional force? [92] There is a corresponding ethical debate[93] on whether or not the Just War Tradition provides a suitable moral framework in support of cyber operations. One view is that the Tradition does not provide adequate support and additional principles are required. The contrary perspective is that cyberspace fits into the Tradition's existing moral framework as it does not raise any fundamentally new ethical issues.[94]

From the legal perspective, there is a similar debate surrounding cyberspace and international law.[95] The UN Charter does not formally define the use of force or armed attack.[96] Cyber power further complicates this issue and there is no official agreement that defines the use of cyber force.[97] For the purposes of this paper, the use of force is considered to be the use of the military instrument whether in a conventional domain or cyberspace. Another aspect is one comparable to access, basing and overflight issues. If an offensive cyber operation utilises a third-party state's infrastructure, should permission be sought prior to the operation? [98] As there is presently no consensus on the majority of these aspects, there have been calls for international treaties to regulate the use of cyberspace. While the debates endure, nations, such as the UK, continue to

[90] Libicki, "Cyberspace Is Not a Warfighting Domain," 322.

[91] Ibid., 324.

[92] Dipert, "Ethics of Cyberwarfare," 392.

[93] For detail see Randall Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics* 9, no. 4 (2010): 384-410 and James Cook, "'Cyberation' and Just War doctrine: A Response to Randall Dipert," *Journal of Military Ethics* 9, no. 4 (2010): 411-423.

[94] George Lucas, "Postmodern War," *Journal of Military Ethics* 9, no. 4 (2010): 295.

[95] For detail see C. Czosseck, R. Ottis and K. Ziolkowski, *2012 4th International Conference on Cyber Conflict* (Tallinn: NATO CCD COE Publications, 2012).

[96] Herbert Lin, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law & Policy* 4, no. 63 (2010): 71.

[97] James Farwell and Rafal Rohozinski, "The New Reality of Cyber War," *Survival* 54, no. 4 (2012): 111.

[98] Jeffrey Caton, "Beyond Domains, Beyond Commons: Context and Theory of Conflict in Cyberspace," in *2012 4th International Conference on Cyber Conflict*, eds C. Czosseck, R. Ottis and K. Ziolkowski (Tallinn: NATO CCD COE Publications, 2012), 162.

use existing domestic and international law, particularly the Law of Armed Conflict, to govern their activities in cyberspace.[99]

The principal terms and concepts relating to power and cyber have been defined. Cyberspace has been analysed and it is assessed that there is utility in considering it as the fifth military domain. Cyberspace's distinguishing characteristics are summarised as follows: cyberspace is both continuously evolving and pliable, which leads to a potential inability to accurately predict cyber effects and weapons that can only be used once; cyber capabilities are ubiquitous due to the low barrier to entry; the attribution of attacks within cyberspace is difficult; cyberspace is designed to be open but is not a global commons in the same sense as space and the high seas; and military and civilian organisations use the same cyberspace, which may lead to an inability to discriminate between combatants and non-combatants. The ubiquity of cyber capabilities means a variety of actors have the ability to exploit cyber power which has resulted in states' power being diffused as non-state actors become more powerful.[100]

[99] UK. DCDC. *Cyber Primer*, 1-23.
[100] Nye, *Future of Power*, 132.

CYBER CAPABILITIES

Cyber has evolved significantly since John Arquilla and David Ronfeldt proclaimed in their seminal article that "Cyberwar is coming!"[101] Cyber capabilities will now be examined. This will start with the development of cyberspace and the corresponding state dependency, including a brief look at the cyber strategies adopted by the US, UK, Russia and China. Next, cyber capabilities will be analysed by detailing the theoretical activities that can be undertaken in cyberspace, how these can be used for enabling conventional operations and conducting information operations, and the concepts of cyber deterrence and arms control. The analysis will finish with key examples of reported cyber activity in open sources to provide context to the theory.

State Dependency

Cyberspace is not limited to the Internet; however, the Internet or its technical standards and protocols make up the majority of cyberspace in one form or other. The genesis of the Internet was the Advanced Research Projects Agency Network experiment where the concept and standards for a global network were developed. The protocols established were based on fundamental principles that make the Internet the open architecture it is today with no central global control. This technology matured to be the international standard for computer networks and is now universal in cyberspace.[102] The development of cyber capabilities, driven by the Internet, made it easier to communicate and, more significantly, generated massive commercial interest due to the revenue opportunities it presented. On one hand, commercial enterprises could become more efficient by exploiting the Internet and on the other, there were potential new revenue streams through the provision of Internet-based services.[103]

The proliferation of Internet-derived technologies has made them cheap and has resulted in their use for general purpose requirements. Internet-based equipment is used on discrete networks and industrial processes where there is no intention to connect them to the Internet. Hence, the technology is in use throughout cyberspace.[104] Bespoke, expensive hardware and software would be required for any information system or process that did not want to rely on Internet-derived technology. Consequently, the majority of commercial and governmental information systems are either connected to the Internet or utilise technology that is based on Internet standards.

---

[101] John Arquilla and David Ronfeldt, "Cyberwar is coming!," *Comparative Strategy* 12, no. 2 (1993): 141.

[102] Internet Society, "Brief History of the Internet," Internet Society, http://www.internetsociety.org (accessed April 7, 2014).

[103] Rattray, "An Environmental Approach to Understanding Cyberpower," 263.

[104] Blumenthal and Clark, "Future of Internet and Cyberpower," 210.

Likewise, armed forces have exploited cyber technologies to improve their effectiveness in the physical domains. Prior to the use of today's cyber terms, the US and UK approaches were known as network-centric warfare and networked enabled capability, respectively. The aim of network enabled capability was to improve "operational effectiveness in the future strategic environment by permitting the more efficient sharing and exploitation of information".[105] The idea was to maintain the technological advantage enjoyed by the US and UK armed forces. This asymmetrical advantage also created a reciprocal weakness, through the consequential dependencies on cyberspace that adversaries could take advantage of.[106]

The acceptance and exploitation of cyberspace by governments, militaries and commercial companies have driven economic growth, military capabilities and societal development. This has fostered trade and links that transcend state boundaries.[107] The financial markets, the heart of the international economy, are reliant on cyberspace which can have major repercussions. In 2007, computer glitches exacerbated an issue in the stock markets which led to the largest drop in the Dow Jones since 9/11.[108] As a result of the increased prevalence of cyber capabilities, many parts of states' critical national infrastructure rely on complex, interdependent cyber systems.[109] This means critical state infrastructure is dependent on the open environment that was designed for the Internet, which makes them susceptible to cyber attacks whether connected directly to the Internet or not; the potential attack vectors are reduced by not being connected to the Internet but are not removed altogether. These aspects highlight the possible impact to a state's economy or security from a cyber fault or attack. As a consequence of the new threat vectors created by cyberspace vulnerabilities, issues that were once the responsibility of engineers and technicians have become matters of public policy. Furthermore, these interdependencies reduce a government's ability to control its economy and erode state sovereignty.[110]

States have recognised the huge benefits that cyberspace can deliver through efficient provision of public services to economic growth. The potential threats to national security have also been publically documented. Writing in 2012, President Obama acknowledged that "the cyber threat to our nation is one of the most serious economic and national security challenges we face".[111]

---

[105] United Kingdom. Capability Manager (Information Superiority). *Network Enabled Capability: An Introduction*. (Version 1.1, 2004), 3.

[106] Ibid., 8.

[107] Harold Kwalwasser, "Internet Governance," In *Cyberpower and National Security*, eds Franklin Kramer, Stuart Starr and Larry Wentz (Washington, DC: Potomac Books, 2009), 492.

[108] John McCarthy, Chris Burrow, Maeve Dion and Olivia Pacheco, "Cyberpower and Critical Infrastructure Protection: A Critical Assessment of Federal Efforts," in *Cyberpower and National Security*, eds Franklin Kramer, Stuart Starr and Larry Wentz (Washington, DC: Potomac Books, 2009), 547.

[109] Ibid., 543.

[110] Kwalwasser, "Internet Governance," 492.

[111] Barack Obama, "Taking the Cyberattack Threat Seriously," The Wall Street Journal, http://online.wsj.com (accessed March 10, 2014).

Consequently, a significant number of states have created and published dedicated cyber security strategies. The US strategy was updated in 2011 with the identified goal:

> The United States will work internationally to promote an open, interoperable, secure and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation.[112]

To achieve the goal the strategy set three objectives: a diplomatic objective to build international consensus that recognises the intrinsic value of cyberspace;[113] a defence objective to encourage responsible behaviour and oppose those undertaking malicious activity, including the right to defend national assets;[114] and a development objective which seeks to improve cyber security through capacity building of states facilitated by bilateral and multilateral organisations.[115] The UK's latest cyber security strategy was also released in 2011 with the vision to "derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions … enhance prosperity, national security and a strong society".[116] The vision is underpinned by four objectives: to tackle cyber crime to provide a secure place to conduct business; improve the UK's resilience to cyber attacks; work internationally to shape the development of cyberspace so that it remains open and stable; and develop a skills and capability base in cyber security.[117] The two strategies have a similar focus on the need for a secure cyberspace to provide economic and social development.

In contrast, Russia published a cyber security strategy in 2013 with the horizon set at 2020.[118] The Russian aim is to "promote the establishment of the international legal regime aimed at creating conditions for the establishment of the system of international information security".[119] The aim is supported by similar objectives to those of the US and UK, focussing on international cooperation through bilateral and multilateral agreements.[120] On the face of it, Russian strategy would appear similar, except for one significant difference. The US and UK promote free speech and open

[112] United States. The White House. *International Strategy for Cyberspace.* (Washington, The White House, 2011), 8.
[113] Ibid., 11.
[114] Ibid., 12.
[115] Ibid., 14.
[116] UK. Cabinet Office. *UK Cyber Security Strategy*, 8.
[117] Ibid.
[118] NATO CCD COE, "National Strategies and Policies," NATO CCD COE, http://ccdcoe.org (accessed March 31, 2014).
[119] Russia. Russian Federation. *Basic principles for State Policy of the Russian Federation in the field of International Information Security to 2020.* (Russian Federation, unofficial translation, 2013), 3.
[120] Ibid., 3-4.

access; whereas, Russia has been accused of managing the flow of information to its citizens[121] and conducting offensive cyber activities against other states.[122]

China is also subject to similar accusations. Unlike Russia, it has not formally published a national cyber security strategy.[123] China's cyber capabilities and intentions have recently come to the fore with reports of it undertaking intrusive acts against a number of foreign states. It has been assessed that cyber activities have become routine for China, with cyber power employed as part of a pre-emptive strategy.[124] Despite Russia and China being more restrictive with the access to information services they deliver to their citizens, they also recognise that cyberspace provides both opportunities and threats. The US, UK, Russia and China have all developed cyber strategies and capabilities to maximise the benefits derived from cyberspace and minimise the threats.

Theoretical Cyber Activities

A considerable volume of literature has been produced on cyber capabilities and the range of opinions within the literature is enormous. Michael Hayden, former director of the Central Intelligence Agency, observed that, "rarely has something been so important and so talked about with less clarity and less apparent understanding than this phenomenon".[125] There have been a significant number of academic books and articles published since the thought-provoking contribution by Arquilla and Ronfeldt proclaiming that cyber war would be "to the twenty first century what blitzkrieg was to the twentieth century".[126] From a similar view point, Clarke views cyber war as a completely new form of combat that is yet to be fully understood.[127] In his book with Knake, the term cyber war refers "to actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption".[128] Thomas Rid questioned the use of the term cyber war. In his opinion, an act of war must "have the potential to be lethal; it has to be instrumental; and it has to be political".[129] Rid contended that a cyber war had not taken place and was unlikely to do so in the future as a cyber act had yet to meet these criteria and probably never would. Instead, Rid classified cyber activity as "sophisticated versions of … subversion, espionage and sabotage".[130] Similarly to the use of cyber force, there is no

[121] Timothy Thomas, "Nation-state Cyber Strategies: Examples from China and Russia," in *Cyberpower and National Security*, eds Franklin Kramer, Stuart Starr and Larry Wentz (Washington, DC: Potomac Books, 2009), 465.
[122] Ibid., 475.
[123] NATO CCD COE, "National Strategies and Policies," NATO CCD COE, http://ccdcoe.org (accessed March 31, 2014).
[124] Thomas, "Nation-state Cyber Strategies," 466.
[125] Michael Hayden, "The Future of Things 'Cyber'," *Strategic Studies Quarterly* 5, no. 1 (2011): 3.
[126] Arquilla and Ronfeldt. "Cyberwar is coming!," 147.
[127] Richard Clarke, "War from Cyberspace," *The National Interest* 104 (November/December 2009): 32.
[128] Clarke and Knake, *Cyber War*, 6.
[129] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 6.
[130] Ibid.

general agreement on the definition of a cyber attack.[131] There is, however, a broad consensus that cyber acts can be divided into the following categories: crime, espionage, terrorism and offensive actions.[132]

Criminal cyber activity includes illegal acts undertaken for political, social or financial gain. The majority of malevolent cyber activity is financially driven[133] and the estimated cost to the UK is £27 billion per annum.[134] A large proportion of cyber criminals exploit standardised resources and a substantial number of criminal attacks fail. Nevertheless, the quantity of attacks is sufficient for them to be profitable.[135] Organised criminals are improving their capabilities with headlines regularly reporting the worst ever theft of personal information or similar.[136] 'Hacktivism' is a criminal activity undertaken for political or social gain. 'Hacktivists' normally use tools that are freely available to conduct acts that disrupt services or websites to make their statement.[137] These activities can have far reaching ramifications and one of the most high-profile examples was the leaking of US classified information to WikiLeaks.[138]

The pervasiveness of criminal activity provides good cover for actors who wish to undertake cyber espionage.[139] Cyberspace is being exploited by actors to collect intelligence for military and industrial purposes.[140] It is widely reported that cyber espionage is being undertaken by most states and, like its conventional variants, is unlikely to be subject to international treaties that restrain it.[141] The loss of intellectual property on the scale that cyber tools can enable could have a considerable impact on a company's competitiveness or a state's economy.[142] Furthermore, a sustained campaign to obtain intellectual property by a smaller nation may be sufficient to undermine a stronger state, which is metaphorically expressed as "death by a thousand cuts".[143] In these types of situation, at what point could a state consider that the theft of its information had crossed a line such that it should take preventive or pre-emptive action in self-defence? There is no definitive answer to this question at present due to the lack of a formal definition of the use of cyber force in international law. The situation is also further clouded by the attribution

[131] Stephanie Meulenbelt, "The 'Worm' as a Weapon of Mass Destruction," *RUSI Journal* 157, no. 2 (2012): 65.
[132] Nye, *Future of Power*, 144.
[133] Jon Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013): 370.
[134] Clement Guitton, "Cyber insecurity as a national threat: overreaction from Germany, France and the UK?," *European Security* 22, no. 1 (2013): 30.
[135] Lindsay, "Stuxnet," 396.
[136] Kelly and Hunker, "Cyber Policy," 213.
[137] Lindsay, "Stuxnet," 371.
[138] Kelly and Hunker, "Cyber Policy," 211.
[139] James Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival* 53, no. 1 (2011): 26.
[140] Pauline Neville-Jones and Mark Phillips, "Where Next for UK Cyber-Security?," *RUSI Journal* 157, no. 6 (2012): 32.
[141] Paul Meyer, "Diplomatic Alternatives to Cyber-Warfare," *RUSI Journal* 157, no. 1 (2012): 16.
[142] Neville-Jones and Phillips, "Where Next for UK Cyber-Security?," 38.
[143] Lindsay, "Stuxnet," 370.

characteristic and the fact that the tools used for espionage activities are analogous to those required for attacks.

Terrorist actions are undertaken to create destruction to compel or intimidate governments in the pursuit of particular aims.[144] The threat from cyber terrorism is frequently described as a major risk with images portrayed of large-scale losses of life and massive critical infrastructure failures.[145] Complex cyber attacks would be needed to cause the required level of destruction; importantly, the probability of this being achieved is very low with no such terrorist attacks being reported to date.[146] As a result, some commentators believe that the "hype surrounding this issue outpaces the magnitude of the risk".[147] Moreover, terrorist groups are predominantly using cyberspace as a tool to facilitate their activities rather than a means of attack.[148] This has enabled terrorist organisations to be transnational but, as with states, it has also created vulnerabilities that intelligence agencies can exploit.[149]

Offensive cyber activity is the most contentious. It covers all offensive acts whether described as an attack or warfare. Consequently, there are many varied definitions that relate to offensive cyber capabilities which differ from the UK doctrinal definition of offensive cyber operations. One definition of cyber attack is a "computer attack emanating from a state, on another state's computer network, with the purpose of disrupting, degrading or destroying information, thereby disabling the state to use or manage that information".[150] As would be expected, the purpose of offensive cyber activity is to impact an adversary's capability by disruption or destruction. Due to the secrecy that surrounds state capabilities, the potential uses and effectiveness of cyber attacks are mainly unknown. The most inflammatory claims are that cyber attacks can cause the equivalent destruction to kinetic attacks without the need for conventional forces.[151] Hence, the claims that cyber has changed the nature of war as it can become a substitute for conventional military force rather than a complementary or enabling function.[152] However, cyber war with such devastating effects is as unlikely as comparable kinetic attacks as it would require states with both the advanced capabilities and the political motivation.[153] The potency of these potential attacks is based on conjecture that the required cyber weapons exist. Most experts believe that cyber

[144] Irving Lachow, "Cyber Terrorism: Menace or Myth?," In *Cyberpower and National Security*, eds Franklin Kramer, Stuart Starr and Larry Wentz (Washington, DC: Potomac Books, 2009), 438.
[145] Ibid., 437.
[146] Guitton, "Cyber insecurity as a national threat," 25.
[147] Lachow, "Cyber Terrorism: Menace or Myth?," 437.
[148] Ibid.
[149] Ibid., 459.
[150] Meulenbelt, "'Worm' as Weapon," 62.
[151] Lindsay, "Stuxnet," 372.
[152] Ibid., 373.
[153] Myriam Cavelty, "The Militarisation of Cyberspace: Why Less May Be Better," in *2012 4th International Conference on Cyber Conflict,* eds C. Czosseck, R. Ottis and K. Ziolkowski (Tallinn: NATO CCD COE Publications, 2012), 150.

weapons will be used to provide complementary or enabling effects rather than devastating, war-winning capabilities in their own right.[154] A cyber weapon is "computer code that is used, or designed to be used, with the aim of threatening or causing physical damage, functional, or mental harm to structures, systems, or living beings".[155] Importantly, cyber weapons may provide a non-kinetic means to disrupt an adversary's operational capability.[156]

The terms cyber attack and cyber war are usually conflated with criminal and espionage activities which form the majority of activity in cyberspace.[157] Efforts to determine what should be considered a cyber attack or the use of force are hindered by poor understanding and use of cyber vocabulary. Terms are used interchangeably which undermines their utility as a conceptual tool.[158] It is argued that terms relating to offensive cyber operations, such as attack, should have their meaning restricted to those that are directly coercive or use force.[159] This, however, may not be straightforward due to the use of force being a contested notion. When considering cyber acts, it is the effects produced or harm caused that constitutes the use of force rather than the means.[160] For example, a cyber attack that causes no physical damage but affects the provision of critical national services through the manipulation of information systems should be considered a use of force due to its coercive and disruptive effects. Whereas, a cyber operation that captures intellectual property should not. That said, it is difficult to categorise the damage or harm caused by the loss of information or information services.[161] Consequently, Herbert Lin argues that the term cyber attack should refer to the methodology of the attack rather than the effect that is trying to be achieved.[162]

Clarke and Knake argue that cyber war is going to have a profound change to the way war is fought; in essence the nature of war is going to change.[163] Rid disagrees with this view, basing his argument on the definition of war.[164] Evidence to date is that there is a high frequency of criminal and espionage related activity compared to the extremely low frequency of high-intensity attacks depicted by Clarke and Knake.[165] Thus, cyber capabilities have presently changed the character of

[154] Nye, *Future of Power*, 135.

[155] Thomas Rid and Peter McBurney, "Cyber-Weapons," *RUSI Journal* 157, no. 1 (2012): 7.

[156] Farwell and Rohozinski, "New Reality of Cyber War," 115.

[157] David Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-power* (Abingdon: Routledge, 2011), 81.

[158] John Stone, "Cyber War Will Take Place!," *Journal of Strategic Studies* 36, no. 1 (2013): 101.

[159] Adam Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies* 35, no. 3 (2012): 405.

[160] Lin, "Offensive Cyber Operations," 73.

[161] Thomas Wingfield, "International Law and Information Operations," in *Cyberpower and National Security*, eds Franklin Kramer, Stuart Starr and Larry Wentz (Washington, DC: Potomac Books, 2009), 525.

[162] Lin, "Offensive Cyber Operations," 74.

[163] Clarke and Knake, *Cyber War*, 67.

[164] Rid, "Cyber War Will Not Take Place," 6.

[165] Lindsay, "Stuxnet," 374.

war rather than the nature.[166] Cyber capabilities are more likely to be used as a component of a larger military campaign. They are unlikely to be capable of independently achieving political outcomes by imposing intolerable costs.[167] There are many viewpoints on cyber capabilities and the lack of common vocabulary will prevent the formulation of norms. The use of the term cyber war detracts from what is actually happening: "continuing hostility among diverse state and non-state actors, conducted largely by non-military means".[168] The distinction between the types of activity is important as it determines the law that governs the act, whether domestic, such as criminal and espionage, or the Law of Armed Conflict for offensive operations.[169] Having examined the theoretical aspects, the potential use of cyber capabilities in information and enabling operations and the concepts of cyber deterrence and arms control will now be analysed.

Information and Enabling Operations, Deterrence and Arms Control

In British doctrine, information is used to enable the effective and efficient application of the instruments of national power. A strategic narrative is used as part of an information strategy or campaign to control the use of information and synchronise the application of the instruments to meet strategic objectives.[170] The importance of the information strategy was highlighted by Nye when he observed that there would not be much point in winning the military campaign if the overarching information campaign was lost.[171] An information campaign is the "co-ordinated information output of all government activity undertaken to influence decision-makers in support of policy objectives, while protecting one's own decision-makers".[172] The information campaign translates the desired outcome into discrete activities for each of the national instruments and the military contribution is through information and media operations.[173] Information operations are the:

> Co-ordinated actions undertaken to influence an adversary or potential adversary in support of political and military objectives by undermining his will, cohesion and decision-making ability, through affecting his information, information based processes and systems while protecting one's own decision-makers and decision-making processes.[174]

---

[166] Betz and Stevens, *Cyberspace and the State*, 76.
[167] Samaan, "Cyber Command," 19.
[168] Betz and Stevens, *Cyberspace and the State*, 81.
[169] Wingfield, "International Law and Information Operations," 541.
[170] UK. DCDC. *British Defence Doctrine*, 1-9.
[171] Betz and Stevens, *Cyberspace and the State*, 87.
[172] United Kingdom. Joint Doctrine and Concept Centre (JDCC). *Information Operations.* Joint Warfare Publication 3-80. (Shrivenham: JDCC, 2002), 1-2.
[173] Ibid., 1-3.
[174] Ibid., 2-1.

Information operations are implemented through several tools and cyber capabilities are considered a key tool due to their ability to affect information and information processes. All aspects may be used: defensive operations to protect decision-making processes; exploitative operations to gain information on adversaries; and offensive to degrade decision-making and undermine cohesion and will of adversaries.[175] Cyber capabilities are not limited to supporting the military instrument as they can also support the diplomatic and economic elements of the information campaign. For example, they could be used to support the diplomatic instrument by preventing an adversary government spreading propaganda on the Internet. Therefore, cyber capabilities have a supporting information role across all the instruments of national power.

Cyber capabilities can also be used to enable the application of the instruments of national power in addition to providing supporting information effects. For the military instrument, cyber effects can enable or support operations conducted in the physical domains. For instance, cyber capabilities could be used to prevent the transmission of an adversary's intelligence surveillance and reconnaissance information to enable land forces to conduct a surprise offensive. Used in this manner, there are parallels between cyber operations and electronic warfare.[176] There may also be situations where cyber capabilities could provide unique effects that support the instruments of national power in achieving strategic objectives. For example, there may be a requirement to coerce a state into a particular course of action. If diplomatic talks and economic sanctions are yet to successfully coerce the state, cyber capabilities could be used to provide coercive effects without the damage that a kinetic strike would cause. Of note, any cyber operation would need to be in accordance with the Law or Armed Conflict to ensure it was ethical and legal.

The unique effects provided by cyber capabilities have increasingly made the instruments of national power cyber dependent. Hence, the importance now allocated to cyberspace in political and military spheres.[177] Independent cyber capabilities, however, are unlikely to be decisive in times of war.[178] There is no guarantee that even the worst-case scenarios described in the literature would alone compel a state to surrender territory or feel existentially threatened.[179] Consequently, cyber capabilities are principally used to deliver supporting effects for the instruments of national power. They are effectively force enabling and force multiplying.

There is also considerable academic discussion on the value of cyber deterrence. The aim of deterrence is to convince an adversary that undertaking a particular course of action would not deliver the advantages it seeks. Deterrence can be achieved by punishment where the costs

[175] Ibid., 2A-3.
[176] Samaan, "Cyber Command," 20.
[177] Harvey, "Determining the Utility of Cyber Power," 25.
[178] Ibid., 58.
[179] Samaan, "Cyber Command," 20.

sustained by the adversary are maximised or denial where the adversary's benefits are minimised.[180] The ability to deter actors in cyberspace is strongly questioned. The main argument against cyber deterrence is based on the attribution characteristic as the inability to identify the aggressor would prevent a retaliatory response in self-defence.[181] In addition, the presumption of rational actors in a deterrence relationship is undermined by the presence of non-state actors.[182] Any cyber deterrence policy would require a credible cyber capability that is both able to attack and defend. Deterrence within cyberspace may not be achievable but it could be used as part of conventional deterrence. Indeed, a credible offensive cyber capability may act as a deterrent against a conventionally superior adversary under particular conditions.[183] Nonetheless, this would require the communication of the credible threat to the adversary being deterred and this may not be achievable while states shroud their cyber capabilities in secrecy.

Often linked to the discussion on cyber deterrence is one on arms control to prevent the proliferation of cyber weapons.[184] An international treaty could also have a deterrent effect by limiting when it would be acceptable for cyber capabilities to be used. However, such a treaty would require agreement between states which, despite some rhetoric, is presently not forthcoming. Moreover, the benefits of such a treaty may not be as clear as with the Nuclear Proliferation Treaty.[185] At the lower end of the capability spectrum, preventing the proliferation of capabilities needed to produce cyber weapons may not be possible as the tools required are freely available.[186] At the higher end, states are unlikely to enter into an agreement that may limit their capabilities or restrict their freedom of manoeuvre in cyberspace, especially espionage activities.[187] Furthermore, the ability to distinguish between code that is for defensive or offensive purposes is extremely difficult, unlike nuclear weapons where the number of warheads can be counted and the spread of nuclear material controlled.[188]

Reported Cyber Activity

To this point, most of the discussion has been based upon theoretical capabilities and scenarios. To provide the basis for the assessment of where cyber sits on the spectrum between the two extremes of buzzword and instrument of national power, examples of reported cyber activity from open-source material will now be examined. There have been a substantial number of cyber

[180] Stevens, "Cyberwar of Ideas?," 151.
[181] Samaan, "Cyber Command," 18.
[182] Stevens, "Cyberwar of Ideas?," 152.
[183] Liff, "Cyberwar," 408.
[184] Martin Libicki, "Cyberwar as a Confidence Game," *Strategic Studies Quarterly* 5, no. 1 (2011): 132.
[185] Stevens, "Cyberwar of Ideas?," 163.
[186] Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol, CA: O'Reilly Media, 2010), 33.
[187] Hayden, "Future of Things 'Cyber'," 7.
[188] Farwell and Rohozinski, "New Reality of Cyber War," 116.

incidents reported that cover the full range of cyber capabilities. Examples of the following will now be explored: criminal acts, espionage, cyber capabilities in support of military operations, and cyber capabilities used to deliver independent effects.[189]

Criminal cyber activity for political, social or financial gain is the most commonly reported. One of the most high-profile uses of cyberspace for political reasons was a cyber attack on Estonia in 2007 by 'hacktivists'. Set against a backdrop of heightened tensions between Estonia and Russia and domestic conflict between the Estonian government and the Russian ethnic minority, Estonia relocated a Russian war memorial. This caused great offence to Russians which manifested as riots and malevolent cyber activity. Over a three-week period Estonia was subject to distributed denial of service attacks,[190] email spam and website defacements.[191] There are varying accounts of the attack's impact but it is generally acknowledged that internet-based financial and governmental services were severely disrupted. The Russian government denied sponsoring the attack and attributed it to irate patriots who took to the Internet to protest.[192] As a consequence of the incident, wider public opinion viewed cyber attacks as more plausible.[193] There are also numerous examples of financially motivated cyber activity. A recent large-scale event occurred in December 2013 when forty million customers of a US retail chain had their credit or debit card credentials stolen. The card details were subsequently for sale on Internet forums and sites frequented by organised crime groups.[194]

Espionage activities have also been widely reported. A prominent instance was the theft of significant F-35 Lightning II information from a contractor. The volume of data amounted to several terabytes and related to design and electronic systems.[195] This information could be used to exploit weakness or to replicate the technology. This incident is an example of targeted information theft; there are also examples where multiple networks have been penetrated as part of a wider espionage operation. One such instance is *GhostNet* which was reported in 2009 to have infected over a thousand computers in over a hundred countries of which approximately a third of the targets were in noteworthy governmental and media organisations. The malicious software, which was not overly advanced, allowed audio and video surveillance, the capture of

[189] For a detailed record see Centre for Strategic and International Studies, "Significant Cyber Incidents Since 2006," Strategic Technologies Program, Centre for Strategic and International Studies, http://csis.org (accessed March 29, 2014).

[190] A denial of service attack is an attempt to make an information service or resource unavailable to the intended users. A distributed denial of service attack is where the attack originates from multiple sources.

[191] Jason Healey, *A Fierce Domain: Conflict in Cyberspace, 1986-2012* (Vienna, VA: Cyber Conflict Studies Association, 2013), 174.

[192] Eberle, "Just War and Cyberwar," 58.

[193] Healey, *Fierce Domain*, 191.

[194] Centre for Strategic and International Studies, "Significant Cyber Incidents Since 2006," Strategic Technologies Program, Centre for Strategic and International Studies, http://csis.org (accessed March 29, 2014).

[195] Thomas Chen, *An Assessment of the Department of Defense Strategy for Operating in Cyberspace* (Carlisle, PA: US Army War College Press, 2013), 2.

sensitive files and the logging of usernames and passwords from the infiltrated computers.[196] China has been linked to operating this expansive spying network.[197] However, the perpetrator's identity has yet to be irrefutably determined.[198] These two examples demonstrate that despite investment in defences, cyber espionage is pervasive and producing results against both private and public establishments.[199]

Cyber operations that enable or amplify the effects of a conventional operation have also taken place. It has been documented that Israel used cyber capabilities in 2007 to disable elements of the Syrian integrated air defence system in order to enable its aircraft to attack a suspected nuclear facility.[200] It was assessed that the cyber attack was critical to the successful prosecution of the target by non-stealth aircraft.[201] A further example of complementary cyber operations is in the Russian Georgian conflict in 2008. Russia invaded Georgia following Georgia's attempt to reassert control in South Ossetia. The Russian invasion included a cyber campaign that was coordinated with the land and air operations.[202] The cyber campaign focussed on the "denial and degradation of Georgian communication systems".[203] This impacted on Georgia's ability to communicate with the wider world which meant the Russian narrative dominated. There were also attacks on Georgian websites and financial services to discredit those in power, influence wider opinion and disturb everyday life.[204] The attacks, which were generally rudimentary in nature, achieved their aim of disrupting services and having a psychological impact on the Georgian public.[205] The cyber campaign had a limited effect on the outcome of the conflict; nonetheless, it did demonstrate the utility of cyber power to enable conventional operations and as a tool for information operations. An improved cyber element in the future could have more sophisticated effects on the outcome of a military campaign.

Cyber capabilities have also been used to deliver independent effects. One of the most discussed incidents was when a cyber attack was used to create physical destruction. In 2010 an advanced cyber weapon known as Stuxnet was discovered. It is alleged that Stuxnet successfully infiltrated information systems at an Iranian nuclear site such that it was able to manipulate control systems

[196] Carr, *Inside Cyber Warfare*, 146.

[197] Paul Cornish, David Livingstone, Dave Clemente and Claire York. *On Cyber* Warfare (London: Chatham House, 2010), 8.

[198] Forrest Hare, "The Significance of Attribution to Cyberspace Coercion: A Political Perspective," in *2012 4th International Conference on Cyber Conflict*, eds C. Czosseck, R. Ottis and K. Ziolkowski (Tallinn: NATO CCD COE Publications, 2012), 129.

[199] Rid, "Cyber War Will Not Take Place," 22.

[200] Heather Dinniss, *Cyber Warfare and the Laws of War* (Cambridge: Cambridge University Press, 2012), 7.

[201] Rid, "Cyber War Will Not Take Place," 17.

[202] Carr, *Inside Cyber Warfare*, 3.

[203] Healey, *Fierce Domain*, 196.

[204] Ibid., 198.

[205] Ibid., 203.

to cause physical damage to centrifuges in order to delay the Iranian nuclear weapons programme.[206] Stuxnet was an advanced weapon for a number of reasons. First, it managed to get onto a discrete system that was air gapped from the Internet. Second, it targeted very specific industrial control systems and was able to manipulate these controls without detection, providing normal feedback to operators while damaging the centrifuges. Third, despite the weapon infecting computers and networks other than those targeted, it did not cause harm to these systems as the weapon was tailored to its target.[207]

There are some important deductions that should be made from this example. First, Stuxnet would have required significant intelligence and support networks to implement the attack; the code used was advanced and would likely have required the support of multiple agencies to develop and deploy the weapon. It has been assessed that the range of capabilities required is only available to a limited number state actors.[208] The attack has also demonstrated the ability for cyber weapons to be designed for specific targets while minimising the collateral damage.[209] Finally, as the Stuxnet code is in the open, it is likely to be no longer effective as the vulnerabilities have undoubtedly been removed. Further, there is potential for aspects of the code to be copied or exploited by other actors. There are varying assessments of the effectiveness of the attack. It is regularly claimed the attack delayed Iran's nuclear programme by about a year.[210] On the contrary, Ivanka Barzashka has argued that Stuxnet was not very successful and may have been of overall benefit to Iran.[211] There is, however, little disagreement that Stuxnet set a precedent for the use of cyber weapons to deliver independent effects.

Stuxnet is also an example of cyber capabilities acting as a tool in support of instruments of national power. Diplomatic and economic activity was used to persuade and coerce Iran to stop its nuclear weapon development. Despite these efforts, it was assessed that Iran continued its programme and the military instrument could have been used to compel Iran though kinetic strikes. This course of action could have had destabilising effects for the region through its overt aggression and potential collateral damage. Cyber capabilities allowed, through their distinctive characteristics, the use of coercive power with reduced likelihood of destabilising the region.[212] The covert cyber attack added further pressure for Iran to cease development. The physical and

[206] Lindsay, "Stuxnet," 366.
[207] Rid, *Cyber War Will Not Take Place*, 44.
[208] Farwell and Rohozinski, "New Reality of Cyber War," 115.
[209] Ibid., 108.
[210] Lindsay, "Stuxnet," 390.
[211] Ivanka Barzashka, "Are Cyber-Weapons Effective?," *RUSI Journal* 158, no. 2 (2013): 54.
[212] Farwell and Rohozinski, "Stuxnet and Future of Cyber War," 34.

coercive effects of Stuxnet have been questioned; however, a combination of all instruments of national power brought Iran to the negotiating table in 2013.[213]

Cyber capabilities have been analysed by examining theoretical and actual cyber activities reported in open sources. Many states have developed cyber strategies due to their dependency on cyberspace, while cyber capabilities have been used for force multiplying and force enabling effects in support of the instruments of national power. Criminal activity is the predominant act undertaken within cyberspace and these are often conflated in literature with offensive military operations. Cyber capabilities have been used to deliver independent effects, but there has yet to be an example of the devastating acts portrayed in the literature that would signal a change to the nature of war.

[213] BBC News, "Iran agrees to curb nuclear activity at Geneva talks," BBC News, http://www.bbc.co.uk/news/ (accessed April 17, 2014).

CYBER: THE LATEST BUZZWORD?

Gibson used the term cyberspace in his novel as "it seemed like an effective buzzword … evocative and essentially meaningless".[214] Cyberspace may not have had any meaning to Gibson but it and its prefix cyber have been used extensively ever since. There are many alarmists or sensationalist newspaper articles, academic journals and books written about the threats in cyberspace with covering headlines or titles using cyber-prefixed words to emphasise threats and risks. These often highlight the vulnerability of critical national infrastructure; the threat posed to the national economy by crime and espionage; and the potential of a war fought in cyberspace.[215] Based on the evidence to date, the ability of cyber power to realise these threats is limited. Rid believes there is a "gulf between hype and reality" with cyber power less capable than normally presumed.[216] Consequently, there is a body of opinion that the cyber threat is being glorified by people or organisations with a vested interest, such as political entities or internet security firms.[217] This raises the question: is cyber now a buzzword similar to what Gibson intended that has no real meaning and may fade out after time or is there substance behind it? Comparable military terms have faded out of popular use, such as effects based operations, when the next expression comes into fashion or the concept is proved not to be the 'be all and end all'.[218]

One of the causes of the difference between reality and the hype surrounding cyberspace is the interpretation of the value of information. There is no agreed method used to quantify the damage inflicted by the loss of information following a cyber attack. Heather Dinniss argued that when assessing the impact of the information revolution on conflict the following four factors should be taken into account: "the ubiquity of information technology, the increasing amount and decreasing cost of information, societies' changing value systems based on information, and finally the effects of increased information on organisational structures within both domestic and international society".[219] Dinniss has made recommendations on the aspects to consider when estimating the impact of the loss of information or process but does not provide guidance on how these should be measured. Michael Schmitt developed the following analytical framework to aid the analysis of cyber effects to determine if they are equivalent to the conventional use of force: "severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility".[220] The framework, however, does not remove the subjective nature of the analysis and is open to interpretation. Hence, the impact of attacks or assessment of potential consequences from a

[214] Betz and Stevens, *Cyberspace and the State*, 36.
[215] Ibid., 11.
[216] Rid, *Cyber War Will Not Take Place*, 173.
[217] Betz and Stevens, *Cyberspace and the State*, 96.
[218] Ibid., 89.
[219] Dinniss, *Cyber Warfare and the Laws of War*, 12.
[220] Caton, "Beyond Domains," 163.

threat are hard to judge and will vary from one person to the next. This may be a contributing factor to the gulf between hype and reality.

The increase in complexity and number of cyber incidents coupled with a corresponding increase in media coverage, has resulted in cyber security issues moving away from the realm of experts to executives, civil rights activists and politicians.[221] This is a major contributing factor to the hyperbole; however, not all of it is misplaced as state and non-state actors are using offensive cyber capabilities.[222] Furthermore, the majority of diplomatic, economic and military confrontations now have a cyber component. The cyber elements range from regular minor inconveniences to infrequent major inconveniences. Notwithstanding, these cyber components have yet to cause long-term disruption.[223] Despite this lack of enduring impact, the threat of cyber incidents remains high on policy agendas and risk registers. There are three principal reasons for this. First, cyber risks are disproportionately psychologically perceived, which leads to regulatory action and high costs that do not necessarily bear results. Second, cyber is a highly politicised issue and the context of any announcement or policy should be taken into account. Third, the media hype surrounding any cyber incident raises the profile of any issue dramatically, which also distorts perception.[224] There may be some doubt as to the likelihood and impact of cyber threats in the long term but there is no doubt that cyberspace has fostered considerable change in contemporary life.

Cyber capabilities have fundamentally changed how humans live, work and socialise. As a result, the opportunities and threats delivered by cyberspace will continue. Hence, the term cyber is unlikely to disappear from mainstream vocabulary. Moreover, the hype surrounding cyber caused by alarmist and sensationalist headlines is likely to remain. The use of dramatic phrases involving cyber may have their purpose as it conveys to the general public greater meaning. Nevertheless, it also serves to increase threat perception above reality and may make people indifferent to the threat posed by cyber crime by being focused on the more unlikely threat to national security. Rid makes the point that when cyber analogies are used, where the analogies do not hold must also be included otherwise misunderstanding creeps into general comprehension.[225] He summarises the problem well when he states that “loose talk of cyber war overhypes the offences and blunts the defences”.[226] Cyber has suffered from this lack of understanding and a misuse of its vocabulary due to its high profile being used for political point scoring, selling newspapers, attracting higher viewing ratings and exploiting available funding.

[221] Cavelty, “Militarisation of Cyberspace,” 141.
[222] Betz and Stevens, *Cyberspace and the State*, 45.
[223] Cavelty, “Militarisation of Cyberspace,” 149.
[224] Ibid.
[225] Rid, *Cyber War Will Not Take Place*, 165.
[226] Ibid., 174.

Cyber capabilities are now so fundamental to civilian and military life that they are here to stay and cannot be disregarded even if one tires of the amount of times that it is reported that a 'cyber war' has taken place. It is, therefore, assessed that cyber is not just a buzzword. Cyber has proven to be "evocative" but it is not "meaningless" as there is substance to the opportunities and threats underlying the hype.[227] Due to the importance of cyberspace to everyday life, the word cyber will continue to be used in both noun and adjective form in common parlance.

[227] Betz and Stevens, *Cyberspace and the State*, 36.

CYBER: INSTRUMENT OF NATIONAL POWER?

Cyber is often portrayed as a new capability that can deliver devastating attacks without the need for the commitment of armed forces and, as a result, there will be standalone cyber wars.[228] For instance, CNN broadcast a live simulation of a cyber attack, called *Cyber Shockwave*, which left viewers with little to imagine of the dire consequences if cyberspace is left undefended.[229] Clarke and Knake describe the situation as a cyber warrior that is able to "reach out from cyberspace" to turn off essential services or destroy targets.[230] Cyber is considered by some commentators to have altered parameters to the extent that the nature of war has changed.[231] Chris Demchak describes the nature to have transformed to one that is fought on a global scale over the long term with catastrophic outcomes that can affect the whole society.[232] If these ground-breaking aspects are true, cyber should be considered an additional instrument of national power due to its ability to deliver national strategic objectives. This proposal will now be analysed to determine if cyber should be considered an instrument of national power.

Eliot Cohen observed that "air power is an unusually seductive form of military strength, in part because like modern courtship, it appears to offer gratification without commitment". [233] Cyber power is often considered even more seductive as it "appears to offer gratification without the need for physical connection (let alone commitment) to other human beings whatsoever".[234] In 1967 when discussing the impact of new technology, Marshall McLuhan commented that "whenever a new environment goes around an old one there is always new terror".[235] David Betz and Tim Stevens argue that cyber power has had a massive impact on life but it changes features in the military sphere less than has been theorised.[236] They propose that lessons should be learned from the introduction of air power. In particular, it should be recognised that the threats and opportunities presented by a new capability have a propensity to be oversold by its early advocates.[237] Early air power theorists had a conviction of the ability for air power to be the decisive factor in a war against a fragile society and there would appear to be similar claims today for the strengths of cyber power.[238] It is possible that today's cyber power theorists are

[228] Clarke and Knake, *Cyber War*, 31.
[229] Betz and Stevens, *Cyberspace and the State*, 127.
[230] Clarke and Knake, *Cyber War*, 101.
[231] Arquilla and Ronfeldt, "Cyberwar is coming!," 147.
[232] Chris Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (Athens, GA: University of Georgia Press, 2011), 4.
[233] Eliot Cohen, "The Mystique of U.S. Air Power," Foreign Affairs, http://www.foreignaffairs.com (accessed April 17, 2014).
[234] Betz and Stevens, *Cyberspace and the State*, 88.
[235] Ibid., 12.
[236] Ibid.
[237] Ibid., 87.
[238] Ibid., 85.

succumbing to the same issues that affected air power theorists. Thus, any claims that cyber power is capable of resolving a geopolitical crisis without the need for conventional forces should be treated with caution.[239] Without doubt, cyber power is an important complement to military, economic and diplomatic capabilities. Yet, crucially, it neither removes the need for these capabilities nor alters the nature of war.[240] Adam Liff also argues that cyber is not an "absolute weapon" and contends that the cyber power theorists who suggest that it is, fall foul of the same issues as the air power theorists who believed that aerial bombardment could be "translated into political influence" to resolve a crisis.[241]

There is also a common understanding that within cyberspace, offensive actions are dominant and hold the advantage over defensive actions. This opinion is formed due to cyberspace's ubiquity, ease of access and availability of cyber weapons. The costs of cyber defence also rise considerably when compared with offensive aspects and, as a result, it is viewed that cyber attacks would generally find a way to succeed.[242] It is, therefore, regularly argued that cyber capabilities increase an adversary's opportunities and the scale of damage possible while minimising the risks. For example, it would be easier to deploy a cyber weapon than to dispatch special forces on a covert operation.[243] For these reasons, it is often asserted that cyber favours weaker states as it is easier to achieve a significant offensive capability than defensive.[244]

However, these arguments miss some fundamental points. Many actors, both state and non-state, can undertake lower-level attacks that are normally associated with crime and espionage. Cyber attacks that cause substantial damage require complex cyber weapons and quality is more important than quantity in the development of these weapons.[245] A considerable amount of intelligence is required to tailor a weapon to a particular target and the deployment of advanced weapons may require a number of agents, such as intelligence services or special forces, especially if the targeted system is not connected to the Internet. It is likely that only a few states have the range of capabilities required to do this. For example, not many states are assessed to have the ability to develop and deploy a Stuxnet-like capability. Hence, only the stronger states are capable of developing complex cyber weapons.[246] The low barrier to entry and ubiquitous nature of cyber weapons only applies to those at the low end of the capability spectrum such as criminal and espionage activities. As with advanced military capabilities in the conventional

[239] Ibid., 89.
[240] Ibid., 96.
[241] Liff, "Cyberwar," 426.
[242] Lindsay, "Stuxnet," 375.
[243] Rid, *Cyber War Will Not Take Place*, 167.
[244] Ibid., 168.
[245] Rid, "Cyber War Will Not Take Place," 28.
[246] Ibid.

domains, there is a high barrier to entry for complex cyber weapons and they are not pervasive. Therefore, offensive actions are dominant over defensive for criminal and espionage activities but not for advanced cyber operations.[247]

There is yet to be an example of a complex cyber weapon causing devastating consequences.[248] Indeed, while details of state capabilities remain classified it is unknown whether such weapons exist. If they do exist, states would require the same political will to use as they would for the employment of equivalent kinetic capabilities. This mitigates the attribution characteristic of cyberspace as very few states would have both the cyber capability and political will to undertake an attack. As argued by Liff, although the spread of cyber capabilities may increase cyber skirmishes between actors, it is unlikely to increase the frequency of comprehensive attacks between states.[249] Furthermore, it does not level the playing field between strong and weak states.[250]

Hence, cyber is another tool that supports the application of the instruments of national power. It is not a new instrument that can meet national strategic aims independently through devastating power or other effects. Air power is not considered an instrument of national power for the same reasons. Rather, it is the military as a whole that is viewed as an instrument of national power as joint action is required to meet strategic-level aims.[251] This, however, does not disregard the importance of cyberspace. It is rightly considered a military domain as power can be exerted both within and through it. Moreover, it would be foolish now for an armed force not to consider cyberspace when conducting operations. A good analogy of fighting without the protection of military cyber power may be akin to fighting on land without the cover of air power; an advanced force without cyber protection may suffer the same fate as Rommel's tanks.[252] Cyber should be considered a complementary capability that can deliver force enabling and force multiplying effects that support the accomplishment of strategic objectives across the instruments of national power, [253] either directly or as part of an information campaign, rather than one which can autonomously achieve political outcomes.[254]

---

[247] Lindsay, "Stuxnet," 396.

[248] Emilio Iasiello, "Cyber Attack: A Dull Tool to Shape Foreign Policy," in *2013 5th International Conference on Cyber Conflict*, eds K. Podins, J. Stinissen and M. Maybaum (Tallinn: NATO CCD COE Publications, 2013), 452.

[249] Liff, "Cyberwar," 426.

[250] Betz and Stevens, *Cyberspace and the State*, 135.

[251] United Kingdom. Development, Concepts and Doctrine Centre (DCDC). *Defence Joint Operating Concept*. Joint Concept Note 1/14. (Shrivenham: DCDC, 2014), 3-8.

[252] Betz and Stevens, *Cyberspace and the State,* 89.

[253] Ibid., 44.

[254] Samaan, "Cyber Command," 19.

CONCLUSION

In conclusion, cyber is neither a buzzword nor an instrument of national power. Cyber cannot be ignored as it is fundamental to civilian life and military effectiveness. Consequently, cyber is not just a buzzword as there is substance to the opportunities and threats underlying the hype surrounding cyber. The volume of hype is also unlikely to subside in the near future and cyber-related terms will continue to be used in common vocabulary. Furthermore, cyber capabilities do not change the nature of war or provide the ability to independently deliver national strategic objectives through overwhelming power or other effects. Hence, cyber should not be considered an instrument of national power. Cyber provides a capability similar to how information is considered to support the diplomatic, economic and military instruments to meet desired political outcomes. Cyber is a complementary tool that supports the instruments of national power directly through the provision of force multiplying and force enabling effects or as part of an information campaign.

The evolution of cyberspace has created a wealth of opportunities for commercial enterprises, the delivery of public goods and services and new methods for social interactions. It has also provided new tools for states and non-state actors to employ in pursuit of political goals.[255] At the lower end of the capability spectrum, this has diffused power from state to non-state actors, and at the higher end, it has made the already powerful states even more powerful.[256] Crucially, cyberspace has also generated dependencies as cyber capabilities are now essential to the contemporary way of life as without computers, nothing would work.[257] As a result, there is a need to secure cyberspace in order to protect these dependencies. This is not limited to governmental networks; defending a state's cyberspace must include both the public and private sectors.[258] Accordingly, many states have developed national cyber security strategies to maximise the benefits derived from cyberspace and minimise the threats.

Cyberspace is an artificial entity that has characteristics inherently different to those of the physical military domains. There is utility in classifying it as a military domain as cyberspace and the conventional domains are interdependent and cyber power can be used to create advantages, influence the behaviour of actors and the course of events in, from or through cyberspace. Notably, cyber can be used to deliver soft and hard power effects. Due to the secrecy that surrounds state cyber capabilities and the range of opinions within the literature, cyber power is mainly inferential. The many theories on cyber capabilities range from inconsequential to effects

[255] Betz and Stevens, *Cyberspace and the State*, 10.
[256] Ibid., 131.
[257] Clarke and Knake, *Cyber War*, 97.
[258] Rid, *Cyber War Will Not Take Place*, 111.

analogous to weapons of mass destruction without the associated collateral damage; there have yet to be any examples of the latter. The majority of activities in cyberspace are related to crime and espionage, rather than offensive military cyber operations, which are often misleadingly reported as 'cyber attacks' or acts of 'cyber war'. As a consequence, cyber risks are disproportionately psychologically perceived and cyber has become a politicised issue that sits high on policy agendas and risk registers. This makes cyber "more terrifying in theory than practice".[259]

Criminal and espionage activities are prevalent in cyberspace as the capabilities needed are ubiquitous. Therefore, states, non-state actors, groups and individuals all have the ability to undertake these activities and the likelihood of attribution is low due to the characteristics of cyberspace and the numerous actors. Offensive cyber activities are limited to fewer actors due to the requirement for more advanced cyber capabilities that are not necessarily widely available. Moreover, complex offensive cyber capabilities, such as Stuxnet, are limited to advanced states due to the requirement for high-grade intelligence and multiple agencies to develop and deploy the weapon. The likelihood of attribution is greater at this higher end of the capability spectrum as very few states would have both the cyber capability and political will to undertake such attacks.

Cyber literature is beset by substantial definitional issues of which one consequence is a lack of analytical consistency. It is important for the advancement of cyber capabilities, strategies and theories that definitions clearly differentiate offensive cyber activities from criminal and espionage.[260] Cyberspace is a complex environment due to its artificial and pliable nature and, unlike the emergence of air power, there is yet to be a dominant cyber power theory. There are, nonetheless, cyber theories that exaggerate the potential effects of cyber capabilities; cyber has changed the character of war and not the nature. Without question, cyber has transformed the world and there will not be a return to a time without it. A secure cyber environment is needed for contemporary life to prosper and the threats and opportunities presented must be viewed in the appropriate context. The privileged position of being able to reflect on the emergence and subsequent development of air power should be exploited to inform the evolution of cyber power theories by taking heed of the errors made.

[259] Iasiello, "Cyber Attack," 452.
[260] Liff, "Cyberwar," 404.

BIBLIOGRAPHY

Books and Publications

Andress, Jason and Steve Winterfeld. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners.* Amsterdam: Elsevier, 2011.

Arquilla, John and David Ronfeldt, eds. *In Athena's Camp: Preparing for Conflict in the Information Age.* Santa Monica, CA: RAND Corporation, 1997.

Arquilla, John and David Ronfeldt. *The Advent of Netwar.* Santa Monica, CA: RAND Corporation, 1996.

Baylis, John, Steve Smith and Patricia Owens. *The Globalization of World Politics: An introduction to international relations.* 5th ed. Oxford: Oxford University Press, 2011.

Betz, David and Tim Stevens. *Cyberspace and the State: Toward a Strategy for Cyber-power.* Abingdon: Routledge, 2011.

Blumenthal, Marjory and David Clark. "The Future of the Internet and Cyberpower." In *Cyberpower and National Security*, edited by Franklin Kramer, Stuart Starr and Larry Wentz, 206-240. Washington, DC: Potomac Books, 2009.

Burnham, Peter, Karin Lutz, Wyn Grant and Zig Layton-Henry. *Research Methods in Politics.* 2nd ed. New York: Palgrave Macmillan, 2008.

Carr, Jeffrey. *Inside Cyber Warfare.* Sebastopol, CA: O'Reilly Media, 2010.

Caton, Jeffrey. "Beyond Domains, Beyond Commons: Context and Theory of Conflict in Cyberspace." In *2012 4th International Conference on Cyber Conflict*, edited by C. Czosseck, R. Ottis and K. Ziolkowski, 157-167. Tallinn: NATO CCD COE Publications, 2012.

Cavelty, Myriam. "The Militarisation of Cyberspace: Why Less May Be Better." In *2012 4th International Conference on Cyber Conflict,* edited by C. Czosseck, R. Ottis and K. Ziolkowski, 141-153. Tallinn: NATO CCD COE Publications, 2012.

Chen, Thomas. *An Assessment of the Department of Defense Strategy for Operating in Cyberspace.* Carlisle, PA: US Army War College Press, 2013.

Clarke, Richard and Robert Knake. *Cyber War: The next threat to national security and what to do about it.* New York: Ecco, 2012.

Clausewitz, Carl von. *On War.* Michael Howard and Peter Paret, eds and trans. Princeton: Princeton University Press, 1976.

Clemente, Dave. *Cyber Security and Global Interdependence: What is Critical?* London: Chatham House, 2013.

Conti, Gregory, John Nelson and David Raymond. "Towards a Cyber Common Operating Picture." In *2013 5th International Conference on Cyber Conflict*, edited by K. Podins, J. Stinissen and M. Maybaum, 279-295. Tallinn: NATO CCD COE Publications, 2013.

Cornish, Paul, Rex Hughes and David Livingstone. *Cyberspace and the National Security of the United Kingdom: Threats and Responses.* London: Chatham House, 2009.

Cornish, Paul, David Livingstone, Dave Clemente and Claire York. *Cyber Security and the UK's Critical National Infrastructure.* London: Chatham House, 2011.

Cornish, Paul, David Livingstone, Dave Clemente and Claire York. *On Cyber Warfare.* London: Chatham House, 2010.

Czosseck, C., R. Ottis and K. Ziolkowski, eds. *2012 4th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications, 2012.

Demchak, Chris. *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*. Athens, GA: University of Georgia Press, 2011.

Dinniss, Heather. *Cyber Warfare and the Laws of War.* Cambridge: Cambridge University Press, 2012.

Gray, Colin. *Another Bloody Century: Future Warfare.* London: Phoenix, 2006.

Gray, Colin. *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling.* Carlisle, PA: US Army War College Press, 2013.

Hare, Forrest. "The Significance of Attribution to Cyberspace Coercion: A Political Perspective." In *2012 4th International Conference on Cyber Conflict*, edited by C. Czosseck, R. Ottis and K. Ziolkowski, 125-139. Tallinn: NATO CCD COE Publications, 2012.

Healey, Jason, ed. *A Fierce Domain: Conflict in Cyberspace, 1986-2012.* Vienna, VA: Cyber Conflict Studies Association, 2013.

Iasiello, Emilio. "Cyber Attack: A Dull Tool to Shape Foreign Policy." In *2013 5th International Conference on Cyber Conflict*, edited by K. Podins, J. Stinissen and M. Maybaum, 451-468. Tallinn: NATO CCD COE Publications, 2013.

Kramer, Franklin, Stuart Starr and Larry Wentz, eds. *Cyberpower and National Security.* Washington, DC: Potomac Books, 2009.

Kramer, Franklin. "Cyberpower and National Security: Policy Recommendations for a Strategic Framework." In *Cyberpower and National Security*, edited by Franklin Kramer, Stuart Starr and Larry Wentz, 3-23. Washington, DC: Potomac Books, 2009.

Kuehl, Daniel. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security*, edited by Franklin Kramer, Stuart Starr and Larry Wentz, 24-42. Washington, DC: Potomac Books, 2009.

Kwalwasser, Harold. "Internet Governance." In *Cyberpower and National Security*, edited by Franklin Kramer, Stuart Starr and Larry Wentz, 491-524. Washington, DC: Potomac Books, 2009.

Lachow, Irving. "Cyber Terrorism: Menace or Myth?" In *Cyberpower and National Security*, edited by Franklin Kramer, Stuart Starr and Larry Wentz, 437-464. Washington, DC: Potomac Books, 2009.

Leed, Maren. *Offensive Cyber Capabilities at the Operational Level: The Way Ahead.* Washington, DC: Center for Strategic and International Studies, 2013.

Libicki, Martin. *Conquest in Cyberspace: National Security and Information Warfare.* Cambridge: Cambridge University Press, 2007.

Libicki, Martin. *Crisis and Escalation in Cyberspace.* Santa Monica, CA: RAND Cooperation, 2012.

Libicki, Martin. *Cyberdeterrence and Cyberwar.* Santa Monica, CA: RAND Cooperation, 2009.

Libicki, Martin. *Defending Cyberspace and Other Metaphors.* Washington, DC: National Defense University, 1997.

Libicki, Martin. *What is Information Warfare?* Washington, DC: National Defense University, 1995.

Lonsdale, David. *The Nature of War in the Information Age: Clausewitzian Future.* London: Frank Cass, 2004.

McCarthy, John, Chris Burrow, Maeve Dion and Olivia Pacheco. "Cyberpower and Critical Infrastructure Protection: A Critical Assessment of Federal Efforts." In *Cyberpower and National Security*, edited by Franklin Kramer, Stuart Starr and Larry Wentz, 543-556. Washington, DC: Potomac Books, 2009.

Mesic, Richard, Myron Hura, Martin Libicki, Anthony Packard and Lynn Scott. *Air Force Cyber Command (Provisional) Decision Support.* Santa Monica, CA: RAND Cooperation, 2010.

Nye, Joseph. *Cyber Power.* Cambridge, MA: Harvard Kennedy School, 2010.

Nye, Joseph. *The Future of Power.* New York: PublicAffairs, 2011.

Podins, K., J. Stinissen and M. Maybaum, eds. *2013 5th International Conference on Cyber Conflict.* Tallinn: NATO CCD COE Publications, 2013.

Rattray, Gregory. "An Environmental Approach to Understanding Cyberpower." In *Cyberpower and National Security*, edited by Franklin Kramer, Stuart Starr and Larry Wentz, 253-274. Washington, DC: Potomac Books, 2009.

Reveron, Derek, ed. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World.* Washington, DC: Georgetown University Press, 2012.

Rid, Thomas. *Cyber War Will Not Take Place.* London: Hurst and Company, 2013.

Skoudis, Edward. "Information Security Issues in Cyberspace." In *Cyberpower and National Security*, edited by Franklin Kramer, Stuart Starr and Larry Wentz, 171-205. Washington, DC: Potomac Books, 2009.

Starr, Stuart. "Toward a Preliminary Theory of Cyberpower." In *Cyberpower and National Security*, edited by Franklin Kramer, Stuart Starr and Larry Wentz, 43-88. Washington, DC: Potomac Books, 2009.

Strachan, Hew. *The Changing Character of War: A Europaeum Lecture delivered at the Graduate Institute of International Relations, Geneva on 9th November 2006.* Oxford: Europaeum, 2007.

Tibbs, Hardin. *The Global Cyber Game: The Defence Academy Cyber Inquiry Report.* Shrivenham: Defence Academy, 2013.

Thomas, Timothy. "Nation-state Cyber Strategies: Examples from China and Russia." In *Cyberpower and National Security*, edited by Franklin Kramer, Stuart Starr and Larry Wentz, 465-488. Washington, DC: Potomac Books, 2009.

Waltz, Kenneth. *Theory of International Politics.* Boston, MA: McGraw-Hill, 1979.

Wingfield, Thomas. "International Law and Information Operations." In *Cyberpower and National Security*, edited by Franklin Kramer, Stuart Starr and Larry Wentz, 525-542. Washington, DC: Potomac Books, 2009.

Articles

Alexander, Keith. “Warfighting in Cyberspace.” *Joint Force Quarterly* 46 (2007): 58-61.

Arquilla, John. “Twenty Years of Cyberwar.” *Journal of Military Ethics* 12, no. 1 (2013): 80-87.

Arquilla, John and David Ronfeldt. “Cyberwar is coming!” *Comparative Strategy* 12, no. 2 (1993): 141-165.

Ashley, Mark. “KWar: Cyber and Epistemological Warfare – Winning the Knowledge War by Rethinking Command and Control.” *Air and Space Power Journal* 26, no. 4 (2012): 45-60.

Barrett, Edward. “Warfare in a New Domain: The Ethics of Military Cyber-operations.” *Journal of Military Ethics* 12, no. 1 (2013): 4-17.

Barzashka, Ivanka. “Are Cyber-Weapons Effective?” *RUSI Journal* 158, no. 2 (2013): 48-56.

Clarke, Richard. “War from Cyberspace.” *The National Interest* 104 (November/December 2009): 31-36.

Cook, James. “‘Cyberation’ and Just War doctrine: A Response to Randall Dipert.” *Journal of Military Ethics* 9, no. 4 (2010): 411-423.

Dipert, Randall. “Other-Than-Internet (OTI) Cyberwarfare: Challenges for Ethics, Law and Policy.” *Journal of Military Ethics* 12, no. 1 (2013): 34-53.

Dipert, Randall. “The Ethics of Cyberwarfare.” *Journal of Military Ethics* 9, no. 4 (2010): 384-410.

Eberle, Christopher. “Just War and Cyberwar.” *Journal of Military Ethics* 12, no. 1 (2013): 54-67.

Farwell, James and Rafal Rohozinski. “Stuxnet and the Future of Cyber War.” *Survival* 53, no. 1 (2011): 23-40.

Farwell, James and Rafal Rohozinski. “The New Reality of Cyber War.” *Survival* 54, no. 4 (2012): 107-120.

Guitton, Clement. “Cyber insecurity as a national threat: overreaction from Germany, France and the UK?” *European Security* 22, no. 1 (2013): 21-35.

Guitton, Clement and Elaine Korzak. “The Sophistication Criterion for Attribution.” *RUSI Journal* 158, no. 4 (2013): 62-68.

Hayden, Michael. “The Future of Things ‘Cyber’.” *Strategic Studies Quarterly* 5, no. 1 (2011): 3-7.

Jenkins, Ryan. “Is Stuxnet Physical? Does it Matter?” *Journal of Military Ethics* 12, no. 1 (2013): 68-79.

Kelly, Terrence and Jeffrey Hunker. “Cyber Policy: Institutional Struggle in a Transformed World.” *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (2012): 210-242.

Keohane, Robert and Joseph Nye. “Power and Interdependence in the Information Age.” *Foreign Affairs* 77, no. 5 (1998): 81-94.

Libicki, Martin. “Cyberspace Is Not a Warfighting Domain.” *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (2012): 321-336.

Libicki, Martin. “Cyberwar as a Confidence Game.” *Strategic Studies Quarterly* 5, no. 1 (2011): 132-146.

Liff, Adam. “Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War.” *Journal of Strategic Studies* 35, no. 3 (2012): 401-428.

Lin, Herbert. “Offensive Cyber Operations and the Use of Force.” *Journal of National Security Law & Policy* 4, no. 63 (2010): 63-86.

Lin, Patrick. “Ethical Blowback from Emerging Technologies.” *Journal of Military Ethics* 9, no. 4 (2010): 313-331.

Lindsay, Jon. “Stuxnet and the Limits of Cyber Warfare.” *Security Studies* 22, no. 3 (2013): 365-404.

Lucas, George. “Postmodern War.” *Journal of Military Ethics* 9, no. 4 (2010): 289-298.

Meulenbelt, Stephanie. “The ‘Worm’ as a Weapon of Mass Destruction.” *RUSI Journal* 157, no. 2 (2012): 62-67.

Meyer, Paul. “Cyber-security through Arms Control.” *RUSI Journal* 156, no.2 (2011): 22-27.

Meyer, Paul. “Diplomatic Alternatives to Cyber-Warfare.” *RUSI Journal* 157, no. 1 (2012): 14-19.

Miller, Robert, Daniel Kuehl and Irving Lachow. “Cyber War: Issues in Attack and Defense.” *Joint Force Quarterly* 61 (2011): 18-23.

Mumford, Andrew. “Proxy Warfare and the Future of Conflict.” *RUSI Journal* 158, no. 2 (2013): 40-46.

Neville-Jones, Pauline and Mark Phillips. “Where Next for UK Cyber-Security?” *RUSI Journal* 157, no. 6 (2012): 32-40.

Nye, Joseph. “Power and foreign policy.” *Journal of Political Power* 4, no. 1 (2011): 9-24.

Peterson, Dale. “Offensive Cyber Weapons: Construction, Development, and Employment.” *Journal of Strategic Studies* 36, no. 1 (2013): 120-124.

Pretorius, Joelien. “Ethics and international security in the information age.” *Defence & Security Analysis* 19, no. 2 (2003): 165-175.

Rathmell, Andrew. “Cyber-terrorism: The shape of future conflict?” *RUSI Journal* 142, no. 5 (1997): 40-45.

Rid, Thomas. “Cyber War Will Not Take Place.” *Journal of Strategic Studies* 35, no. 1 (2012): 5-32.

Rid, Thomas and Peter McBurney. “Cyber-Weapons.” *RUSI Journal* 157, no. 1 (2012): 6-13.

Ronfeldt, David. “Cyberocracy is Coming.” *The Information Society* 8, no. 4 (1992): 243-296.

Rosenfield, Daniel. “Rethinking Cyber War.” *Critical Review* 21, no. 1 (2009): 77-90.

Samaan, Jean-Loup. “Cyber Command: The Rift in US Military Cyber-strategy.” *RUSI Journal* 155, no. 6 (2010): 16-21.

Stevens, Tim. “A Cyberwar of Ideas? Deterrence and Norms in Cyberspace.” *Contemporary Security Policy* 33, no. 1 (2012): 148-170.

Stone, John. “Cyber War Will Take Place!” *Journal of Strategic Studies* 36, no. 1 (2013): 101-108.

Trias, Eric and Bryan Bell. “Cyber This, Cyber That … So What?” *Air and Space Power Journal* 23, no. 1 (2010): 90-100.

Williams, Brett. “Ten Propositions Regarding Cyberspace Operations.” *Joint Force Quarterly* 61 (2011): 10-17.

Dissertations and Papers

Biggadike, M. “Cyber: The UK Military and the 5th Dimension.” Defence Research Paper, JSCSC, 2012.

Buchan, Glenn. “Information War and the Air Force: Wave of the Future? Current Fad?” Issue Paper, RAND Corporation, 1996.

Cahanin, Steven. “Principles of War for Cyberspace.” Research Report, United States Air War College, 2011.

Convertino, Mike, Lou DeMattei and Tammy Knierim. “Flying and Fighting in Cyberspace.” Research Report, United States Air War College, 2007.

Harvey, Shaun. “Determining the Utility of Cyber Power.” Dissertation, University of Reading, 2012.

Kolhatkar, Aniket. “Cyber Warfare: New Threat to Security or Hype.” Defence Research Paper, JSCSC, 2011.

Mackie, Stuart. “What Role Could Cyber Capabilities Play in a Nation’s Deterrence Framework.” Defence Research Paper, JSCSC, 2013.

Neal-Hopes, Timothy. “Preventing a Cyber Dresden: How the Evolution of Air Power can Guide the Evolution of Cyber Power.” Biblioscholar Dissertation, School of Advanced Air and Space Studies, 2011.

Sharma, Amit. “Cyber Wars: A Paradigm Shift from Means to Ends.” Paper, Defence Research and Development Organization India, undated.

Taipale, K. A. “Cyber-deterrence.” Paper, Stilwell Center for Advanced Studies in Science and Technology Policy, 2010.

Vatis, Michael. “Cyber Attacks During the War on Terrorism: A Predictive Analysis.” Paper, Institute for Security Technology Studies Dartmouth College, 2001.

Watson, Brian. “Has the UK grasped the Challenges and Threats in the Cyber Domain; what are the major challenges and are they being met?” Defence Research Paper, JSCSC, 2013.

Withers, Paul. “What is the Utility of the Fifth Domain?” Dissertation, King’s College London, 2014.

NATO. NATO CCD COE. *National Cyber Security Framework Manual.* Tallinn: NATO CCD COE, 2012.

Russia. Russian Federation. *Basic principles for State Policy of the Russian Federation in the field of International Information Security to 2020.* Russian Federation, unofficial translation, 2013.

United Kingdom. Cabinet Office. *A Strong Britain in an Age of Uncertainty: The National Security Strategy.* London: Cabinet Office, 2010.

United Kingdom. Cabinet Office. *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review.* London: Cabinet Office, 2010.

United Kingdom. Cabinet Office. *Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space.* London: Cabinet Office, 2009.

United Kingdom. Cabinet Office. *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world.* London: Cabinet Office, 2011.

United Kingdom. Capability Manager (Information Superiority). *Network Enabled Capability: An Introduction*. Version 1.1, 2004.

United Kingdom. Development, Concepts and Doctrine Centre (DCDC). *British Defence Doctrine.* Joint Doctrine Publication 0-01. 4th ed. Shrivenham: DCDC, 2011.

United Kingdom. Development, Concepts and Doctrine Centre (DCDC). *UK Air and Space Doctrine.* Joint Doctrine Publication 0-30. Shrivenham: DCDC, 2013.

United Kingdom. Development, Concepts and Doctrine Centre (DCDC). *Information Superiority.* Joint Doctrine Note 2/13. Shrivenham: DCDC, 2013.

United Kingdom. Development, Concepts and Doctrine Centre (DCDC). *Cyber Operations: The Defence Contribution.* Joint Doctrine Note 3/13. Shrivenham: DCDC, 2013.

United Kingdom. Development, Concepts and Doctrine Centre (DCDC). *Defence Joint Operating Concept.* Joint Concept Note 1/14. Shrivenham: DCDC, 2014.

United Kingdom. Development, Concepts and Doctrine Centre (DCDC). *Cyber Primer*. Shrivenham: DCDC, 2013.

United Kingdom. Joint Doctrine and Concept Centre (JDCC). *Information Operations.* Joint Warfare Publication 3-80. Shrivenham: JDCC, 2002.

United States. The White House. *International Strategy for Cyberspace.* Washington, The White House, 2011.

United States. Department of Defense. *Department of Defense Strategy for Operating in Cyberspace.* Washington, Department of Defense, 2011.

United States. Department of Defense. *Dictionary of Military and Associated Terms.* Joint Publication 1-02. Washington, Department of Defense, 2010 (amended February 2014).

United States. Department of the Army. *Cyber Electromagnetic Activities.* Field Manual 3-38. Washington: Department of the Army, 2014.

United States. Congressional Research Service. *Information operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues.* Congressional Research Service, 2007.

United States. Cyber Consequences Unit. *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008.* US Cyber Consequences Unit, 2009.

Electronic Sources

Arquilla, John. “Cyberwar Is Already Upon Us.” Foreign Policy. http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us (accessed December 3, 2013).

BBC News. “Iran agrees to curb nuclear activity at Geneva talks.” BBC News. http://www.bbc.co.uk/news/world-middle-east-25074729 (accessed April 17, 2014).

Bumiller, Elisabeth and Thom Shanker. “Panetta Warns of Dire Threat of Cyberattack on U.S.” The New York Times. http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=2& (accessed March 31, 2014).

Campbell, Gregor. “Cybersecurity and Reality: What’s in a Word?” Info Security. http://www.infosecurity-magazine.com/view/32534/comment-cybersecurity-and-reality-whats-in-a-word/ (accessed April 1, 2014).

Centre for Strategic and International Studies. “Significant Cyber Incidents Since 2006.” Strategic Technologies Program, Centre for Strategic and International Studies. http://csis.org/program/significant-cyber-events (accessed March 29, 2014).

Cohen, Eliot. “The Mystique of U.S. Air Power.” Foreign Affairs. http://www.foreignaffairs.com/articles/49442/eliot-a-cohen/the-mystique-of-us-air-power (accessed April 17, 2014).

Collins, Nick. “Cyber terrorism is 'biggest threat to aircraft'.” The Telegraph. http://www.telegraph.co.uk/finance/newsbysector/transport/10526620/Cyber-terrorism-is-biggest-threat-to-aircraft.html (accessed April 1, 2014).

Coughlin, Con. “China’s cyber-war machine threatens us all.” The Telegraph. http://www.telegraph.co.uk/technology/internet-security/9880195/Chinas-cyber-war-machine-threatens-us-all.html (accessed April 1, 2014).

Curtis, Sophie. “UK to create 'cyber strike force'.” The Telegraph. http://www.telegraph.co.uk/technology/internet-security/10343652/UK-to-create-cyber-strike-force.html (accessed April 1, 2014).

Defence Select Committee. “Defence and Cyber-security: Written evidence from the Ministry of Defence.” UK Parliament. http://www.publications.parliament.uk/pa/cm201012/cmselect/cmdfence/writev/1881/dcs01.htm (accessed March 31, 2014).

Economist, The. “Cyber-warfare: Hype and fear.” The Economist. http://www.economist.com/news/international/21567886-america-leading-way-developing-doctrines-cyber-warfare-other-countries-may (accessed March 31, 2014).

Healey, Jason and Karl Grindal. “Lessons from the First Cyber Commanders.” Atlantic Council. http://www.atlanticcouncil.org/blogs/new-atlanticist/lessons-from-the-first-cyber-commanders (accessed March 31, 2014).

Hill, Simon. “Is ‘Cyberwar’ another harmless buzzword, or an impending threat of nuclear proportions?” Digital Trends. http://www.digitaltrends.com/opinion/is-cyberwar-another-harmless-buzzword-or-an-impending-threat-of-nuclear-proportions/#!B47Fn (accessed March 31, 2014).

Howie, Mike. “Suddenly, cybersecurity becomes the buzz word in international fora as cyber criminals prowl about looking for whom to attack.” Vigilance. http://vigilance-securitymagazine.com/industry-news/viewpoints/2599-suddenly-cybersecurity-becomes-the-buzz-word-in-international-fora-as-cyber-criminals-prowl-about-looking-for-whom-to-attack (accessed March 31, 2014).

Infosec Island. “Cyber Espionage: A Buzzword-Term Often Overused.” Infosec Island. http://infosecisland.com/blogview/19595-Cyber-Espionage-A-Buzzword-Term-Often-Overused.html (accessed March 31, 2014).

Internet Society. “Brief History of the Internet.” Internet Society. http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet (accessed April 7, 2014).

Kozloski, Robert. “The Information Domain as an Element of National Power.” Center for Contemporary Conflict. http://www.hsdl.org/?view&did=232244 (accessed March 31, 2014).

Libicki, Martin. “Don’t Buy the Cyberhype: How to Prevent Cyberwars from Becoming Real Ones.” Foreign Affairs. http://www.foreignaffairs.com/articles/139819/martin-c-libicki/dont-buy-the-cyberhype (accessed March 31, 2014).

Lin, Patrick, Fritz Allhoff and Neil Rowe. “War 2.0: Cyberweapons and Ethics.” Communications of the ACM. http://www3.nd.edu/~mlee20/Cyberweapons_Ethics.pdf (accessed March 31, 2014).

Lobham, Iain. “Director GCHQ cyber speech at the International Institute of Strategic Studies.” GCHQ. http://www.gchq.gov.uk/press_and_media/speeches/Pages/Cyber-speech-at-the-IISS.aspx (accessed March 31, 2014).

Obama, Barack. “Taking the Cyberattack Threat Seriously.” The Wall Street Journal. http://online.wsj.com/news/articles/SB10000872396390444330904577535492693044650 (accessed March 10, 2014).

NATO CCD COE. “National Strategies and Policies.” NATO CCD COE. http://ccdcoe.org/328.html (accessed March 31, 2014).

Regency IT Consulting. “‘Cybersecurity’ – Not just a buzzword; a wake-up call.” Regency IT Consulting. https://www.regencyitc.co.uk/latest-news/cybersecurity-not-just-a-buzzword-a-wake-up-call/ (accessed March 31, 2014).

Rid, Thomas. “Think Again: Cyberwar.” Foreign Policy. http://www.foreignpolicy.com/articles/2012/02/27/cyberwar (accessed December 3, 2013).

Riley, Michael, Ben Elgin, Dune Lawrence and Carol Matlack. “Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It.” Bloomberg BusinessWeek. http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data (accessed April 10, 2014).

Sensing Cyber Blog. “Cyber Security – Not Just Another Buzzword.” Sensing Cyber. http://blog.sensecy.com/2014/01/26/cyber-security-not-just-another-buzzword/ (accessed March 31, 2014).

Smith, Dan. “Cyber warfare and the new age battleground.” The Telegraph. http://www.telegraph.co.uk/sponsored/technology/technology-trends/10231677/cyber-warfare-what-is.html (accessed April 1, 2014).

Tipton, Hord. “Cyber warfare: Don’t get caught in the cross hairs.” The Telegraph. http://www.telegraph.co.uk/technology/internet/10135324/Cyber-warfare-Dont-get-caught-in-the-cross-hairs.html (accessed April 1, 2014).

World Telecommunication/ICT Policy Forum. “IPv4 and IPv6 issues.” International Telecommunication Union. https://www.itu.int/en/wtpf-13/Documents/backgrounder-wtpf-13-ipv4-ipv6-en.pdf (accessed April 6, 2014).

INTENTIONALLY BLANK