IS THERE A COMMON UNDERSTANDING OF WHAT CONSTITUTES CYBER WARFARE?

A Paper by Shane Martin Coughlan

2nd Edition

This research paper was originally submitted as part of a programme of study for the award of a MA in International Studies (Globalisation and Governance) at the University of Birmingham School of Politics and International Studies on September 30th 2003. It was supervised by Dr. Terry Terrif.

shane@opendawn.com
www.opendawn.com/cyber-warfare

First Edition Published in September 2003.
Second Edition Published in March 2016.

ISBN 978-1-329-98783-8

Dedication to the First Edition

This paper is dedicated to Rose, my grandmother, who taught me to work hard at what I want to do, and Kevin, my cousin, who insists that anything is possible.

Dedication to the Second Edition

The second edition is dedicated to all those who wrote about this field during the last decade and who helped create a framework for sensible security discourse.

Acknowledgements for the First Edition

I would like to thank Dr Terry Terrif for supervising this paper, and for providing a comprehensive insight into security studies as a field. Without his inspirational teaching this paper would have been impossible. I also wish to thank the Department of Political Science and International Studies at the University of Birmingham, under whose auspices this work was undertaken. Professor Colin Hay, Dr Nicola Smith, and Elizabeth Bradley are to be given particular thanks for their support. My gratitude extends to the graduate class of 2002-2003, who provided a forum for conversation and a collective for study. Franz, Audrey, Oh, Nancy, Haiwei, Hisaaki, Alin, Afshan and all the others contributed in different ways to this work.

This paper, and my study at the University of Birmingham, would have been impossible without the teaching, inspiration, and motivation provided by the unsurpassable academic staff at the University of Wolverhampton during my undergraduate degree. Dr Alan Apperly, Dr Darek Galasinski, Dr Mike Cunningham, Dr Martin Durham and Philip Crookes made me what I am.

In addition to the substantial list above, I would also like to thank my mother for believing in me (perhaps too much), my sister for putting up with me, and my uncle, aunt and grandmother for their invaluable support. Finally, let us not forget the heroic Zoe, without whose editing and footnote adventures this paper would be impossible to read.

Thanks guys.

Shane Martin Coughlan, September 2003

Acknowledgements for the Second Edition

In the twelve and a half years since this paper was originally published a lot has changed. My original introduction stated that “Cyber warfare is a relatively new addition to the lexicon of warfare” but this is clearly no longer the case. We live in an age of Digital Warfare and every major government has taken steps to address their national security policy in this context. It is my hope that the Second Edition of this research, released in more formats to allow a broader readership, can contribute to the on-going discourse about how security policy can continually be refined to effectively address digital threats. I would like to thank my colleagues from the class of ’03 for sharing discussions over the years that provided a gentle but consistent reminder of why such activities are important.

Shane Martin Coughlan, March 2016

Table of Contents

"*You still don't know if you're dealing with a kid, organized crime, an intelligence service or an economi*c competitor." [1]

Frank Cilluffo
Senior policy analyst for the Center of Strategic & International Studies

"*It doesn't matter much, does it? If we lose some critical infrastructure, we're still screwed.*" [2]

Ryan Russell
Incident analyst at SecurityFocus.com

[1] Robyn Weisman, "California Power Grid Hack Underscores Threat to U.S." *Newsfactor,* (13 June 2001), http://www.newsfactor.com/perl/story/11220.html.
[2] Ibid.

Abstract

This paper applies a qualitative grounded theory analysis to delineate a common understanding of the constitution of cyber warfare from twelve media, institutional, educational, governmental and military sources. Partly motivating this is the need to address the confusion between cyber warfare and what is termed 'Information Warfare', a broad discipline encompassing all military information operations. Another motivation is the hypothesis that agreement on the constitution, danger and potential of cyber warfare is unsubstantial or vague, that cyber warfare is a misunderstood or neglected concept, and perhaps even suffers from hyperbole and misrepresentation. Though there is a high public awareness of cyber war, there is little attempt to define the concept in existing literature. This paper unpacks the scope, danger and timescale of cyber warfare according to existing texts, and lays the foundation for an analytical framework of patterned and coherent research. In doing so, it uncovers a surprising amount of agreement in the field, and the following definition of cyber warfare emerges from the study:

> *Cyber warfare is symmetric or asymmetric offensive and defensive digital network activity by states or state-like actors, encompassing danger to critical national infrastructure and military systems. It requires a high degree of interdependence between digital networks and infrastructure on the part of the defender, and technological advance on the part of the attacker. It can be understood as a future threat rather than a present one, and fits neatly into the paradigm of Information Warfare.*

Introduction

This paper asks is if there can be a common understanding of cyber warfare. Whether we connect it with C4I[3], regard it as one and same as Information Warfare (IW)[4], or whether we conceive of cyber war as something entirely new, it is important that we establish what is known, what has occurred, and what is projected to occur in the future. This study attempts to define the generally agreed aspects of this new field, and works from the tentative hypothesis that agreement on the constitution, danger and potential of cyber warfare is unsubstantial or vague. This paper asserts that cyber warfare is at best a misunderstood or neglected concept, and at worst, a field that suffers from hyperbole and misrepresentation. This paper will undertake a grounded qualitative analysis of existing texts on the subject of cyber warfare. By identifying common themes linked to cyber warfare, this paper hopes to contribute to the establishment of a common framework for the understanding and research of this new sub-field of security.

Cyber warfare is a relatively new addition to the lexicon of warfare. With the increasing use of computers in military and government, there has been a growing awareness of both a new vulnerability in national infrastructure and a new method of attacking one's enemies. There is the potential of using information systems to protect, control or attack information networks[5]. Cyber warfare could mean winning wars without firing shots, the shutting of entire national infrastructures at the push of a button, and the complete manipulation or destruction of an enemy's communication networks. It could mean threats from across the world by states with no ability to launch a conventional attack, or attacks by non-state actors using cheap laptops. At the extreme end of the literature on the subject, there has been talk of super-viruses shutting down nations, and how a disgruntled individual or small group could wage a 'war' on a nation[6]. Cyber warfare is the new wonder weapon, and the new unknown threat. However, the concept of cyber warfare, and the technology on which it relies, is beset by vague depictions of the dangers it presents, or the benefits it offers.

Cyber warfare is conceptualised by security expert Amit Yoran, newly appointed cyber-security chief at the US Department of Homeland Security[7] and vice-president of computer corporation Symantec, as the future "primary theatre of operations"[8]. US presidential advisor Richard Clarke has said that "In the future, an enemy group, foreigners or Americans, criminals or terrorists, could hurt our

---

[3] C4I stands for Command, Control, Communications, Computers, and Intelligence. More information can be obtained at "What is C4I? Realizing the Potential of C4I: Fundamental Challenges," *c4i.org*, (21 February 2003), http://www.c4i.org/whatsc4i.html.

[4] Information Warfare covers many aspects of the control, manipulation, and deployment of information services for defensive and offensive purposes as demonstrated in "Report of the Defence Science Board Task Force on Information Warfare Defensive (IW-D)," *Cryptome.org*, (8 January 1997), http://cryptome.org/iwd.htm.

[5] See for example the BBC media article "When states go to cyber war,"*BBC News*, (16 February 2000), http://news.bbc.co.uk/1/hi/sci/tech/642867.stm, Timothy Shimeall, Phil Williams and Casey Dunleavy, "Countering Cyber War," *NATO Review* 49 (Winter 2001/2002): 16-18, (online version used available at http://www.nato.int/docu/rev-pdf/eng/0104-en.pdf) , and the anonymous academic article "Cyber War," (n.d.), http://faculty.bus.olemiss.edu/breithel/b620s02/riley/Cyber_War.htm.

[6] Liang Qiao and Xiangsui Wang, "Unrestricted Warfare," *c4i.org,* (February 1999), http://www.c4i.org/unrestricted.pdf.

[7]The Associated Press, "White House Selects Cybersecurity Chief," *The New York Times*, (15 September 2003), http://www.nytimes.com/aponline/technology/AP-Cybersecurity-Chief.html.

[8] "Interview: Amit Yoran," *Frontline: Cyber war!*, (24 April 2003) http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/yoran.html.

economy by shutting down or causing confusion to the systems"[9]. According to Matthew Devost, an anti-terrorism expert based in the USA, the CIA believes at least 100 countries are developing cyber warfare capacity.[10] There is a consensus that cyber warfare is something noteworthy, but it is not clear if this consensus extends to a common understanding of what cyber warfare actually is. It is so new that there is no standard definition to describe it.

This leads to one of the most frequent confusions regarding cyber warfare: its relation to IW. IW is not unproblematic in definition[11], but can be understood as the "offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary's information, information-based processes, information systems, and computer-based networks while protecting one's own"[12]. While IW covers the territory of cyber warfare, it also covers a much broader mandate. Electronic ('cyber') communication is only one aspect of IW, which includes all information operations in a conflict. Chinese strategist Sun Tzu and Napoleonic strategist Carl von Clausewitz referred to information operations, and the importance of such operations in war[13]. IW predates electronic communication, and is not interchangeable with cyber warfare for this reason, though existing literature tends to do so in practice. As the analysis of literature included later in this paper makes clear, this adds greatly to the confusion.

The potential of cyber warfare remains unrealised, and possibly unrealisable, if a clear definition and place for its study and understanding does not exist. Without an agreed framework for examination, cyber warfare will remain no more than a phantom menace, or, more catastrophically, a menace that is hard to contextualise and coordinate research around. The lesson of 9/11 is that such a situation is untenable. Researchers and policy makers cannot ignore the new security issues created by changing technology. Cyber warfare, and the place of technology in combat of all sorts, state and non-state, is one of the most pressing issues for our consideration. It is important that we attempt to contextualise this sub-field as quickly as possible, and to introduce coherent analytical frameworks to its examination.

This study makes a tentative step in trying to establish some conventions in this field. The significance of the study is that it defines the known quantities in cyber warfare, and creates a common understanding of its constitution from publicly available documents. By the conclusion of this paper the reader will have a clearer understanding of what cyber warfare is, how we perceive it, and what issues may arise in the consideration of this topic. Perhaps building from this paper future research might attempt to create empirical indices on confirmed cyber warfare development in Western and non-Western nations. It would be useful to examine the impact of confirmed cyber attacks on critical infrastructure. A US project entitled 'Eligible Receiver' has already begun this process, though it is not exactly clear what occurred

---

[9] "Interview: Richard Clarke," *Frontline: Cyber war!,* (24 April 2003) , http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/clarke.html.

[10] John Lettice, "At least 100 countries building cyber weapons," *SurvivalForum.com,* (24 September 2002), http://www.survivalforum.com/modules.php?name=News&file=article&sid=688.

[11] Michael Patton, "Introduction," *Information Warfare – An Introduction*, (n.d.), http://www.tlc.utexas.edu/courses/tlc321/final/patton/intro.htm.

[12] Ivan Goldberg, *Institute For The Advanced Study Of Information Warfare Page*, (12 March 2003), http://www.psycom.net/iwar.1.html.

[13] Both writers are frequently mentioned in IW literature. An example is in Major Curtis A. Carver Jr., "Information Warfare: Task Force XXI or Task Force Smith?," *Military Review, Command & General Staff College* LXXVIII (1998), http://www-cgsc.army.mil/milrev/English/SepNov98/carver.htm.

during the project, who ran it, and how many people were involved[14]. Eventually we might see the creation of a comprehensive guidebook to cyber warfare occurrences, research, and projected outcomes.

This paper consists of four primary sections. There is a literature analysis to examine existing work regarding cyber warfare, an explanation of the methodology applied to this research, an examination of the results of this research, and a discussion of the implications of the research for cyber warfare and security studies in general. Some aspects of this paper may appear unusual to the reader. One of these is the heavy reliance on sources that are Internet based. Rather than being regarded as careless research, or an experiment in 'post-modern' academia, this choice of sources is reflective of the material available on the topic of cyber warfare. The vast majority of work on the subject is most easily accessed through electronic media, and a substantial amount of the material is only available online. It should be remembered that cyber warfare is a new field, and hardly mature. Thus, the established texts discussing it are limited, and what mention is made of cyber warfare in physical books tends to subsume it into chapters on Information Warfare or network security.

Another perhaps unusual approach is that of the methodology applied to sorting the texts that the author deems as relevant to the research. Qualitative grounded research assumes two primary methods of sifting through material to uncover useful trends, measures or meanings. One is to create units of meaning from the texts examined, and the other is to categorise these units into collections of common importance. Data collection and exploration is inductive in grounded theory, and the research model is evolutionary rather than static. Open sampling may work at the beginning of a study, but moves quickly towards discriminate sampling. Such sampling allows the choosing of people, sites, and documents that enhance the possibility of comparative analysis to saturate the categories of research and complete the study. The study proceeds until there is theoretical saturation; until no new relevant data are discovered regarding a category, and until the categories are well developed and validated. Therefore, the research accomplishes the stated aims in a different way from quantitative studies, eschewing statistical collection in favour of seeking meaning in individual texts.

[14] You can find a collection of the multiple Eligible Receiver 'realities' in Joseph K, "Guide To Tech Terminology," *Crypt Newsletter*, (19 September 2003), http://sun.soci.niu.edu/~crypt/other/eligib.htm.

Analysis of Relevant Literature

The analysis of cyber warfare-related literature is a formidable task. Authors variously identify cyber warfare as network security, as an aspect of the emerging paradigm of IW, as a synonym for IW, and as a blanket term for all technology security and threats. Though there is awareness of a serious threat to networks, there is no framework for the categorisation, classification and examination of cyber warfare and other cyber risks. This paper proposes that until we address this matter, productive further examination of the field will be problematic, and seeks to define a common understanding of cyber warfare. In doing so, it contributes a small fraction of the necessary research for creating an overarching cyber warfare framework, and an even smaller fraction of the research needed for an overarching categorisation of cyber risks. This paper applies grounded analysis to a modest sample of texts to get its results. To provide a context for this research sample there must be a critical examination of a very wide range of sources. There must be a strong foundation through which to introduce the reader to cyber warfare in existing literature, and to build the research model of this paper.

To accomplish this the literature analysis first examines media representation, then institutional representation, then academic, then governmental and finally military. The media help to provide a context for understanding the placement of cyber warfare in public consciousness, while governmental, educational and institutional considerations of cyber warfare have weight as relatively authoritative sources in the making of policy around the subject. This study omits commercial considerations of cyber war because of inherent bias. Companies making security products are unlikely to conclude that such products are unnecessary, and at the same time, commercial examination, such as that of the Pakistani Computer Emergency Response Team, tends to equate cyber warfare with network security[15]. This is understandable given their user base and target market, but is unhelpful in the attempt to understand cyber warfare as a whole. Thus, the literature analysis structure provides an introduction to the perception of cyber warfare, and progresses to detailed understanding and policy formation regarding the issue.

Physical books and papers discussing cyber warfare are rare. This is partly attributable to the relative youth of this aspect of security studies, and partly to the confusion about what it actually is. There is some ambiguity regarding the status of cyber warfare, and different writers categorise it as a subfield of C4I, an aspect of Information Warfare (itself a subfield of C4I in some representations), or as a synonym of Information Warfare. Current writing tends to equate cyber warfare with existing aspects of security study rather than attempt to deal with it directly, and to formulate a comprehensive theory around it. However, unique material on cyber warfare does exist. There is a diverse range of sources available for the consideration of cyber warfare. These sources include media publications, governmental documents (especially from the US government), educational establishments and a slew of non-profit organisations. They are predominantly located online, through government websites, academic sites, and other servers. Therefore, the majority of material used in this paper originates from the Internet.

Most of the cyber warfare texts used in the analysis originate in the USA, and deal with US-centric aspects of cyber conflicts. This is reflective of the public

[15] "The Future of Computers & Internet CyberWarfare??(sic)," *Pakcert.com.pk*, (n.d.), http://www.pakcert.com.pk/cyberwarfare.

material available on the subject. Russia and China are developing policies on cyber warfare, though it is hard to ascertain the exact approach that they are undertaking. Both countries prevent the free availability of documentation that impacts national security. However, important texts are available on cyber war for both countries[16], and these closely mirror the American publications on the subject. The prominence of papers from the USA is to be expected. The USA relies heavily on information technology, and is perhaps the most vulnerable nation to a cyber attack, and the nation in the best position to launch one.

The media, on their part, are aware of the emergence of a new battle space, and refer to it as a potentially catastrophic new threat. Respected news organisations like the British Broadcasting Corporation talk of states going to cyber war[17], and technology magazines like Wired[18] talk of cyber war between the US and China[19]. There exists a public awareness of cyber warfare, though it is based less on studies and research and more on assumption and speculation. The headline story mentioned in the introduction that suggested 100 states were developing cyber warfare capacity[20] is not unique. According to media sources, while rogue states like North Korea are developing cyber warfare units[21], the next cold war is forming around the Internet[22]. Indeed, the media represent cyber warfare as an active part of daily life in security. According to a respected media source, former US president Bill Clinton reportedly ordered the use of hacking against Serbian leaders during the 1998 Kosovo conflict[23], and the CIA supposedly funded efforts to undermine Chinese government censorship of the Internet[24]. Such reporting is not fictional per se, but caution must exist in its interpretation. Glib references about the use of cyber warfare overlook limitations in technological capacity, use, and preparation by nation states. Even the USA, the most technologically advanced nation and the world's largest military spender, has only recently established guidelines for cyber warfare[25]. Media discussion of the subject, like its discussion of so many subjects, can be regarded as generally sensationalist, and originating more in the need to excite an audience than in the desire to reflect accurately a new and barely researched field. Thus, the media are not particularly helpful in working out what cyber warfare is, though they may play an important role in creating the public perception of cyber conflicts or potential.

---

[16] There is CIA translated text from Russia regarding cyber warfare – "Russia: Information War," *Crypt Newsletter*, (7 February 1996), http://www.soci.niu.edu/~crypt/other/boyt.htm - and a translated Chinese text – Major General Pufeng Wang , "The Challenge of Information Warfare," *Institute for National Strategic Studies*, (1995), http://www.fas.org/irp/world/china/docs/iw_mg_wang.htm.

[17] ("When States Go to Cyber War" 2000).

[18] Wired magazine, http://www.wired.com this reference is unnecessary.wired is a well known source

[19] Michelle Delio, "It's (Cyber) War: China vs US," *Wired*, (30 April 2001), http://www.wired.com/news/print/0,1294,43437,00.html.

[20] (Lettice 2002)

[21]" North Korea May Be Training Hackers for Cyber War," *Securesynergy.com*, (17 May 2003), http://www.securesynergy.com/securitynews/newsitems/2003/may-03/170503-01.htm.

[22] Jackie Cohen, "Preparing for World War Web," *CNN.com,* (15 February 1999), http://edition.cnn.com/TECH/computing/9902/15/webwar.idg/index.html

[23] Philip Sherwell, Sasa Nikolic and Julius Strauss, "Clinton Orders 'Cyber-Sabotage' to Oust Serb Leader," Daily Telegraph on *Freerepublic.com*, (7 April 1999), http://www.freerepublic.com/forum/a3780596c7940.htm.

[24] Duncan Campbell, "CIA Funds Cyber War Against Beijing Censor," *Guardian Unlimited*, (1 September 2001), http://www.guardian.co.uk/internetnews/story/0,7369,545238,00.html.

[25] Bradley Graham, "Bush Orders Guidelines for Cyber-Warfare," *Washingtonpost.com*, (7 February 2003), http://www.washingtonpost.com/ac2/wp-dyn/A38110-2003Feb6?language=printer.

There are numerous institutions examining cyber warfare. Some like the Computer Emergency Response Team (CERT)[26], the Center for Strategic and International Studies (CSIS)[27], SANS[28] and RAND[29] are close to the US government affairs. Others like C4I.org[30] and Iwar.org.uk[31] are more independent, though their output may be similar. A characteristic of institutional commentary on cyber warfare is the observation that this new topic is increasingly important in security considerations. One such example of this is the paper '*Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*' by John Lewis of CSIS[32]. A key element of the perceived cyber warfare threat is the danger to critical infrastructure. Electricity, gas and telecommunication and transportation structures are supposedly vulnerable to attack due to their reliance on remote networks and computer controlled systems. A RAND study pointed out that US government and military personnel tended to view "information infrastructure vulnerabilities and the potential for strategic information warfare far more seriously the more they learned about the subject and debated its implications"[33]. However, unlike the media, institutional representations of cyber war tend to err on the side of caution. While they frequently mention the possibility of cyber warfare changing the "function of warfare"[34] or in the way that war occurs, there exist an equal number of clauses stating that though computer networks in general are relatively unsecured, very few critical infrastructures are particularly vulnerable[35]. C4I reproduced an article from the Washington Post[36] that suggested current usage of information technology in the US military spectrum is at best adolescent[37]. While cyber warfare has the potential to become extremely important in defence and offence, it is still at its very early stages. A digital Armageddon is unlikely to happen soon given the combination of lack of information networking, lack of access to critical networks and incompatibility between systems.

The "capability to collect, process, and disseminate an uninterrupted flow of information, while exploiting or denying an adversary's ability to do the same"[38] is regarded as important by institutions. The potential vulnerability of critical infrastructure, the prospect of cyber warfare allowing bloodless and remote engagements, the dangers of other states developing cyber weapons, and the possibility of information control over a conventional battle space are issues too important to be ignored. While decrying earlier research into cyber warfare as too sensationalist or prone to "The Sky Is Falling"[39] sentiment, John Lewis suggests that

---

[26] The CERT homepage is at http://www.cert.org.
[27] The CSIS homepage is at http://www.csis.org.
[28] The SANS homepage is at http://www.sans.org.
[29] The RAND homepage is at http://www.rand.org.
[30] The C4I homepage is at http://www.c4i.org.
[31] The Iwar homepage is at http://www.iwar.org.uk.
[32] James A. Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," *CSIS.org*, (December 2002), http://www.csis.org/tech/0211_lewis.pdf.
[33] "Strategic War... in Cyberspace," *RAND.org*, (January 1996), http://www.rand.org/publications/RB/RB7106/RB7106.html.
[34] (Qiao and Wang 1999)
[35] (Lewis 2002)
[36] Washington Post Online, http://www.washingtonpost.com.
[37] William M. Arkin, "Toys 'R' U.S.," Washingtonpost.com in *c4i.org*, (13 March 2000), http://www.c4i.org/militarytoys.html.
[38] Toshi Yoshihara," Chinese Information Warfare: A Phantom Menace Or Emerging Threat?, " *IWAR.org* , (November 2001), http://www.iwar.org.uk/iwar/resources/china/iw/chininfo.pdf.
[39] (Lewis 2002)

unless increased networking of infrastructure is married with increased security awareness, problems will potentially arise. A separate paper published by CERT suggests that the long-term survivability of the US electronic power system is threatened by insufficient capacity, though it concludes that future research will have to examine the link between information technology and potential weaknesses[40]. Neither paper states cyber threats are an immediate concern, though they both conclude that it is an important future consideration. Cyber warfare is something that we have begun to react to ahead of its time.

In the aftermath of 9/11, such an approach may be prudent, particularly given the recorded consideration or development of cyber corps by potentially hostile nations, and the potential use of cyber attacks by non-state actors. The Federation of American Scientists (FAS)[41] published a translated text from a former director of the Academy of Military Science, Beijing[42]. In it Major General Wang Pufeng suggests that the adoption of information technology and practice into strategic thought will bring about a revolution in military affairs, and the use of such technology will be "highly critical to achieving victory in future wars" for China[43]. A slightly more emotive and far lengthier text from China entitled *Unrestricted Warfare* conceptualises a new type of "unrestricted warfare' in which cyber attacks are an integral part[44] of combat. Though neither text refers to cyber warfare as something currently existent, both regard it as potentially key in securing victory in future wars, especially with a nation like the USA, where asymmetrical conflict is inevitable. Likewise, non-state actors would retain the potential to utilise information systems for an asymmetrical assault. A paper published by the SANS institute concluded that there is the danger of terrorists accessing "the networks controlling dams, air traffic, medical records and nuclear power plants"[45]. While it would be hasty to start unplugging the Internet, foreign research of cyber warfare and the vulnerability of existing and future networks mean that cyber war needs consideration.

It is rare to find a definition for cyber warfare. Of the texts examined only one paper, *Can cyberterrorists actually kill people?*[46], attempts a precise definition of Information Warfare (which it treats as an interchangeable synonym for cyber warfare). Information Warfare is "any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions"[47]. Apart from a horrific use of semi-colons, this definition is less than perfect. Such a definition of Information Warfare includes physical attacks on non-electric information networks, and remains unclear over what an information function is. It is a catchall definition, and relatively meaningless as a result. Institutional papers assume that cyber warfare is a known quantity, envisioned as the use of computers to attack systems relying on computers. They omit specific details that would help to contextualise such occurrences.

Academic texts on cyber warfare do not exist in abundance, and they differ quite substantially from the media texts on the same subject. In academia, the threat of

---

[40] Imju Byon, "Survivability of the U.S. Electric Power Industry," (MSc Thesis, Carnegie Mellon University , 2000), CERT.org, http://www.cert.org/archive/pdf/surv-us-electric-thesis.pdf , 53-54.
[41] The FAS homepage is at http://www.fas.org.
[42] (Wang 1995)
[43] Ibid.
[44] (Qiao and Wang 1999)
[45] Scott Anthony Newton, "Can Cyberterrorists Actually Kill People?," *Sans.org*, (November 2001), http://www.sans.org/rr/paper.php?id=820 ,10.
[46] (Newton 2001)
[47] Ibid. 3

cyber warfare lays in the future, a viewpoint that is similar to institutional representations. Cyber warfare can threaten critical infrastructure, and is a possible tool for use in asymmetric warfare against the USA, or another powerful nation, by either state or terrorist actors[48]. Such a conceptualisation assumes that the United States is unequalled in conventional warfare, and that attacks on critical infrastructure would be effective as a deterrent, or as a "Digital Pearl Harbour"[49]. While the idea of Digital Pearl Harbours is unlikely to attract a particularly serious audience in military affairs, where triple redundancy or greater is the norm, it does strike a nerve with regards potentially vulnerable civilian infrastructure. On the 14th of August 2003 a substantial proportion of the US and Canadian interlinked electricity grid failed, leaving around 50 million people without power, and major cities like New York in darkness[50]. A tree hitting power lines, and the lack of redundancy and fail-safes in an aging network caused the blackout. By combining the highlighted weakness of the network shown on this occasion with the known hack of the Californian power grid in May 2001[51], some form of (civilian) Digital Pearl Harbour is conceivable. Whether such a 'Pearl Harbour' would prove to be fatal or merely annoying is not entirely known, though the logistics of a large-scale attack on any national infrastructure would depend on communications networking on a scale that currently does not exist. Linking cyber warfare and a catastrophic attack on the US naval force during World War 2 is more useful for publicizing the subject than examining it.

A paper by E. Anders Eriksson entitled *Information Warfare: Hype Or Reality*? equates Information Warfare with cyber attacks and discusses how such attacks could be classified[52]. Eriksson says that we live in a network society, characterised by digital networks, modularity, and telematics. The network society is a distinct evolution from the first industrial revolution of steam railways and telegraphs, and the second industrial revolution of electricity, airplanes and television. The networking and communication technology underlying the society allow niche players to gain a voice impossible in the industrial revolutions, and enable high-performance special operations, precision munitions and cyber weapons. The network society is vulnerable to information asset and knowledge attacks, and the technology underlying the society is vulnerable to disruption.

For Eriksson there are two main avenues of cyber threats. One is the use of communication technology for propaganda, coordination and intelligence collection. This use of information technology is regarded as a given[53]. The second is the use of communication technology to directly attack networks like the Internet, or to disrupt a network to disable something that depends on it[54]. The use of information technology to directly attack networks fits two categories. One Eriksson calls Weapons of Mass Disruption (WMD), and the other Weapons of Precise Disruption (WPD)[55]. The names are self explanatory, though the reasoning of such categorisation in IW or cyber warfare is undefined in the author's text. *Information Warfare: Hype Or*

---

[48] Paul Mullin and Tim Thomas, Security AND Foreign Policy in a Cyber-Future, http://www.dean.usma.edu/sosh/conferences/scusa/scusa/Cyber-Future.htm
[49] ("Cyber War")
[50] "Major Power Outage Hits New York, Other Large Cities," *CNN.com*, (15 August 2003), http://edition.cnn.com/2003/US/08/14/power.outage/index.html.
[51] (Weisman 2001)
[52] E. Anders Eriksson, "Information Warfare: Hype Or Reality?," *CNS-The Nonproliferation Review*, 6, 63 (Spring-Summer 1999), http://cns.miis.edu/pubs/npr/vol06/63/erikss63.pdf.
[53] (Eriksson 61)
[54] Ibid.
[55] Ibid.62

Reality? is an interesting paper because it highlights the academic difficulty in conceptualising cyber warfare. Eriksson assumes information network attacks or protection is the most important part of Information Warfare, and reduces the role of passive information operations such as propaganda and intelligence gathering. Furthermore, he neglects to build from a 'real world' framework, and instead arbitrarily identifies certain traits with certain types of society, and proposes unsubstantiated models of potential cyber conflict. Like the documents examined from the media and institutions, Eriksson understands cyber warfare to be a problem, but he is not sure how it will work.

Two reports exemplify this problem. Kings College London published *Information Warfare Attack Assessment System (IWAAS)*[56] and Stanford University *Enlisting Event Patterns for Cyber Battlefield Awareness*[57]. Both papers assume that IW or cyber warfare will consist of network attacks and seek to create frameworks for detecting or countering an intrusion threat. *Information Warfare Attack Assessment System (IWAAS)* identifies increased deregulation and digitalisation of civilian networks and the increased use of civilian or off-the-shelf technology in military systems as vulnerabilities, and reasons for research into "offensive Information Warfare"[58]. The IWAAS attempts to define a state of 'cyberpeace' (a safe level of attacks on the network), and to offer short, medium and long-term assessments of cyber threats[59]. The IWAAS model expands existing intrusion detections models to create a 'warfare' level of national network intrusion. Capabilities, motives, objectives and methods of attack are analysed to allow for the discovery of attack, and the development of a threat awareness report. *Enlisting Event Patterns for Cyber Battlefield Awareness* identifies cyber warfare as a reaction to events in the (undefined) information infrastructure[60], and thereafter concentrates on applying the Stanford University Complex Event Processor to create hierarchies of event occurrences, and to allow a prediction of potential threat to a network. Thus, it creates a hypothetical computer monitoring system to reduce false alarms, increase accurate detection rates, and to discover large intrusion patterns at an early stage. In short, *Enlisting Event Patterns for Cyber Battlefield Awareness* is a guide to better network security. Both papers above are prescriptive, and lack quantitative or qualitative studies to support their assertions. They both define methods of understanding or detecting network intrusions, and assume that such intrusions constitute IW or cyber warfare.

Academic work on cyber warfare is not always so vague in the construction of research models, though prescriptive and assumptive pseudo-research is the norm. Raymond C. Parks and David P. Duggan's *Principles Of Cyber-Warfare* outlines a model for understanding cyber warfare and how it can be contextualised, and makes an effort to differentiate it from traditional warfare[61]. They describe special

---

[56] Andrew Rathmell, Richard Overill and Lorenzo Valeri, "Information Warfare Attack Assessment System (IWAAS)," *International Centre for Security Analysis- Kings College London*, (October 1997), http://www.kcl.ac.uk/orgs/icsa/Old/iwaasppr.PDF.

[57] Louis Perrochon et al., "Enlisting Event Patterns for Cyber Battlefield Awareness," *Program Analysis and Verification Group- CEP*, (January 2000), http://pavg.stanford.edu/cep/Cyberbattlefield.pdf.

[58] (Rathmell, Overill and Valeri 1997:1)

[59] Ibid. 1-2

[60] Ibid. 1

[61] Raymond C. Parks and David P. Duggan, "Principles Of Cyber-Warfare," *Information Technology and Operations Center*, (June 2001), http://www.itoc.usma.edu/Workshop/2001/Authors/Submitted_Abstracts/paperT2C1(10).pdf.

characteristics of cyber space[62] that affect strategic operations. In cyber space distance has little or no meaning, the arena is unreliable, it is hard to hide because of the constitution of the networks, actions have effects that are kinetic and potentially global, and there are no laws of behaviour except when events require a physical world action as well as a digital one. The digital environment requires different methodologies from the physical one to accomplish goals. In cyber conflicts, the attacker and the defender control very small parts of cyber space as a whole, and seek to control the section that their target is using[63]. One important point made by Parks and Duggan is that cyber tools employed in cyber war have dual use. An attacker would use a vulnerability scanner to probe for your weaknesses, and you would do the same to test your security. This is quite different from kinetic weaponry. A physical battle commander is unlikely to "walk out to where he expects the enemy to be and look at his own troops with […] night-vision gear"[64].

Principles Of Cyber-Warfare is useful because it emphasises the difference between digital domain and physical world warfare, and advocates the creation of new frameworks of analysis for cyber study. It stresses that the environment is key to this, and concludes that digital network creation and maintenance by man is rife with imperfections that a more naturally evolving evolutionary communication network would eliminate[65]. The study also places cyber warfare inside the domain of IW, and therefore assumes IW to constitute more than the attack and defence of information networks[66]. However, this paper is still flawed. Though it argues for an understanding of cyber warfare based on the environment in which it operates, the paper does not present any proof of its assertion that in cyber space distance has no relevance, the arena is unreliable, that it is hard to hide and that there are no laws of behaviour. Similarly, there is no attempt to define cyber warfare explicitly, or to define the constitution of IW. Assumption and assertion have priority over research and analytical examination.

It is not surprising that the majority of texts discussing cyber warfare originate from governmental and military sources. There is a perceived vulnerability of "critical information infrastructure to a potentially devastating high tech attack"[67]. Lawrence K. Gershwin, US National Intelligence Officer for Science and Technology, says an attack on "military, economic, or telecommunications infrastructure can be launched from anywhere in the world [against] America's heartland"[68]. He conceives states as the primary cyber threat, with terrorism, organised crime and protest groups or individuals also providing serious challenges to infrastructure safety. Policy makers regard cyber warfare as real, and some suggest that it is as dangerous as Weapons of Mass Destruction (WMD) or international terrorism. The director of the CIA said

---

[62] Cyber space is the digital arena that networks can be understood to create

[63] They can do so by assuming the identity of the legitimate authority of that section. This is possible because there is no such thing as hinterland in cyber space. Every part of the network is 'owned' by someone, and by pretending to be him or her, you can operate in their space. For more information see Parks and Duggan , 2001.

[64] (Parks and Duggan , 2001:124)

[65] Ibid. 125

[66] Ibid.

[67] "Testimony by Director of Central Intelligence George J. Tenet Before the Senate Committee on Government Affairs," *CIA- Speeches and Testimony*, (24 June 1998), http://www.cia.gov/cia/public_affairs/speeches/1998/dci_testimony_062498.html.

[68] Lawrence K. Gershwin, "Statement for the Record for the Joint Economic Committee- Cyber Threat Trends and US Network Security," *CIA- Speeches and Testimony*, (21 June 2001) http://www.odci.gov/cia/public_affairs/speeches/2001/gershwin_speech_06222001.html

"information warfare has the potential to deal a crippling blow to our national security if we do not take strong measures to counter it"[69]. Media regard cyber warfare as something glamorous and new, institutions regard it as something meriting examination, and academics see it as an interesting new research topic. For governmental and military sources, it is something quite different. It is a threat to the homeland security of a nation, and a complicating factor in the ability of a nation to project force externally. Whether cyber warfare is understood to be exclusively network attack and defence, or is regarded as a blanket term for all information operations (being seen as interchangeable with the term Information Warfare), it is a security imperative.

Governmental documents on cyber warfare and IW are rife. Defence Secretary Cohen suggested that the USA's superpower status could attract cyber warfare threats[70]. General Richard Myers of US Space Command confirmed that cyber warfare is a way of "asymmetrically perhaps, attacking adversaries", and emphasises US military awareness of the issue[71]. CIA official John Serabian even asserted that "Information warfare [...] has the potential "to deal a crippling blow" to U.S. national security"[72]. While displaying similar concerns about IW or cyber warfare, such documents also highlight the uncertainty over what such an attack would consist of, or who would launch it. Serabian defines IW as interference with government and industry computers to attack critical infrastructure, and therefore equates network security with cyber protection or counter-IW operations. He also connects IW with agents beyond states, and includes terrorist activity in his definition[73]. Defence Secretary Cohen and General Myers both talk about cyber warfare as something that a weaker state could use as an advantage in a military situation. If Serabian and Cohen/Myers are referring to the same issue, then terrorism is the same as state warfare, which confuses the traditional definition of what constitutes a war.

These writings understand that "Computers are the weapons and the Front Line is everywhere"[74] in a future of IW, though the exact way that such warfare will unfold is undefined. To divine a common understanding of the way that computers, networks and security may work there have been a number of combined exercises, including seminar games[75], discussions with non-governmental experts[76], and public

---

[69] ("Testimony by Director of Central Intelligence George J. Tenet Before the Senate Committee on Government Affairs" 1998)

[70] "Cohen Says "Superpower" Label Attracts Asymmetrical Threats," *U.S. Embassy, Islamabad,Pakistan Page*, (23 August 2000), http://usembassy.state.gov/posts/pk1/wwwh00082302.html.

[71] " Pentagon Briefing on U.S. Space Command", *Department of State Washington File, U.S. Embassy Australia Page*, (5 January 2000), http://usembassy-australia.state.gov/hyper/2000/0105/epf302.htm.

[72] "CIA Official Assesses Information Warfare Threat," *USIS Washington File, U.S. Embassy Australia Page,* (10 December 1998), http://usembassy-australia.state.gov/hyper/WF981210/epf406.htm.

[73] ("CIA Official Assesses Information Warfare Threat" 1998)

[74] Susan Ellis, "Computers Are Weapons In Potential Cyber Attacks," *USIS Washington File, U.S.Embassy Australia Page*, (25 August 1998), http://usembassy-australia.state.gov/hyper/WF980825/epf206.htm.

[75] "Business Process and Procedures for Tomorrow's Wars: The Results of Defense Reform Initiative: Seminar Game 00," *Defense Reform,* (March 2001), http://www.dod.mil/dodreform/briefs/seminargame2000.pdf.

[76] "Global Trends 2015: A Dialogue About the Future With Nongovernment Experts," *DCI/CIA-Reports*, (December 2000) http://www.odci.gov/cia/reports/globaltrends2015/index.html.

statements by intelligence sources[77]. The CIA has been able to confirm "the appearance of doctrine and dedicated offensive cyber warfare programs in other countries", and identified the openness of the US digital infrastructure as a source of strength and at the same time, a key weakness with regards attacks and intelligence[78]. *Global Trends*, a document prepared in consultation with non-governmental experts, reiterated the potential weakness of digital infrastructure to attacks by terrorists or enemy states, though "whether cyber warfare will ever evolve into a decisive combat arm" is still unknown[79].

Fuelling the consideration of cyber warfare are two identified trends. One is the rise of both the terrorist threat and their potential use of cyber tools[80], and the other is the formation of cyber warfare policies in other nations[81]. Since 1998, terrorism and computer security has been scrutinised[82], and in the aftermath of 9/11 terrorist threats have gained a new importance in security considerations. US sources believe that "adversaries will engage asymmetrically, within and across our borders"[83]. While terrorist cyber attacks are not an imminent problem for the US, there is a desire to raise public consciousness of their possibility[84]. Organisations like Al-Qaida remain the greatest officially recognised threat to the US[85], and the relatively low investment of manpower, resources and money that a cyber attack requires may be attractive to them. Likewise, the active and public development of cyber warfare rhetoric by China causes concern in the USA[86], and prompts further discussion about cyber policy and potential dangers.

Two of the most influential documents on cyber warfare are US Presidential Decision Directives 62[87] and 63[88] released May 1998 as part of the Clinton Administration's commitment to security. PDD 62 is concerned with countering terrorism in the 21st century, and explicitly identifies the need to protect "the computer-based systems that lie at the heart of America's economy"[89]. It says government agencies must adopt a unified approach to anti-terrorism to protect national infrastructure. To accomplish this PDD 62 mandates the creation of a

---

[77] John C. Gannon, "Intelligence Challenges Through 2015," *DCI/CIA- Speeches & Testimony*, (7 April 2000), http://www.odci.gov/cia/public_affairs/speeches/2000/gannon_speech_05022000.html and, Gershwin 2001.
[78] (Gannon 2000)
[79] ("Global Trends 2015: A Dialogue About the Future With Nongovernment Experts" 2000)
[80] "National Strategy For Combating Terrorism,"*U.S. Embassy India Page*, (February 2003), http://usembassy.state.gov/posts/in3/wwwfns.pdf.
[81] "Japanese Newsletter on Taiwan Information Defense Concerns," U.S. Embassy China, (30 June 2003), http://www.usembassy-china.org.cn/sandt/taiinfowar.html.
[82] Jennifer Coffey, "FBI Sees Increase In Threat Of Cyber-Terrorism," *USIS Washington File, U.S. Embassy Australia Page*, (17 April 1998), http://usembassy-australia.state.gov/hyper/WF980417/epf512.htm.
[83] ("National Strategy For Combating Terrorism" 2003:25)
[84] "Transcript: Reno, Shalala, Clarke 1/22 Briefing On Terrorism," *USIS Washington File, U.S. Embassy Australia Page*, (22 January 1999), http://usembassy-australia.state.gov/hyper/WF990122/epf505.htm.
[85] "Al-Qaida Still Presents Greatest Threat to U.S., CIA Head Says," *U.S. Embassy Pakistan Page*, (20 March 2002), http://usembassy.state.gov/islamabad/wwwh02032002.html.
[86] "Byrd's Remarks Before U.S.-China Security Review Commission," *U.S. Embassy Japan Page*, (14 June 2001), http://usembassy.state.gov/posts/ja1/wwwhse0202.html.
[87] The White House, " Presidential Decision Directive 62," *FAS.org*, (22 May 1998), http://www.fas.org/irp/offdocs/pdd-62.htm.
[88] The White House, "Presidential Decision Directive/NSC-63," *FAS.org*, (22 May 1998), http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.
[89] ("Presidential Decision Directive 62" 1998)

National Coordinator for Security, Infrastructure Protection and Counter-Terrorism. The National Coordinator acts as a liaison and overseer of policy in anti-terrorism, infrastructure protection and security. PDD 63 is concerned with critical infrastructure protection, and identifies "vulnerabilities to equipment failure, human error, weather and other natural causes, and physical and cyber attacks" that need to be addressed[90]. It is a much larger document than PDD 62, and makes several important policy decisions. A goal of initial infrastructure protection is set for the year 2000, and by 2003 a certain minimal level of safety or recoverability is planned. Inter-governmental agency cooperation is to be increased, and a partnership between public and private industry is called for through the creation of the National Infrastructure Assurance Council. Furthermore, the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism will create an Information Sharing and Analysis Center (ISAC) to allow full public/private cooperation in infrastructure protection. PDD 62 and 63 thus identify the possibility of attacks on critical infrastructure either from terrorism (PDD 62) or from a more diverse range of sources (PDD 63). A focus on infrastructure protection continues in the Bush presidency, and is an imperative after 9/11. Executive Order 13231 reinforced the commitment to such protection, and specifically the protection of information networks[91].

PDD 62, 63 and E.O. 13231 implicitly characterised cyber threats as any attack on systems that were essential to normal national infrastructure operation. Thus, terrorism, state-sponsored attacks and even individuals hacking into systems were characterised as belonging to the same category. The goal of these high level documents was not to define cyber warfare, or IW, but to provide a framework for implementing some form of national cyber security. In common with academic documents and those produced by institutions, governmental publications display abstract concern for potential vulnerabilities rather than proven problems backed by empirical data. The threat is vague, the potential cost of an attack unquantifiable, and the understanding of the phenomenon of cyber warfare remains subsumed beneath a keenness to pre-empt any effect it may have. Other writings do not simplify matters. They treat cyber warfare and IW as interchangeable terms, assume the primary aspect of both fields is network security or defence, and therefore inherently focus on the potential effect of attacks instead of how we could understand such attacks. By concentrating largely on opinion rather than empirical study, such studies neglect to create an analytical framework through which we can effectively classify and research cyber events. The vagueness of their definitions is unhelpful in assessing true levels of danger.

Cyber warfare and IW remain relatively unknown quantities in all aspect of research, analysis and policy formation. While practical tests of infrastructure protection have taken place, most notably in the form of 'Eligible Receiver'[92], no proof positive of threat levels is available. Even 'Eligible Receiver' is unhelpful. Allegedly, it was a simulation where US agents posing as agents of a hostile power supposedly broke "into the power grids of all the major American cities from Los Angeles to Chicago to Washington, D.C., to New York"[93]. However, as mentioned in the introduction, no two sources have been able to relate the events of the experiment

[90] ("Presidential Decision Directive/NSC-63" 1998)
[91] John D. Moteff, "Critical Infrastructures: Background, Policy, and Implementation," *Foreign Press Centers, U.S. Department of State*, (4 February 2002), http://fpc.state.gov/documents/organization/8087.pdf.
[92] (Joseph K 2003)
[93] (Ellis 1998)

in the same way[94]. 'Eligible Receiver's utility outside of propaganda is uncertain, and it contributes little more than hype and scaremongering to the public debate on cyber warfare.

This paper argues that cyber warfare needs to be explicitly defined to reduce the underlying confusion over its place inside the security lexicon. Currently cyber warfare potentially encompasses all electronic and non-electronic information attacks, regardless of their seriousness, origin, or implementation. In this bizarre situation two problems occur, one tied to the word 'warfare', and the other to the word 'cyber'. Firstly, if the definition of cyber warfare includes the actions of individuals, interest groups, terrorists and nations then an individual can wage 'war' against a state. While 'war' can mean conflict between any two parties[95], in general practice it tends to indicate state conflicts. If cyber warfare includes all conflicts between all types of party, it complicates immensely the definition of war itself. The same definitional problem exists with the use of the term 'Information Warfare' to describe all information operations, though it is irrelevant to the purposes of this paper. Secondly, it is not clear if cyber warfare is exclusively linked to network attacks and defence. Governmental, academic, and institutional texts arbitrarily place cyber warfare inside IW, or regarding it as a synonym for IW. This practice is unhelpful for both IW and cyber warfare. Information Warfare is the utilisation of information in battle space, be it physical, digital or otherwise. Conversely, cyber warfare implies a focus on electronics by its use of the word 'cyber'. According to the Collins English Dictionary, 'cyber' indicates computers[96]. It is derivative of the word 'cybernetic', which Norman Wiener created in 1947 to describe a field that combined electrical engineering, mathematics, biology, neurophysiology, anthropology, and psychology[97]. By confusing the terms, authors inadvertently tie IW to electronic warfare though it has a much broader mandate, and expand electronic or 'cyber' operations to cover all aspects of human communication.

The failure to create a coherent definition of cyber warfare prevents effective studies of it, and the creation of methods of classifying cybernetic attacks. The term becomes little more than a blanket phrase that potentially covers all aspects of digital and physical information security. 'Information Warfare' is a far better phrase for this, and is an already well-established aspect of security analysis.

---

[94] (Joseph K 2003)
[95] Definition of the word 'war' found at *Wordreference.com*, (n.d.), http://www.wordreference.com/english/definition.asp?en=war.
[96] Definition of the word 'cyber', *Wordreference.com* (n.d.), http://www.wordreference.com/english/definition.asp?en=cyber.
[97] "Cybernetics: A Definition- Entry in Macmillan Encyclopedia of Computers, 1991," *Pangaro.com*, (n.d.), http://www.pangaro.com/published/cyber-macmillan.html.

Methodology of Research

The literature analysis above shows the definition of cyber warfare in current research and policy documents to be insubstantial and confusing. By distilling a common series of perceptions on the subject, this paper seeks to mediate the confusion, and create a common understanding of what constitutes cyber warfare. Rather than attempting to fabricate a 'new' definition of cyber warfare, this paper culls one from existing public documents. This ensures the validity and applicability of research results, at least in relation to existent material. The aim is to contribute the first step towards creating an analytical framework of cyber warfare. To accomplish this objective a qualitative analytical model using grounded theory is favoured over qualitative approaches.

This type of study is inductive, and the research model evolves during the collection and exploration of data. The intention is to choose people, sites, and documents that enhance the possibility of comparative analysis, and to allow the creation of categories through which to classify them. When the categories are well developed and validated there is theoretical saturation, and the study concludes. This type of study may initially utilise indiscriminate sampling methods, but quickly adopts targeted sampling. The aim is to find and explore texts that are useful for answering the research questions, rather than indiscriminately sampling large amounts of material. As such, it is a quite different approach from those adopted in quantitative studies. General research guides[98] and specific papers [99] often refer to grounded theory analytical approaches. Previous studies using grounded theory include examinations of beer consumption in Australia [100], examinations of healthcare in the UK [101], examinations of the impact of equal opportunity officers in universities [102] and a military study into the effects of stress on leadership [103]. Thus, it is both well established and proven as a methodology. It is highly flexible, and offers great utility in exploratory research such as the one contained in this paper.

The qualitative approach to the research question, and the use of grounded theory to analyse the subject material, ensures the greatest possible utility and validity of research results. Qualitative research allows a 'deep' reading of texts, and is uniquely appropriate to decoding the perceptions underlying assertions. Quantitative research would be ill suited to this task. Until definitions exist through which we can classify cyber warfare, the applicability of quantitative research methods is limited. Later, when there is a normative framework for understanding cyber warfare, the

---

[98] Kjell Erik Rudestam and Rae R. Newton , *Surviving Your Dissertation – A Comprehensive Guide To Content And Process, 2nd ed*., (London: Sage, 2001).

[99] Bob Dick, "Grounded Theory: A Thumbnail Sketch," *Resource Papers in Action Research, Graduate College of Management, Southern Cross University, Australia*, (2002), http://www.scu.edu.au/schools/gcm/ar/arp/grounded.html.

[100] Simone Pettigrew, "A Grounded Theory of Beer Consumption in Australia," Qualitative Market Research: An International Journal 5, no. 2 (2002) at *Emerald*, http://www.emeraldinsight.com/pdfs/awards2003/qmr.pdf.

[101] Abdullah A. Akbar, " 'Pay-per-use' Concept in Healthcare: A Grounded Theory Perspective," *IEEE Computer Society*, (2002), http://dlib2.computer.org/conferen/hicss/1874/pdf/187460169a.pdf?SMSESSION=NO.

[102] Ann Joan Burrett, "Picking The Pitch: A Grounded Theory Study Of The Impact Of Equal Opportunity Officers On The Culture Of Universities," (Ph.D. thesis, Southern Cross University, 2002), http://thesis.scu.edu.au/adt-NSCU/uploads/approved/adt-NSCU20020926.105835/public/01front.pdf.

[103] Gerry Larsson et al., "Leadership Under Severe Stress: A Grounded Theory Study," AU-24 Concepts for Air Force Leadership, (2001), http://www.au.af.mil/au/awc/awcgate/au-24/larsson2.pdf.

quantitative focus on statistical data will be useful in identifying patterns of attacks. This paper uses grounded theory to allow for the creation of a simple categorisation of research that is easy to replicate and verify. Categories are defined according to their utility in accomplishing the inquiry aims, and source research data are ordered and sorted into them. This approach ensures the reading of the source research data is highly ordered and methodological.

Because of the wide breadth, if not depth, of the discussion surrounding cyber warfare this paper is selective in its use of research material. Authority and credibility is vital in the source material for the research, especially if the results obtained are to have applicability beyond this paper. Thus, while acknowledging that there is a wide range of material in media, institutional, academic, governmental and military settings, this research will use only a small sample as its source. Articles included in the study originate from reputable media organisations, verifiable institutions, academics based at world-renowned educational establishments, and US, Chinese, Russian or NATO government and military sources.

Reputable media organisations include those that are well established, have verifiable ownership, and possess a reputation for journalistic credibility. Examples of these would be the BBC and CNN. The above criteria exclude Internet-only media organisations. Verifiable institutional sources include those that have strong ties to the academic world or governments, and have a reputation for publishing critical and authoritative works. Examples of these would be CERT, FAS, CSIS and RAND. The above criteria exclude less high-profile institutions. Academic writings from world-renowned educational establishments include educational organisations or figures that have credentials that transcend national borders. Examples of these would be institutions like Kings College London, Stanford University, or US and EU government-sponsored research programs. The above criteria exclude information originating on educational servers but lacking obvious linkage to the larger programs or the institution that hosts the content (such as the article "Cyber War'[104]). US, Chinese, Russian and NATO government or military articles included in the research are filtered with the proviso that they should originate from high-level sources and have high visibility. Because of this proviso, there is a reasonable chance that they will be representative of larger policy discussions occurring inside these governmental and military organisations.

Since this research seeks to provide an initial definition of cyber warfare rather than attempting the creation of a full analytical model, the size of the source material sample will be limited. Constructing the sample consists of two inquiry phases. The first, which was undertaken in order to allow the creation of the above literature analysis, involves reading and critically examining a wide range of material from each of the defined fields: media, institutions, education, government and military. This process acts as a filter mechanism to allow the author to gain a greater understanding of writings on the topic. The second phase of the sampling involves selecting a limited number of articles from each of the defined fields to allow the application of grounded theory. Two media articles, two institutional articles, two educational articles, two articles each from US and Chinese government or military sources, and one article each from Russian and NATO government or military sources are selected according to two criteria; the reputability of the source and the relevance of the article to cyber warfare. The relevance of the article to cyber warfare is determined by how many times it refers to the topic explicitly.

[104] ("Cyber War")

Once the source articles are located, a grounded data analysis procedure is applied. This consists of three phases. The first is open coding, where texts undergo review to allow the creation of descriptive categories. Units of knowledge are identified in each text, and are categorised with similar units from other texts to fit 'types'. The second phase is axial coding, where the categorised units undergo analysis to identify properties, and are compared with other units to uncover trends. The final phase is selective coding, where certain trends are identified as central, and a theoretical model is generated to relate the other trends to it according to how they influence it, are caused by it, provide a context for it, or mediate it. When all data identified into units fit a category, the rules for inclusion and exclusion into categories work, and the research concludes.

Initial examination of the twelve source texts suggests three main categories of analysis. The first category determines the scope of cyber warfare. To define cyber warfare we must define the area in which it operates. Thus, this category examines whether cyber warfare is limited to network security, or covers all information operations (and is it therefore a synonym for IW). The second category determines the threat that cyber warfare presents. It examines the perceived danger to national critical infrastructures, military systems, and the potential of cyber warfare allowing conventionally weak nations or groups to gain effective asymmetric warfare. The final category is the smallest, and delineates the perceived timescale of cyber threats. It determines if cyber warfare is a problem for the present, or if it is something that lies in the future.

There are three questions used to determine **the scope of cyber warfare**. The first asks if offensive and defensive digital actions are cyber warfare or Information Warfare. The literature analysis highlighted the lack of delineation between cyber warfare and IW. The lack of clarity over whether cyber warfare is a synonym for IW or an aspect of IW operations is a major problem in existing publications. The second question asks if cyber warfare is limited to network attacks, or if it includes all information operations. In texts that make explicit reference to cyber warfare, the scope of the threat must be determined. This question asks if cyber warfare is a synonym for IW. If cyber warfare includes all information operations, it is merely IW relabelled. The third question asks if cyber warfare is something only nations can do. The connection between cyber warfare and non-state actors would indicate that the term is inappropriately used. This question helps us understand if cyber warfare is a term for all types of cyber attack (and thus not representative of 'warfare'), or if it describes only military information operations.

There are three questions used to determine **the level of danger cyber warfare presents**. The first asks if cyber warfare is a real threat to infrastructure. The introduction to this paper mentioned the possibility of cyber attacks effectively shutting down entire nations, and there is no doubt that perceived danger to national infrastructure is a key element in discourse surrounding cyber warfare. By defining the perceived plausibility of this assertion, it is possible to begin to create a measure of the threat faced. The second question asks if cyber warfare is a threat to military systems. There is a substantial difference between a threat to civilian and military infrastructure. It is possible that attacks on the infrastructure of a nation could leave its military capacity relatively unharmed, and allow conventional weaponry retaliation to a cyber attack. However, if cyber warfare is a threat to military infrastructure it becomes a very serious problem indeed. The third question asks if cyber warfare will 'level the playing field' in asymmetric warfare. The literature review mentioned the asymmetric use of cyber warfare by weak nations to challenge nations that are more

powerful. For developing nations or small states, cyber warfare might be a way to attack a superpower like the USA.

There is one question used in determining **the timescale of the threat**. It asks if cyber warfare is a current problem, or a future one. The lack of clarity surrounding the answer to this question contributes to the confusion about how to address this issue.

To ensure the internal validity of this research the analysis model requires triangulation of material through related text confirmation. The data sourcing ensures that though the sample size is small there are two examples of each source type, and the breadth of the sampling ensures that multiple potential representations of the subject matter are possible. The credible sampling employed with this research also ensures high external validity. The research aims are modest, and this paper does not claim to provide a new model or definition for cyber warfare. The examination of material from multiple sources that possess high validity creates an amalgamated basic definition of cyber warfare that is applicable to further research.

Results of Research

This chapter presents the results of the seven research questions in a relatively unembellished manner, and a more exploratory discussion of trends or issues uncovered is left to the chapter following. This delineates more clearly between raw data results and (potentially) subjective interpretations of such data. While such methodology does little to increase the validity of any research results, it is aesthetically pleasing to the author. This chapter contains the results of the seven research questions, and a brief examination of how they help to define the scope, danger and timescale of cyber warfare. Using these findings, it then offers a potential definition of cyber warfare. There is a table listing the title and original location of each of the twelve sources used in the model in appendix 1 of this paper, and there is a table summarising the results of the seven research questions in appendix 2. There is also a CD ROM included in appendix three, and it contains digital copies of each source text. The next chapter contains a discussion of the implications of the findings.

The first question applied to the source texts distinguishes between those that refer to cyber warfare directly, or use another term such as IW to describe information operations. Six out of the twelve articles refer directly to cyber warfare, five refer to IW, and one refers to the possibility of an unnamed type of war on the Internet[105]. The media articles are both extremely speculative, with the BBC examining a hypothetical war in 2015[106] and CNN suggesting the next world war could be Internet based[107]. This is distinct from the patterned usage of the terms cyber warfare and IW in the institutional, educational, government and military sources. While maintaining exploratory elements, these articles are more descriptive of the problems and benefit that cyber warfare or IW will bring. Their focus is on building theory or policy-related understandings of the paradigm. Thus, an initial pattern emerges showing roughly half the texts to name cyber warfare directly, and half to use the term IW. This is consistent with the documents encountered in the analysis of literature, and symptomatic of the lack of clear definition for the field.

The second question applied to the source texts distinguishes between those that limit cyber warfare to digital network security, and those that describe it as covering all information operations. Eight articles explicitly link cyber warfare to network attacks, three regard it primarily a network security arena, and only one refers to all information operations. In combination with the results obtained from the first question, it becomes clear that articles that count cyber warfare or IW as broader than network attacks are those that originate from government or military sources in China and Russia. These articles do not name cyber warfare, but regard all information activity as IW, even if such activity is primarily connected to digital networks[108]. Perhaps more interestingly, half of the institutional[109] and half of the educational[110] sources examined regard IW as connected exclusively to network security. This is consistent with the previously noted confusion over the use of the term IW. While government and military sources appear to regard IW as covering all

[105] (Cohen 1999)
[106] ("When States Go to Cyber-War" 2000)
[107] (Cohen 1999)
[108] See for example the two Chinese texts on IW: "The Challenge Of Information Warfare," (Wang 1995) and Senior Colonel Baocun Wang and Fei Li ,"Information Warfare," *Institute for National Strategic Studies*, (June 1995), http://www.fas.org/irp/world/china/docs/iw_wang.htm.
[109](" Strategic War... in Cyberspace" 1996)
[110] (Eriksson 1999)

information operations and cyber warfare as being network related, no such distinction appears to exist in institutional and academic enquiry.

The third question applied to the source texts distinguishes between those that limit cyber warfare to states, and those that describe it as something that non-state actors could utilise. Six articles regard cyber warfare as the domain of states, two clearly differentiate between state and 'cyber terrorism' threats, three primarily link it with states, and only one regards it as connected with all potential actors[111]. The institutional text[112] and US governmental text[113] that differentiate between cyber warfare and cyber terrorism implicitly regard cyber warfare as the domain of states. The two media and one institutional texts that did not explicitly limit cyber warfare to states, presumed a digital battlefield would consist of such actors. The remaining US governmental article that links cyber warfare (using the term "cyber threats"[114]) to non-state actors is therefore an anomaly in our analysis. Thus, the confusion about the usage of the term 'warfare' to describe actions by non-state actors is less prevalent than initial analysis of the literature suggests.

These three questions show that the **scope of cyber warfare** is limited in practice to network attacks, though confusion of the term with IW (and the larger scope of IW) does lead to exceptions. Cyber warfare is also limited to actions by state actors, with different terms used to describe cyber activities by other actors. The results of the research in this category reveal that confusion over the scope of cyber warfare, and use of the term 'warfare' to mean actions by non-state actors, is minimal. Cyber warfare is effectively conceptualised to mean digital network activity by states.

The fourth question applied to the source texts distinguishes between those that regard cyber warfare as a real threat to critical national infrastructure of states, and those that do not. Eleven articles regard cyber warfare as a threat to infrastructure, and one believes it is not[115]. It is interesting to note that the one paper that believes cyber warfare poses no danger is from an institutional source, while all governmental and military papers explicitly agree that cyber warfare (and IW) is a threat. Thus, regardless of the use of the term cyber warfare or IW, and regardless of whether it is linked to state or non-state actors, cyber warfare is seen as a serious threat to state security.

The fifth question applied to the source texts distinguishes between those that regard cyber warfare as a threat to the military infrastructure of states, and those that do not. Nine articles explicitly regard cyber warfare as dangerous to military infrastructure, one regards it as a danger but is unclear to what extent[116], one implies a danger to military systems, and only one paper does not[117]. The paper that disregards cyber warfare as a military threat is the same institutional paper that disregarded it as a threat to national infrastructure[118]. The reason for its individuality lies in its strict differentiation between network security and infrastructure security. This leads to the assertion that "while many computer networks remain very vulnerable to attack, few

---

[111] John A. Serabian Jr., "Cyber Threats and the U.S. Economy," *DCI/CIA- Speeches and Testimony*, (23 February 2000), http://www.odci.gov/cia/public_affairs/speeches/2000/cyberthreats_022300.html.
[112] (Lewis 2002)
[113] "DoD CIO Annual Information Assurance Report," *DoD/DIAP,* (April 2002), http://www.dod.mil/nii/org/sio/ia/diap/documents/PUBLIC_CIO_IA-AnRpt_1999.pdf.
[114] (Serabian 2000)
[115] (Lewis 2002)
[116] (Serabian 2000)
[117] (Lewis 2002)
[118] Ibid.

critical infrastructures are equally vulnerable"[119]. In the other texts examined, there is no distinction between computer networks and critical infrastructure, and this may partly explain the confusion in two of the other texts over what type of danger cyber warfare presents. However, as with critical infrastructure, cyber warfare is regarded as a threat to military infrastructure by all governmental and military sources.

The sixth question applied to the source texts distinguishes between those that regard cyber warfare as being of use to 'level the playing field' in asymmetric warfare, and those that do not. Six articles do not mention the possibility of cyber warfare being used in asymmetric conflict, three lack specific reference to asymmetric warfare but suggest cyber warfare methods that would imply such use, and two make explicit reference to asymmetric potential. The two articles that perceive asymmetric potential in cyber warfare are from government or military sources[120], as is the article that suggests implicitly that cyber forces will have a substantial advantage over traditional forces[121]. Thus, while the majority of source material ignores or lacks any explicit reference to asymmetric uses of cyber warfare, there is some examination of its potential.

These three questions show that the **level of danger cyber warfare presents** includes the potential to disrupt both critical national infrastructure and military systems. Cyber warfare is also potentially useful for conventionally weak states to attack strong states. The results of the research in this category are conclusive in showing that a broad range of sources almost universally believe cyber warfare is a very serious security issue.

The seventh question applied to the source texts distinguishes between those that regard cyber warfare as being a future threat, and those that regard it as a current problem. Nine articles regard cyber warfare as a future threat, three as a current threat, and one as a threat that exists in some measure today and will get increasingly important[122]. While one institutional, one educational, one governmental and one military text believe that cyber warfare exists to some extent today, the majority see it as a problem that lies ahead. The results obtained through question two reinforce this by showing the majority of texts regarded cyber warfare as network security. Outside the USA, the immediate danger of network attacks is low because large-scale computer networking of critical systems in both civilian and military infrastructures being in relative infancy. Even inside the USA, as pointed out by one of the institutional articles[123], the connection between networks and infrastructure is tenuous. Thus, while cyber warfare is dangerous to both civilian and military networks in the eyes of most authors examined, it is not an immediate problem.

This question shows that the **timescale of the threat** places it in the future. Cyber warfare is an emerging problem, though it is not generally regarded as a present issue. The results of the research in this category are conclusive in showing that a broad range of sources believe cyber warfare is a problem that lies ahead, and is dependent on increased networking of infrastructure both in civilian and military systems.

Certain patterns emerged from the analysis of the research material. The most explicit patterns include the use of cyber warfare to mean network security, the association between cyber warfare and states, and the belief that cyber warfare poses a

[119] Ibid. 1
[120] (Serabian 2000; Wang
[121] (Wang and Li 1995)
[122] ("Strategic War... in Cyberspace" 1996)
[123] (Lewis 2002)

threat to critical national infrastructure and military services. Asymmetric warfare, when mentioned, is complimentary to cyber warfare. There is agreement that cyber warfare will be important and highly dangerous, but it is dependent on the emergence of increased networking in societies, and the ability of an attacking state to exploit existing network vulnerabilities.

The predicted confusion over the use of the terms cyber warfare and IW is present in the sample. The media, institutional and academic texts understand both cyber warfare and IW to mean network security. This confusion is absent in governmental and military texts, where the two terms are more clearly delineated. Perhaps there is a lack of engagement between non-governmental fields and the field of military research, where IW is categorised carefully, and subsumed into the larger literature covering topics such as C4I and the Revolution in Military Affairs (RMA).

The predicted confusion over the use of the term 'warfare' to mean actions by non-state actors is almost totally absent from the sample. Only one source connects cyber threats to all actors, and while it does not differentiate between state and non-state cyber threats, it does not explicitly state that cyber warfare can be used as a term for them all[124]. Given the use of the term cyber terrorism in several of the sample texts, and the separate use of the term cyber crime in articles related to network security[125], there are some indications of the emergence of a 'family' of differentiated cyber events. Thus, cyber warfare is something that states do, and there are other terms for different types of cyber threat.

The distillation of a common understanding of what constitutes cyber warfare from the source texts is possible, though the results are not unanimous.

Firstly, we must define IW to differentiate it from cyber warfare, and to allow us to place our defined cyber warfare into context with IW. IW is defined in this paper as "offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary's information, information-based processes, information systems, and computer-based networks while protecting one's own"[126]. Cyber warfare is different from IW because the sources examined have a virtually exclusive conception of it as digital network security. If anything, cyber warfare is a subset of IW, fitting under the information operations umbrella beside physical information operations and non-computer electronic information operations.

Secondly, using the material divined from the source material we can expand on cyber warfare now that we understand it to consist of network security. The research sample reveals cyber warfare is network security undertaken by a state to defend or attack another state (or state-like) actor. The sample shows cyber warfare to be perceived as a threat to both critical national infrastructure and to military systems, though this is perhaps dependent on increasing the network dependence of such systems. Cyber warfare has asymmetric applications, potentially allowing states without conventional military strength or projection to attack targets that are more powerful. Cyber warfare, while offering some limited degree of utility today, will grow in importance due to the increased size, range and dependence on digital networks.

Thus, using the results of the application of our seven questions to the research sample we can generate the following definitional statement:

---

[124] (Serabian 2000)
[125] See for example Douglas Thomas and Brian D. Loader, eds., *Cybercrime – Law Enforcement, Security And Surveillance In the Information Age*, (London: Routledge, 2000).
[126] (Goldberg 2003)

Cyber warfare is symmetric or asymmetric offensive and defensive digital network activity by states or state-like actors, encompassing danger to critical national infrastructure and military systems. It requires a high degree of interdependence between digital networks and infrastructure on the part of the defender, and technological advance on the part of the attacker. It can be understood as a future threat rather than a present one, and fits neatly into the paradigm of Information Warfare.

A Discussion of the Results

The research undertaken in this paper uncovered distinct and conclusive trends of common understanding concerning cyber warfare. The grounded theory analysis of twelve texts uncovered a basic definition of the subject, and revealed a greater than expected degree of consensus regarding the scope, danger and timescale involved. This paper accomplishes its stated objective by defining cyber warfare as *symmetric or asymmetric offensive and defensive digital network activity by states or state-like actors, encompassing potential danger to critical national infrastructure and military systems*. The definition may be unwieldy, but it is consistent with the research sample. Furthermore, it has immediate utility, and is directly applicable to existing texts on the subject. One example is *Principles of Cyber Warfare* by Raymond C. Parks and David P. Duggan, which places an undefined but named cyber warfare inside the paradigm of IW[127]. The definition of cyber warfare contained in this paper is perfectly compatible with their research. By making unequivocal the existing implicit assumptions regarding the topic, this paper allows researchers to both categorise existing texts more effectively, and to expand the research sample to encompass more sources. Thus, this paper successfully contributes the first step towards creating an analytical framework for cyber warfare.

It is interesting to note that the results of the research partly contradict the hypothesis motivating this paper. The introduction suggested that agreement on the constitution, danger and potential of cyber warfare is unsubstantial or vague, that cyber warfare was a misunderstood or neglected concept, and perhaps even suffered from hyperbole and misrepresentation. The analysis of literature appeared to support this, but the application of a patterned research model proved it incorrect. There was agreement over who the actors were, what they would seek to affect, and when such events might be expected. It would appear that people do know what cyber warfare is, and that they are simply not very adapt at articulating it. This consensus is both unexpected and useful, and makes further study on the topic easier. It is important to stress that it does not entirely invalidate the hypothesis motivating this study, for there is a degree of misrepresentation in the field (especially with regards representing cyber warfare as IW). This study also revealed a startling weakness in existing texts. Even though writers agree that cyber warfare will allow attacks on critical national infrastructure or military systems though digital networks, there is a complete lack of empirical research available regarding the plausibility of such an event. There is currently no publicly available data conclusively linking critical national infrastructure and military systems to digital networks that would be susceptible to cyber attack. Until such research exists, there is the chance that the very concept of cyber warfare is hyperbole.

The results of this research identified a flaw in our sampling model that requires attention in future work. The exclusion of commercial texts from the research sample and the analysis of literature needs to be re-examined, as the conclusions of the commercial sector appear to be identical to those of the media, institutions, educational, governmental and military sources[128]. They were excluded from the literature analysis and research sample because of potential bias and profiteering regarding cyber warfare. However, our research shows the commercial connection between cyber warfare and network security is reflective of general literature on the

[127] (Parks and Duggan 2001)
[128] See for example: "The Future of Computers & Internet CyberWarfare??"

subject, and the exclusion of such texts should not occur in future studies. There is perhaps one proviso. The discrimination between cyber warfare and other cyber events is unclear in the commercial texts encountered, and requires examination. A press release from security company mi2g[129] counted Chinese independent hacker attacks during the Kosovo crisis as cyber warfare[130]. Such an assertion would contradict this paper's discovery of a trend in media, institutional, education, governmental and military texts to regard cyber warfare as state-orientated.

We need a substantial amount of future research to define, categorise and analyse cyber warfare. The first step of such research could be to confirm the tentative definition of cyber warfare contained in this paper, perhaps using a quantitative study to determine if the definition is indeed broadly applicable. Cyber warfare also needs clarification to place it in context with other similar concepts in the field of security, and this is especially true of IW. One example would be that the demarcation of differences between the terms 'cyber warfare' and 'Information Warfare' must be explicit to prevent further confusion. Furthermore, while cyber warfare can fit into the paradigm of IW as digital information operations, it is not yet clear if the term can be used more widely or is exclusively linked to digital networks. Potential confusion exists over whether cyber warfare is computer-mediated communication, or whether the term encompasses ELECINT[131] and other traditional electronic forms of communication warfare. There is a lot of ground to cover before a comprehensive and tested theoretical model exists.

At least part of this ground needs to consider this paper's identification of an emerging 'family' of cyber events. The terms 'cyber warfare', 'cyber terrorism'[132] and 'cyber crime'[133] appeared in the literature analysed, and there is no clear way to tell them apart. Research must classify these different cyber occurrences, and to create ways to differentiate between them. There is a very practical reason for this. All the identified cyber events appear to centre on attacks or abuses of digital information networks. If all cyber events consist of network attacks, it is hard to tell them apart. Therefore, it is hard to respond to a network attack proportionately. This leaves open the possibility of a nuclear response to a non-state cyber attack[134]. Once further research does create a clear demarcation between different 'cyber' events, articles encountered in the literature analysis such as Information Warfare Attack Assessment System (IWAAS)[135] and Enlisting Event Patterns for Cyber Battlefield Awareness [136] can contribute greatly to securing digital networks. We need to empirically examine the strength and weakness of networks, and to examine the degree of dependency that critical national infrastructure and military systems have on such networks. Instead of relying on supposition, we need to delineate exactly what effects cyber attacks have under different circumstances, and to plot the dangers and responses to a cyber attack.

---

[129] mi2g have a homepage at http://www.mi2g.com.
[130] "NATO Countries Under China Cyber Attack – Press Release - Chinese Retaliate Aggressively to Belgrade Embassy Bombing," mi*2g*, (11 May 1999), http://mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//mi2g.com/cgi/mi2g/press/110599.php.
[131] Electronic Intelligence
[132] David Coursey, "Cyberterrorists: How Real Are They? How Ready Are We?," *Survivalforum.com,* (10 April 2003), http://www.survivalforum.com/modules.php?name=News&file=article&sid=255.
[133] (Thomas and Loader, eds. 2000)
[134] Timothy L. Thomas, "Russian Views On Information-Based Warfare," *Airpower Journal*, (Special Edition 1996), http://www.airpower.maxwell.af.mil/airchronicles/apj/thomas.pdf.
[135] (Rathmell, Overill and Valeri 1997)
[136] (Perrochon et al., 2000)

Writers from different sources all agree that cyber warfare is important, and they largely agree on the scope, danger and timescale it inhabits. This is remarkable given that no empirical study exists testing the propositions surrounding the topic. The concepts underlying cyber warfare and cyber events in general have apparently seized the imagination of many writers and thinkers. Whether these concepts will turn out to have been uncritically absorbed or amount to a genuine security problem is entirely ambiguous. There has simply been too little research into the field to comment with any degree of authority. However, there can be no doubt cyber warfare merits attention. Phantom menace or fatal enemy, it requires study and dissemination. If it is hyperbole and presents no threat, then let us find out, and if it is a threat then let us understand it clearly. It cannot have escaped the reader that the vast majority of texts encountered in the construction of this paper are not research documents but opinion pieces. It is imperative that this changes. Not even the richest nation can afford a serious attack on infrastructure, nor can it afford to waste untold sums on preparing for something that may never happen. This paper has provided a ‘small’ definition for cyber warfare. From this writers can grow to understand the limitations, placement and meaning of the topic. However, it is a big subject, and requires a ‘big’ and comprehensive definition. Only a succession of quantitative and qualitative studies examining everything from confirmed network attacks to emerging policy on cyber corps can accomplish this.

There is much to do.

Bibliography

Physical Books:

Bamford, James. *Body Of Secret – How America's NSA and Britain's GCHQ Eavesdrop On The World*. London: Arrow Books, 2002.

Denning, Dorothy E. *Information Warfare And Security*. Harlow: Addison-Wesley, 1999.

Freedman, Lawrence, ed. *War*.Oxford: Oxford University Press, 1994.

Gill,Bates and Taeho Kim. *China's Arms Acquisitions From Abroad – A Quest For 'Superb And Secret Weapons'*. Oxford: Oxford University Press, 1995.

Gurley Bace, Rebecca. *Intrusion Detection*. Indianapolis: Macmillan Technical Publishing, 2000.

Harvey, Frank P. and Ann L. Griffiths, eds. *Foreign And Security Policy In The Information Age*. Nova Scotia: Dalhousie University, 1999.

Herman ,Michael. *Intelligence Services In The Information Age*. London: Frank Cass, 2001.

Moskos, Charles C., John Allen Williams and David R. Segal, eds. *The Postmodern Military*. Oxford: Oxford University Press, 2000.

Moffat, James. *Command And Control In The Information Age – Representing Its Impact*. London: TSO, 2002.

Rudestam, Kjell Erik and Rae R. Newton. *Surviving Your Dissertation – A Comprehensive Guide To Content And Process, 2nd ed.* London: Sage, 2001.

Shulsky, Abram N. *Silent Warfare – Understanding The World of Intelligence, 2nd ed.*London: Brassey's, 1993.

Thomas, Douglas and Brian D. Loader, eds. *Cybercrime – Law Enforcement, Security And Surveillance In the Information Age*. London: Routledge, 2000.

Waltz, Edward. *Information Warfare – Principles And Operations*. London: Artech House, 1998.

Internet Sources:

Abe, Hiroo. "Information Warfare and Its Perspective in Japan." *Defense Research Center*, (n.d.), http://www.drc-jpn.org/abe-e.HTM.

Agence France Presse. "US military concerned about China's cyberwarfare capabilities." *Online Readings ANS/GOV 338L East Asian International*

Relations, (March 28, 2001),http://inic.utexas.edu/~bennett/__338/CyberWar.html.

Agence France-Presse. "War of the Frequencies Being Fought Out Over Iran's Capital." *Spacedaily*, (June 12, 2003), http://www.spacedaily.com/2003/030612030728.d43r4jgw.html.

Akbar,Abdullah A. " 'Pay-per-use' Concept in Healthcare: A Grounded Theory Perspective." *IEEE Computer Society*, (2002), http://dlib2.computer.org/conferen/hicss/1874/pdf/187460169a.pdf?SMSESSION=NO.

Alford, Jr., Lt Col Lionel D. "Cyber Warfare: Protecting Military Systems." *Acquisition Review Quarterly*, (Spring 2000), http://www.dau.mil/pubs/arq/2000arq/alford.pdf.

"Al-Qaida Still Presents Greatest Threat to U.S., CIA Head Says." *U.S. Embassy Pakistan Page*, (March 20, 2002), http://usembassy.state.gov/islamabad/wwwh02032002.html.

"A National Strategy to Secure Cyberspace part 2." Strateg.ru,(n.d.), http://stra.teg.ru/library/national/34/usa-cyberspace/2.

Arkin,William M. "Toys 'R' U.S." Washingtonpost.com in *c4i.org*, (March 13, 2000), http://www.c4i.org/militarytoys.html.

Arquilla, John and David Ronfeldt. "The Advent of NetWar (Revisited)." Chap. 1 in Arquilla, John and David Ronfeldt, eds. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica:Rand, 2001. Online version used available at http://www.rand.org/publications/MR/MR1382/MR1382.ch1.pdf.

Arquilla, John J. and David F. Ronfeldt. "Cyberwar and Netwar: New Modes, Old Concepts, of Conflict." Excerpted from "Cyber War Is Coming" in *Comparative Strategy*, 12 (1993): 141-165. Online version used available at http://www.rand.org/publications/randreview/issues/RRR.fall95.cyber/cyberwar.html.

Associated Press, The. "White House Selects Cybersecurity Chief." *The New York Times*, (September 15, 2003), http://www.nytimes.com/aponline/technology/AP-Cybersecurity-Chief.html.

Barnes, William. "Singapore Weapons Factory for Junta." *China Morning Post*, (July 21, 1998), http://www.ibiblio.org/obl/reg.burma/archives/199807/msg00491.html.

Berkowitz, Bruce. "Information Warfare: Time to Prepare, Issues in Science and Technology Online." *Issues in Science and Technology Online*, (Winter 2000), http://www.nap.edu/issues/17.2/berkowitz.htm.

"Blackouts Cause N. America Chaos." *BBC News,* (August 15, 2003), http://news.bbc.co.uk/1/hi/world/americas/3152451.stm.

Borin, Elliot. "Planning for the Next Cyberwar." *Wired Magazine*, (April 18, 2003), http://www.wired.com/news/print/0,1294,58422,00.html.

Boytsov, Major M. "In Foreign Navies." Translated by the CIA's Foreign Broadcast Information Service. *Crypt Newsletter*, (February 7, 1996), http://www.soci.niu.edu/~crypt/other/boyt.htm.

"Breaking Technology News with David Burd and Dr. Richard Shurtz." *Stratford's Tech Talk Radio Newsletter*, (April 19, 2003), http://www.stratford.edu/techtalknews/techtalklatestnewsletter.html.

Bunker, Robert J. "Five Dimensional (Cyber) Warfighting: Can The Army After Next Be Defeated Through Complex Concepts And Technologies?" *Aeronautics.ru*, (March 10, 1998), http://www.aeronautics.ru/archive/research_literature/aviation_articles/Janes/topics/plasma_stealth/Five-Dimensional%20Warfighting.pdf.

Burns, Megan. "Information Warfare: What and How?" *Megan's Homepage*, (1999), http://www-2.cs.cmu.edu/~burnsm/InfoWarfare.html.

Burrett, Ann Joan. "Picking The Pitch: A Grounded Theory Study Of The Impact Of Equal Opportunity Officers On The Culture Of Universities." Ph.D. thesis, Southern Cross University, 2002, http://thesis.scu.edu.au/adt-NSCU/uploads/approved/adt-NSCU20020926.105835/public/01front.pdf.

"Business Process and Procedures for Tomorrow's Wars: The Results of Defense Reform Initiative: Seminar Game 00." *Defense Reform,* (March 2001), http://www.dod.mil/dodreform/briefs/seminargame2000.pdf.

Byon, Imju. "Survivability of the U.S. Electric Power Industry." MSc Thesis, Carnegie Mellon University , 2000. *CERT.org*, http://www.cert.org/archive/pdf/surv-us-electric-thesis.pdf

"Byrd's Remarks Before U.S.-China Security Review Commission." *U.S. Embassy Japan Page*, (June 14, 2001), http://usembassy.state.gov/posts/ja1/wwwhse0202.html.

Campbell,Duncan. "CIA Funds Cyber War Against Beijing Censor." *Guardian Unlimited*, (September 1, 2001), http://www.guardian.co.uk/internetnews/story/0,7369,545238,00.html.

Carver Jr., Major Curtis A. "Information Warfare: Task Force XXI or Task Force Smith?" *Military Review, Command & General Staff College* LXXVIII (1998), http://www-cgsc.army.mil/milrev/English/SepNov98/carver.htm.

Chong, Ja Ian. "PLA Modernisation and Taiwan Security." *Peace Forum, Strategic & International Studies, Taiwan Research Institute*, (July 29, 2003), http://dsis.dotweb.com.tw/onweb.jsp?webno=3333333305&webitem_no=553.

"CIA Official Assesses Information Warfare Threat." *USIS Washington File, U.S. Embassy Australia Page,* (December 10, 1998), http://usembassy-australia.state.gov/hyper/WF981210/epf406.htm.

"CIA's Tenet Says al-Qa'ida Still a Serious Threat." *U.S. Embassy Pakistan Page*, (February 07, 2002), http://usembassy.state.gov/posts/pk1/wwwh02020703.html.

Coffey, Jennifer. "FBI Sees Increase In Threat Of Cyber-Terrorism." *USIS Washington File, U.S. Embassy Australia Page*, (April 17, 1998), http://usembassy-australia.state.gov/hyper/WF980417/epf512.htm.

Cohen, Jackie. "Preparing for World War Web." *CNN.com,* (February 15, 1999), http://edition.cnn.com/TECH/computing/9902/15/webwar.idg/index.html.

"Cohen Says "Superpower" Label Attracts Asymmetrical Threats." *U.S. Embassy, Islamabad,Pakistan Page*, (August 23, 2000), http://usembassy.state.gov/posts/pk1/wwwh00082302.html.

Cohen, William S. "Center for Strategic and International Studies." *Defense Link*, (October 2, 2000), http://www.defenselink.mil/speeches/2000/s20001002-secdef.html.

Cohen, William S. "Foreign Policy and Defense Challenges." *Washington File, U.S.Embassy Australia Page*, (April 10, 2000), http://usembassy-australia.state.gov/hyper/2000/1004/epf301.htm

Conrad, Phillip A. "Information Warfare: Are you battlefield ready?", *Indiana University of Pennsylvania, Library Resources, SANS White Papers*,(February 13, 2001), http://www.lib.iup.edu/comscisec/SANSpapers/conrad.htm.

Costello, Sam. "U.S.-China Cyberwar a Dud, Although Trouble Lingers." *Infoworld*, (May 10, 2001), http://archive.infoworld.com/articles/hn/xml/01/05/10/010510hnhack.xml.

Coursey, David. "Cyberterrorists: How Real Are They? How Ready Are We?" *Survivalforum.com,* (April 10, 2003), http://www.survivalforum.com/modules.php?name=News&file=article&sid=255.

"Creating a Computer Security Incident Response Team: A Process for Getting Started." *CERT.org*, (May 8, 2003), http://www.cert.org/csirts/Creating-A-CSIRT.html.

Cummins, Daniel A. "Information Warfare: Going on the Offensive." *Offensive Information Warfare*, (October 1, 2000), http://faculty.ed.umuc.edu/~meinkej/inss690/cummins/cummins.htm.

"Cybernetics: A Definition- Entry in Macmillan Encyclopedia of Computers, 1991." *Pangaro.com*, (n.d.), http://www.pangaro.com/published/cyber-macmillan.html.

"Cyber Protests: The Threat to the U.S. Information Infrastructure." *National Infrastructure Protection Center*, (October 2001), http://www.nipc.gov/publications/nipcpub/cyberprotests.pdf.

"Cyber Strike: Serious Damage to Nation's Infrastructure." Posted by admin. Originally published on NewsFactor.com. *Survival Forum*, (March 15, 2003), http://www.survivalforum.com/modules.php?name=News&file=article&sid=79.

"Cyber War." (n.d.), http://faculty.bus.olemiss.edu/breithel/b620s02/riley/Cyber_War.htm.

"Cyber Warfare to Be Part of Taiwan War Drill." *The Straits Times*, (August 8, 2000), http://www.hartford-hwp.com/archives/27a/026.html.

Davis, Joshua. "If We Run Out of Batteries, This War is Screwed.", *Wired Magazine*, (June 2003), http://www.wired.com/wired/archive/11.06/battlefield_pr.html.

"DDSI: Towards a European Cyber-Security Strategy." *Review* 2, no 2 (n.d.), http://www.rand.org/randeurope/review/2.2-rathmell.html.

Delio, Michelle. "It's (Cyber) War: China vs US." *Wired*, (April 30, 2001), http://www.wired.com/news/print/0,1294,43437,00.html.

Denning, Dorothy E. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." Chap. 8 in Arquilla, John and David Ronfeldt, eds. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica: Rand, 2001. Online version used available at http://www.rand.org/publications/MR/MR1382/MR1382.ch8.pdf.

Dick, Bob. "Grounded Theory: A Thumbnail Sketch." *Resource Papers in Action Research, Graduate College of Management, Southern Cross University, Australia*, (2002), http://www.scu.edu.au/schools/gcm/ar/arp/grounded.html.

"DoD CIO Annual Information Assurance Report." *DoD/DIAP,* (April 2002), http://www.dod.mil/nii/org/sio/ia/diap/documents/PUBLIC_CIO_IA-AnRpt_1999.pdf.

Dougherty,Jon. "Chinese Preparing New Cyber-Attacks." Posted by admin. Originally published on WorldNetDaily.com. *Survival Forum*, (May 31, 2002), http://www.survivalforum.com/modules.php?name=News&file=article&sid=567.

Ellis, Susan. "Computers Are Weapons In Potential Cyber Attacks." *USIS Washington File, U.S.Embassy Australia Page*, (August 25, 1998), http://usembassy-australia.state.gov/hyper/WF980825/epf206.htm.

Erbschloe, Michael. "Information Warfare: How to Survive Cyber Attacks, Sample of Chapter 3." *Security Watch*, (n.d.), http://www.securitywatch.com/lit/network_security/infowar_sample.html.

Eriksson, E. Anders "Information Warfare: Hype Or Reality?" *CNS-The Nonproliferation Review*, 6, 63 (Spring-Summer 1999), http://cns.miis.edu/pubs/npr/vol06/63/erikss63.pdf.

"FBI to Alter Cyber Security Unit." Originally published by The Associated Press. *Survival Forum*, (March 26, 2003), http://www.survivalforum.com/modules.php?name=News&file=article&sid=149.

"Fierce Cyber War Predicted." *CNN.com*, (March 3, 2003), http://edition.cnn.com/2003/TECH/ptech/03/03/sprj.irq.info.war.ap.

Gannon, John C. "Intelligence Challenges Through 2015." *DCI/CIA-Speeches & Testimony*, (April 7, 2000), http://www.odci.gov/cia/public_affairs/speeches/2000/gannon_speech_05022000.html.

Gilmer, Carter. "The Future of Information Warfare." *SANS, InfoSec Reading Room*, (2001), http://www.sans.org/rr/paper.php?id=819.

Gilmore, Gerry J. "DoD Taps Reservists To Fill New Info Ops Units." *American Forces Press Service*, (December 8, 2000), http://www.dod.mil/news/Dec2000/n12082000_200012084.html.

Goldberg, Ivan. *Institute For The Advanced Study Of Information Warfare Page*, (March 12, 2003), http://www.psycom.net/iwar.1.html.

"Government Warns 'Patriot Hackers' Against Cyber Attacks On Iraqi Interests." Originally published by The Associated Press. *Survival Forum*, (February 13, 2003), http://www.survivalforum.com/modules.php?name=News&file=article&sid=789.

Graham, Bradley. "Bush Orders Guidelines for Cyber-Warfare," *Washingtonpost.com*, (February 7, 2003), http://www.washingtonpost.com/ac2/wp-dyn/A38110-2003Feb6?language=printer.

Hamre, Dr. John J. "Dr. Hamre's Speech to the Council on Foreign Relations." *Defense Link*, (June 5, 1998), http://www.dod.mil/news/Jun1998/t06181998_t0605cfr.html.

"Home Users Suffer Web Worm Woe." *BBC News*, (August 13, 2003), http://news.bbc.co.uk/1/hi/technology/3147147.stm.

Hrovat, Eric. "Information Warfare: The Unconventional Art In A Digital World." *SANS, InfoSec Reading Room*, (June 30, 2001), http://www.sans.org/rr/paper.php?id=787.

Hughes, Lieutenant General Patrick M. "Global Threats and Challenges: The Decades Ahead." *Defense Link*, (February 2, 1999), http://www.defenselink.mil/speeches/1999/s19990202-hughes.html.

Hughes, Scott. "Striking The Balance Between Information Sharing And Security In Corporate IT Systems." *Security Innovator*, (November 25, 2002), http://www.technologyreports.net/securefrontiers/?articleID=940.

" Internet Worm Threat 'Thwarted'." *BBC News*, (August 16, 2003), http://news.bbc.co.uk/1/hi/technology/3154117.stm.

"Interview: Amit Yoran." *Frontline: Cyber war!*, (April 24, 2003), http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/yoran.html.

"Interview: Richard Clarke." *Frontline: Cyber war!,* (April 24, 2003) , http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/clarke.html.

"Interview with John Holum on U.S. Security Policy." Originally published on USIA electronic journal "U.S. Foreign Policy Agenda." *USIS Washington File, U.S. Embassy Australia Page* , (July 15, 1998), http://usembassy-australia.state.gov/hyper/WF980715/epf313.htm.

"Japanese Newsletter on Taiwan Information Defense Concerns." U.S. Embassy China, (June 30, 2003), http://www.usembassy-china.org.cn/sandt/taiinfowar.html.

"Japanese Textbook Dispute Sparks Cyber Attack." *CNN.com*, (March 31, 2001), http://edition.cnn.com/2001/WORLD/asiapcf/east/03/31/japan.korea.website/index.html.

Johnson, L. Scott. "Toward a Functional Model of Information Warfare." *IR 360 Course Readings, San Fransisco State University*, (2001), http://bss.sfsu.edu/fischer/IR%20360/Readings/Information%20War.htm.

Kabay, M.E. "Edited Version of Chapter 12 from 'The NCSA Guide to Enterprise Security'." *Mich Kabay's Home Page-Overviews,* (1996), http://www2.norwich.edu/mkabay/overviews/infowar_1995.htm.

Kaspar, Lt Col Beth M." The End of Secrecy? Military Competitiveness in the Age of Transparency." *FAS.org*, (August 2001), http://www.fas.org/sgp/eprint/kaspar.pdf.

K, Joseph. "Guide To Tech Terminology." *Crypt Newsletter*, (September 19, 2003), http://sun.soci.niu.edu/~crypt/other/eligib.htm.

Ko, Shu-ling. "Cabinet Says Computers Under Attack." *The Taipei Times*, (September 4, 2003), http://www.taipeitimes.com/News/front/archives/2003/09/04/2003066387.

Krutzsch, Ernest. "Cyber Warfare." *Indiana University of Pennsylvania, Library Resources, SANS White Papers*, (December 13, 2000), http://www.lib.iup.edu/comscisec/SANSpapers/krutzsch.htm.

Larsson, Gerry, et al. "Leadership Under Severe Stress: A Grounded Theory Study." AU-24 Concepts for Air Force Leadership, (2001), http://www.au.af.mil/au/awc/awcgate/au-24/larsson2.pdf.

Lawson, Shannon M. "Information Warfare: An Analysis of the Threat of Cyberterrorism Towards the US Critical Infrastructure." *SANS, InfoSec Reading Room*, (2002), http://www.sans.org/rr/paper.php?id=821.

Lewis, James A."Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats."*CSIS.org*, (December 2002), http://www.csis.org/tech/0211_lewis.pdf.

Lettice,John. "At least 100 countries building cyber weapons." *SurvivalForum.com,* (September 24, 2002), http://www.survivalforum.com/modules.php?name=News&file=article&sid=688.

Lichtblau, Eric. "CIA Warns of Chinese Plans for Cyber-Attacks on U.S." *The English Russian World,* (April 25, 2002), http://www.erw.uln.ru/N11/CIA%20Warns%20of%20Chinese%20Plans%20for%20Cyber-Attacks.htm.

Lippman, Wes. "Cyberwar In the Middle East." *Eng 4 Technology of Cyberspace, Student Research, Thayer School of Engineering at Darthmouth College*, (February 6, 2003), http://engineering.dartmouth.edu/~engs004/middleeast.ppt.

Lunardi, Timothy. "When Computers are Weapons: Information Warfare and the Security Dilemma." In *Georgetown Essays on Information Warfare* 1, no 9, (May 3, 1999) edited by Dorothy E. Denning avilable online at http://www.cs.georgetown.edu/~denning/infosec/iw-essays/v1n9.txt.

"Major Power Outage Hits New York, Other Large Cities." *CNN.com*, (August 15, 2003), http://edition.cnn.com/2003/US/08/14/power.outage/index.html.

Mann, Charles C. "Homeland Insecurity." *The Atlantic Online*, (September 2002), http://www.theatlantic.com/issues/2002/09/mann.htm.

Martin, Josh. "Tech Notes." *IPI Global Journalist*, (2003), http://www.journalism.missouri.edu/globalj/Magazine/tech&events-20023q.html.

"Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network, chapter 8: Internet Warfare." *Sams.Net*, (n.d.), http://docs.rinet.ru:8083/LomamVse/ch08/ch08.htm.

McWilliams, Brian. "Iraq's Crash Course in Cyberwar." *Wired Magazine*, (May 22, 2003), http://www.wired.com/news/conflict/0,2100,58901,00.html.

McWilliams, Brian. "North Korea's School for Hackers." *Wired Magazine*, (June 2, 2003), http://www.wired.com/news/politics/0,1283,59043,00.html.

Minnich, MAJ James M. "North Korean Tactics." *CALL, Fort Leavenworth, KS*., (October 18,2001), http://call.army.mil/products/spc_prod/korea/contents.htm.

Moteff, John D. "Critical Infrastructures: Background, Policy, and Implementation." *Foreign Press Centers, U.S. Department of State*, (February 4, 2002), http://fpc.state.gov/documents/organization/8087.pdf.

"Ms. Guidance : Cyberwar: Information Warfare and Psychological Operations." http://www.t0.or.at/msguide/cyberwar.htm.

Mulvenon, James C. "The PLA and Information Warfare." Chap. 9 in Mulvenon, James C.and Richard H. Yang, eds. *The People's Liberation Army in the Information Age*.Santa Monica: RAND, 1999. Online version used available at http://www.rand.org/publications/CF/CF145/CF145.chap9.pdf.

Murray, Toby. "Cyber Warfare." (Spring 2003), http://www.cis.ksu.edu/~howell/492s03/student-talks/Murray/slides.ppt.

"National Strategy For Combating Terrorism."*U.S. Embassy India Page*, (February 2003), http://usembassy.state.gov/posts/in3/wwwfns.pdf.

"NATO Countries Under China Cyber Attack – Press Release - Chinese Retaliate Aggressively to Belgrade Embassy Bombing." mi*2g*, (May 11, 1999), http://mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//mi2g.com/cgi/mi2g/press/110599.php.

Newton, Scott Anthony "Can Cyberterrorists Actually Kill People?" *Sans.org*, (November 2001), http://www.sans.org/rr/paper.php?id=820.

"North Korea May Be Training Hackers for Cyber War." *Securesynergy.com*, (May 17, 2003), http://www.securesynergy.com/securitynews/newsitems/2003/may-03/170503-01.htm.

Orr IV, Stephen R. "Information Warfare / Cyber-Terrorism and World Governments." *Homepage of Stephen R. Orr IV*,(November 1, 2002), http://tiger.towson.edu/users/sorr1/IW%20CT.doc.

Paige Jr., Emmett. "The Future of Information Security." *Defense Issues* 11, no 71 (June 25, 1996), http://www.defenselink.mil/speeches/1996/di1171.html.

Parks, Raymond C. and David P. Duggan. "Principles Of Cyber-Warfare." *Information Technology and Operations Center*, (June 2001), http://www.itoc.usma.edu/Workshop/2001/Authors/Submitted_Abstracts/paperT2C1(10).pdf.

Patton ,Michael. "Introduction." *Information Warfare – An Introduction*, (n.d.), http://www.tlc.utexas.edu/courses/tlc321/final/patton/intro.htm.

"Pentagon Briefing on U.S. Space Command."*Department of State Washington File, U.S. Embassy Australia Page*, (January 5, 2000), http://usembassy-australia.state.gov/hyper/2000/0105/epf302.htm.

Perrochon, Louis et al., "Enlisting Event Patterns for Cyber Battlefield Awareness." *Program Analysis and Verification Group- CEP*, (January 2000), http://pavg.stanford.edu/cep/Cyberbattlefield.pdf.

Pethia, Richard. "The Melissa Virus: Inoculating Our Information Technology from Emerging Threats." *CERT.org*, (April 15, 1999), http://www.cert.org/congressional_testimony/pethia9904.html.

Pettigrew, Simone. "A Grounded Theory of Beer Consumption in Australia." Qualitative Market Research: An International Journal 5, no. 2 (2002) at *Emerald*, http://www.emeraldinsight.com/pdfs/awards2003/qmr.pdf.

Qiao, Liang and Xiangsui Wang. "Unrestricted Warfare." *c4i.org,* (February 1999), http://www.c4i.org/unrestricted.pdf.

Ragsdale, Lt. Col. (P) Dan. "Cyber Warfare at USMA." *Pointer View*, (April 25, 2003), http://www.usma.edu/PublicAffairs/PV/030425/CyberWarfare.htm.

Raman, B. "Proxy War in Cyber Space." *South Asia Analysis Group*, (May 10, 2000), http://www.saag.org/papers2/paper150.html.

Raman, B. "Terrorism: The Technological Imperative." *South Asia Analysis Group,* (February 17,2000), http://www.saag.org/papers2/paper104.html.

Rathmell, Andrew, Richard Overill and Lorenzo Valeri. "Information Warfare Attack Assessment System (IWAAS)." *International Centre for Security Analysis- Kings College London*, (October 1997), http://www.kcl.ac.uk/orgs/icsa/Old/iwaasppr.PDF.

"Report of the Defence Science Board Task Force on Information Warfare Defensive (IW-D)." *Cryptome.org*, (January 8, 1997), http://cryptome.org/iwd.htm.

Rich, CPT Marshall S. "The Fifth Dimensional Battlefield: Cyber Warfare." *The Management Group*, (March 14, 2000), http://www.mgt-gp.com/downloads/The%20Fifth%20Dimensional%20Battlefield%20-%20Cyberwarfare.PDF.

"Risk of Internet Collapse Rising." Originally published on BBC News. *Survival Forum*, (November 27, 2002), http://www.survivalforum.com/modules.php?name=News&file=article&sid=743.

Rumsfeld, Donald. "Media Roundtable in Canberra." *U.S. Embassy Australia Page*, (July 29, 2001), http://usembassy-australia.state.gov/ausmin/rumsfeld-rt.html.

Rumsfeld, Donald. "Rumsfeld Remarks to North Atlantic Council." *U.S. Embassy Pakistan Page*, (June 9,2001), http://usembassy.state.gov/posts/pk1/wwwh01060904.html.

Rumsfeld, Donald. "Rumsfeld Testifies on Need for New Strategic Framework, Senate Armed Services Committee." *U.S. Embassy Pakistan Page*, (June 21, 2001) http://usembassy.state.gov/posts/pk1/wwwh01062204.html.

"Russia: Information War." *Crypt Newsletter*, (February 7, 1996), http://www.soci.niu.edu/~crypt/other/boyt.htm.

Santoli, Al ed. "China's Electronic Spy Bases in Cuba; India-China Border Tension." *China Reform Monitor No. 487, American Foreign Policy Council,* (March 3, 2003), http://www.afpc.org/crm/crm487.shtml.

"Secret U.S. Plan for Cyber-War to Feature Windows XP." Posted by Scott Ott. *ScrappleFace*, (February 7, 2003), http://www.scrappleface.com/MT/archives/000640.html.

Serabian Jr., John A. "Cyber Threats and the U.S. Economy." *DCI/CIA-Speeches and Testimony*, (February 23, 2000), http://www.odci.gov/cia/public_affairs/speeches/2000/cyberthreats_022300.html.

Shanker, Thom and Eric Schmitt. "Cyber-Warfare in Iraq Already Has Broken Out." *International Herald Tribune*, (February 24, 2003), http://www.iht.com/articles/87692.html.

Sherwell, Philip, Sasa Nikolic and Julius Strauss. "Clinton Orders 'Cyber-sabotage' to Oust Serb Leader." Daily Telegraph on *Freerepublic.com*, (April 7, 1999), http://www.freerepublic.com/forum/a3780596c7940.htm.

Shimeall, Timothy, Phil Williams and Casey Dunleavy. "Countering Cyber War." *NATO Review* 49 (Winter 2001/2002): 16-18, (online version used available at http://www.nato.int/docu/rev-pdf/eng/0104-en.pdf).

Sobiesk, Edward. "Redefining the Role of Information Warfare in Chinese Strategy." *SANS, InfoSec Reading Room*, (March 1, 2003), http://www.sans.org/rr/paper.php?id=896.

Sokolov, Andrey."The War Seizes the Internet." Translated by Maria Gousseva. *Pravda.ru*, (March 21, 2003),http://english.pravda.ru/society/2003/03/21/44825.html.

Sproles, Jimmy and Will Byars. "Cyber-terrorism." *Computer Ethics at ETSU*,(1998), http://www-cs.etsu-tn.edu/gotterbarn/stdntppr.

"Strategic War... in Cyberspace." *RAND.org*, (January 1996), http://www.rand.org/publications/RB/RB7106/RB7106.html.

Sullivan, Bob. " 'Fizzer' Worm Spreads Around Globe." *Survival Forum*, (May 13, 2003), http://www.survivalforum.com/modules.php?name=News&new_topic=8.

Szafranski, Colonel Richard. "A Theory of Information Warfare: Preparing For 2020." *Airpower Journal* , (Spring 1995), http://www.airpower.maxwell.af.mil/airchronicles/apj/szfran.html.

"Taiwan Circles Wagons in Cyber-Warfare." *China News*, (August 17, 1999), http://www.fas.org/news/taiwan/1999/cn-08-17-99-11.htm.

Tasi, Michael. "Continuities and Changes in New Defense Thinking." *Peace Forum, Strategic & International Studies, Taiwan Research Institute,* (May 29,2001), http://dsis.dotweb.com.tw/onweb.jsp?webno=3333333306&webitem_no=88.

Tenet, George J. "Remarks As Prepared for Delivery by the Director of Central Intelligence." *DCI/CIA- Speeches and Testimony*, "December 7, 2000", http://www.odci.gov/cia/public_affairs/speeches/2000/LAspeechrev1_20001207.htm.

Tenet, George J. "Worldwide Threat - Converging Dangers in a Post 9/11 World." *DCI/CIA-Speeches and Testimony*, (February 6, 2002), http://www.odci.gov/cia/public_affairs/speeches/2002/dci_speech_02062002.html.

"Testimony by Director of Central Intelligence George J. Tenet Before the Senate Committee on Government Affairs." *CIA- Speeches and Testimony*, (June 24, 1998), http://www.cia.gov/cia/public_affairs/speeches/1998/dci_testimony_062498.html.

"The Future of Computers & Internet CyberWarfare??(sic)." *Pakcert.com.pk*, (n.d.), http://www.pakcert.com.pk/cyberwarfare.

Thomas, Timothy L. "Russian Views On Information-Based Warfare." *Airpower Journal*, (Special Edition 1996), http://www.airpower.maxwell.af.mil/airchronicles/apj/thomas.pdf.

"Transcript: Reno, Shalala, Clarke 1/22 Briefing On Terrorism." *USIS Washington File, U.S. Embassy Australia Page*, (January 22, 1999), http://usembassy-australia.state.gov/hyper/WF990122/epf505.htm.

"'Truce' in US-China Hacking War." *BBC News*, (May 10, 2001), http://news.bbc.co.uk/1/hi/world/asia-pacific/1322839.stm.

United States General Accounting Office. "Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems.", *GAO.gov*, (July 2002), http://www.gao.gov/new.items/d02474.pdf.

U.S. Marine Corps. "Information Operations." *c4i.org*, (February 27, 2001), http://www.c4i.org/mcwp336.pdf.

"US Ponders Cyber War Plans." *BBC News*, (February 7, 2003), http://news.bbc.co.uk/1/hi/technology/2737885.stm.

Wang, Major General Pufeng. "The Challenge of Information Warfare." *Institute for National Strategic Studies*, (1995), http://www.fas.org/irp/world/china/docs/iw_mg_wang.htm.

Wang, Senior Colonel Baocun and Fei Li."Information Warfare." *Institute for National Strategic Studies*, (June 1995), http://www.fas.org/irp/world/china/docs/iw_wang.htm.

Weisman, Robyn. "California Power Grid Hack Underscores Threat to U.S." *Newsfactor,* (13 June 2001), http://www.newsfactor.com/perl/story/11220.html.

Welch, Donald and Greg Conti. "A Framework for an Information Warfare Simulation." Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 5-6 June, 2001. Available online at http://www.itoc.usma.edu/Workshop/2001/Authors/Submitted_Abstracts/paperT1C3(36).pdf.

"What is C4I? Realizing the Potential of C4I: Fundamental Challenges." *c4i.org*, (February 21, 2003), http://www.c4i.org/whatsc4i.html.

"When states go to cyber war."*BBC News*, (February 16, 2000), http://news.bbc.co.uk/1/hi/sci/tech/642867.stm.

White House, The. " Presidential Decision Directive 62." FAS.org, (May 22, 1998), http://www.fas.org/irp/offdocs/pdd-62.htm.

White House, The. "Presidential Decision Directive/NSC-63." FAS.org, (May 22, 1998), http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

Wiser, Jr., Leslie G. "Cyber Security." *House Committee on Government Affairs*, (August 29, 2001), http://www.fbi.gov/congress/congress01/wiser082901.htm.

Wordreference.com, (n.d.), http://www.wordreference.com/english/definition.asp?en=war.

Yoshihara, Toshi. " Chinese Information Warfare: A Phantom Menace Or Emerging Threat? " *IWAR.org* , (November 2001), http://www.iwar.org.uk/iwar/resources/china/iw/chininfo.pdf.

Appendix 1 –Table Showing Research Source Material

Source	Title	URL
Media source 1	When states go to cyber-war	http://news.bbc.co.uk/1/hi/sci/tech/642867.stm
Media source 2	Preparing for World War Web	http://edition.cnn.com/TECH/computing/9902/15/webwar.idg/index.html
Institutional source 1	Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats	http://www.csis.org/tech/0211_lewis.pdf
Institutional source 2	Strategic War . . . in Cyberspace	http://www.rand.org/publications/RB/RB7106/RB7106.html
Education source 1	INFORMATION WARFARE: HYPE OR REALITY?	http://cns.miis.edu/pubs/npr/vol06/63/erikss63.pdf
Education source 2	Principles of Cyber-warfare	http://www.itoc.usma.edu/Workshop/2001/Authors/Submitted_Abstracts/paperT2C1(10).pdf
US source 1	Cyber Threats and the U.S. Economy	http://www.odci.gov/cia/public_affairs/speeches/2000/cyberthreats_022300.html
US source 2	DoD CIO Annual Information Assurance Report	http://www.dod.mil/nii/org/sio/ia/diap/documents/PUBLIC_CIO_IA-AnRpt_1999.pdf
China source 1	INFORMATION WARFARE	http://www.fas.org/irp/world/china/docs/iw_wang.htm
China source 2	THE CHALLENGE OF INFORMATION WARFARE	http://www.fas.org/irp/world/china/docs/iw_mg_wang.htm
Russian source 1	RUSSIAN VIEWS ON INFORMATION-BASED WARFARE	http://www.airpower.maxwell.af.mil/airchronicles/apj/thomas.pdf
NATO source 1	Countering cyber war	http://www.nato.int/docu/rev-pdf/eng/0104-en.pdf

Appendix 2 –Table Showing Results of the Research Questions

	Media Source 1	Media source 2	Institutional source 1	Institutional source	Educational source 1	Educational Source 2
Is cyber warfare named, or are offensive and defensive digital actions called IW?	Cyber warfare is named	Neither...the article mentions a war on the internet	Cyber warfare is named	Referred to as IW	Referred to as IW	Cyber warfare is named
Is cyber warfare limited to network attacks, or does it include all information operations?	Network attacks	Network attacks	Network attacks that affect critical infrastructure	Network attacks	Network attacks	Network attacks
Is cyber warfare regarded as something only nations can do?	Primarily states, though not limited to them	Primarily states, though not limited to them	Differentation between cyber warfare and cyber terrorism, so cyber warfare linked to nations	Primarily states, though not limited to them	Yes	Yes
Is cyber warfare regarded as a real threat to infrastructure?	Yes	Yes	No	Yes	Yes	Yes
Is cyber warfare regarded as a threat to military systems?	Not explicit, though it is implied	Yes	No	Yes	Yes	Yes
Is cyber warfare going to be useful to 'level the playing field' in asymetric war?	Not mentioned	Not explicit	No	Not explicit, but potential for low entry-cost war exists.	Not mentioned	Not mentioned
Is cyber warfare regarded as a current problem, or a future one?	Future	Future	Future	Current...increasingly important as technology dependency increases	Future	Current

	US source 1	US source 2	China source 1	China source 2	Russia source 1	NATO source 1
Is cyber warfare named, or are offensive and defensive digital actions called IW?	Cyber warfare is named	Cyber warfare is named	Referred to as IW	Referred to as IW	Referred to as IW	Cyber warfare is named
Is cyber warfare limited to network attacks, or does it include all information operations?	Network attacks	Network attacks	It is mainly connected to digital networks	Wider than network attacks, though strongly tied to networks and technology	It includes all information operations	Network attacks
Is cyber warfare regarded as something only nations can do?	Cyber-threats (network attacks) are connected with all actors	Differentation between cyber warfare and cyber terrorism, so cyber warfare linked to nations	Yes	Yes	Yes	Yes
Is cyber warfare regarded as a real threat to infrastructure?	Yes	Yes	Yes	Yes	Yes	Yes
Is cyber warfare regarded as a threat to military systems?	Yes, but it is not clear to what extent	Yes	Yes	Yes	Yes	Yes
Is cyber warfare going to be useful to 'level the playing field' in asymetric war?	Yes	Not mentioned	Not explicit, but smaller 'cyber' forces are regarded as superior to traditional forces	Yes	Not mentioned	Not mentioned
Is cyber warfare regarded as a current problem, or a future one?	Future	Current	Future	Future	Current	Future