2010

Information Warfare: Time for a redefinition

Patricia A H Williams
Edith Cowan University

DOI: 10.4225/75/57a83781befa6
Originally published in the Proceedings of the 11th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia,30th November - 2nd December 2010

Information Warfare: Time for a redefinition

Patricia A H Williams
secau - Security Research Centre
School of Computer and Security Science
Edith Cowan University
Perth, Western Australia
trish.williams@ecu.edu.au

Abstract

Information warfare has become an increasingly diverse field. The changes to its composition have been primarily driven by changes in technology and the resulting increased access to information. Further, it has been the progressively more diverse methods available for communication that has fuelled expanding applications for information warfare techniques into non-military environments. In order for younger generations of students to understand the place of information warfare in the larger security picture, there is a need to shift the emphasis from many of the military underpinnings to its relevance in modern society and the challenges in the commercial environment. This paper provides a platform for discussion of the sphere of information warfare and its relevance to contemporary society. Whilst the methods of information operations and the understanding of military origins have not changed, the manner in which the topics are presented and how these relate to today's corporate environment and increasingly global society have become a new focus. The importance of this is to make information warfare relevant to today's generation of students and to develop information strategists rather than information specialists who can function effectively on a global stage.

Keywords

Information warfare, education, information operations.

INTRODUCTION

Where information warfare was once a distinct discipline with military underpinnings, it has increasingly become fused with both the computer security and intelligence disciplines. Information warfare is still defined in some quarters as "information operations conducted during time of crises or conflict to achieve or promote specific objectives over a specific adversary or adversaries" (IWS, n.d.). Hutchison and Warren (2001) defined the essence of information warfare as where information "has to be manipulated to the advantage of those trying to influence it". These principles have not changed, yet the extent to which the application of these principles has infiltrated the contemporary corporate environment has shifted and extended. Whilst the definition is primarily military, the application of it has diverged into the corporate environment. Similarly, its composition and implication for the armed forces has also altered with the advancement of technology. The military are increasingly dependent on communication systems, networks and electronic sensors, reflecting a change in the characterisation war from a physical battlefield to a modern digitized one, supported by information and executed remotely (Frater & Ryan, 2001). Related to this is the application in the commercial environment where competitive business wars are waged with knowledge and control of communication networks. The changes driven by new technology reflect both a transformation in the command and control of military forces, and in how they are organised and trained. Perhaps what is key to this discussion is not that the focus of information warfare should move away from the its military basis, but that firstly its objectives and techniques now apply increasingly to the corporate environment, and secondly that the manner in which warfare is waged will evolve and change because of the advances in technology. Therefore, there is a shift in both application and execution of information warfare. This paper looks at this issue with reference this important and expanding discipline.

Positioning Information Warfare

Authors such as Borden modelled information warfare in 1999 from a military perspective and heavily focussed on war-fighting technologies. Traditional areas were command and control, psychological operations, attack and defensive operations. In 2001, Hutchison & Warren defined the principles of information warfare and showed how, since its emergence in the 1980's, it had become a broader discipline. It was originally suggested that information warfare was open to an organisational perspective where competitors, "criminals, dysfunctional/disgruntled staff, suppliers, hackers/crackers, intelligence services, foreign and domestic governments, the law, the media clients and pressure groups", all had the potential to be involved in information warfare. Since this was written, the possibility for these people and groups to influence the corporate environment has become a reality. New areas were identified in the mid 1990's and included electronic warfare, intelligence based warfare, information electronic warfare and cyber war (Libicki, 1995). The coining of the phrase 'digital wars' also known as cyber war was introduced. Yet, information warfare is also referred to as

cyberwar, network centric warfare, information operations and command and control warfare (Borden, 1999). In today's definition, information warfare incorporates all of these.

The change in terminology, in what information warfare consists of, has seen inclusion of previously disparate areas. Whilst linked to information system destruction or damage as seen in the Gulf War, the current definitions include areas such as specific information infrastructure attack, cyber terrorism, cyber crime, attacks on commercial and military web sites, website defacement, cyber war, netwar, denial of service attacks and so on. Ultimately, information warfare is about using information to make decisions and for the adversary, trying to influence, deny, or disrupt information used in decision making processes. This is the fundamental objective of information warfare as decision making is dependent on the quality, amount and correctness of the information available at the time the decisions are made (Marakas, 2003).

Indeed, Kuehl (2007) suggests that the challenge in education in an ever broadening field is to produce information warriors who no longer just coordinate services but are proficient in integrating information operations. This means we need a new breed of information warfare workers, 'information strategists' who can do more than analyse. Information strategists can coordinate and exploit information on a broader national diplomatic, military and economic basis.

The paper looks at this challenging environment, what has altered in the application of information warfare, and links this to the need for information strategists in a global environment.

A CHANGING ENVIRONMENT

Underpinning all information warfare topics is the theory that conceptualises data, information and knowledge within the information warfare context. The basic premise, and theory of techniques, has not altered drastically over the past 10-15 years. What has altered is the context in which information warfare is now used. This has occurred both in the military context and how it can effectively applied to the corporate and organisational environments. In addition, the complexity of, and in many cases the ease of access to, information using electronic techniques has altered. Further, these characteristics have become concerns for society and individuals, as their effects are replicated from the military to the public domain. The move into the public domain means that society not just the military has to deal with the exposure to terrorism, as highlighted and popularised by the reporting on the September 11 attacks on the World Trade Centre. This exposure extends to cyber terrorism and being able to distinguish the hype from the facts as presented by the media and understanding its relevance to international and public affairs. National security has extended it reach. It is no longer solely the province of the military to protect a country and its inhabitants; it is also today commerce and industry that has become a both a target and contributor to the protection of national security and a country's way of life (Wilson, 2009).

There is no doubt that major changes have occurred because of networking and the Internet, and the ability for people to communicate quicker. In addition, for the military at least, the increasing dependence on non-military information systems over which the military has little or no control means that increasing vulnerabilities are created and cyber warfare become prominent (Libicki, 1995). As use of the Internet as a source of information and its global access, language and culture begins to play a part in the equation when using foreign information systems.

Traditional information warfare topics such offensive and defensive operations, espionage, ethics and legalities, propaganda and intelligence have not essentially changed or become obsolete although there are some new additions. What has altered is the perspective an application of these areas. The areas of cyber security, critical infrastructure protection, cyber terrorism, technology convergence, electronic warfare, individual warfare and space war are some of the new areas for debate.

Cyber Security

Cyber security is a general term that covers all aspects of attack protection, and is not specifically an information warfare topic, however encompasses the spectrum of protection from a proliferating spectrum of cyber threats. It enters the sphere of information warfare as it relates to national and international political agendas and in relation to a global communications infrastructure. This infrastructure is complex and difficult to comprehend or deconstruct in tracing offensive events and therefore being able to protect against events is essential. Where it has direct relevance is in discussion of structured attacks with systematic, supported (with intelligence and funding) and goal oriented activities (ITU, 2005). Critical infrastructure protection, due to its fundamental role in modern society and the potential societal impact attacks on it would result in, is a major target for terrorist and activist group activity, and therefore also falls under the heading of information warfare. The potential for catastrophic incidents is growing with the improving efficiency of networks and automated supply and logistics chains (McCathy *et al*, 2009).

Ethical / Legal Perspectives and International Agreement

As the complexity and dependency on information technology increases, so does the legal requirement to counteract nefarious and criminal activity. In addition, the ethical debate involved in information warfare to segregate the military from civil impacts of cyber terrorist activity, the state versus the non-state action, the acceptable from the unacceptable, is complex and disparate. In modern society and education there is less unconditional acceptance of the state and government viewpoint and thus it promotes animated and heated discussion. Further, any international agreement on information operations and limitations is as yet unscheduled. With the proliferation of information warfare has come the issue of effects on combatant and non-combatant targets and the intentional and unintentional impact on civilians and societies. Thus, the morality of information warfare will always be on the agenda.

Cyber Espionage

Espionage is one information operations technique that links competitive intelligence gathering to the edges of legal and ethical action, and is classed as information warfare. In the global networked environment this presents many challenges due to lack of definition of jurisdiction (Schneier, 2000). Such action is no longer restricted to military targets as it has been a mainstream aspect of competitive advantage for some time (Callon, 1996). Its techniques still include surveillance and social engineering, albeit some advances in how these are undertaken have taken place. Cyber espionage extends to terrorist groups as well as military and industrial actors. Attacks of this nature are not uncommon and need more consideration in information warfare discussions (Wilson, 2009).

New perspectives on Propaganda

Propaganda is also now more commonly called perception management and forms part of the gamut of deception techniques (Rowe and Rothstein, 2004). It uses traditional techniques to influence emotions, motives and reasoning. The art of persuasion and power are still the basis for this topic, however, what has changed is the terminology and methods used. Conventional propaganda is now also called public relations, ‘spin’ and misinformation, even advertising. Its success is still influenced by personal characteristics and increasingly by individual media literacy. The methods and sphere of influence have expanded with the use of networks and the Internet. Interestingly, the methods have become more sophisticated in some applications, yet in others have returned to more traditional scenarios such as social engineering. The overarching term that is inclusive of propaganda is psychological operations.

The social and organisational impacts of propaganda on modern society need to be analysed, and what threats and risks these pose. It is not only the explosion of the Internet and other media sources that need consideration, it is the ease with which any digital object (document, image, and video) can be manipulated to support and distribute false assertions. These techniques have been heavily used in the Middle East conflicts (Macdonald, 2007). The US troops fighting in Iraq were ‘mystified’ as to how different the war they fought and how it was portrayed in the media were (StrategyPage.com, 2007). In addition, the use of newsgroup and forums as channels for information, disinformation, and extremist communication, to date, has not been considered mainstream for education in information warfare.

> “The term information warfare can mean the use of smart technology in a traditional war or the use of IT systems attacking part of a country's infrastructure. ….. In some cases it appears that national laws cannot stem the tide of these emerging groups and governments are responding to this new threat with draconian measures by introducing electronic surveillance and interception to combat the increasing use of encryption favoured by terrorists and criminals alike. Governments have to strike a balance between freedom of speech on the one hand and the security of a country and its people on the other“(Crilley, 2001).

The socio-political motivations of groups using these mediums require more serious investigation within the security discipline if effective countermeasures are to be employed.

Intelligence and Counter Intelligence

Intelligence operations are an integral part of information warfare, however they have become so important in many areas that it has become a sub-discipline in its own right. Whilst it is still important to address it in information warfare, the execution of intelligence tasks is better suited to more specific learning in this specific discipline. However, the importance and place of intelligence, intelligence gathering and analysis in information warfare must be made explicit and contextualised for both military and non-military perspectives.

It is becoming apparent that more state-based attacks on governments, particularly towards the US, are occurring. The reality of such attacks and subsequent impact needs to be fully comprehended as a threat to modern society through undermining and destabilising government and economies. For instance, the disastrous damage that could be effected to US critical infrastructure and the economy, by countries such as China are detailed in a report to US Congress (USCC, 2009, pp.167-181). There have been numerous major attacks on the US government and defense systems over the past three years, many of which are state based or supported form China. Indeed, the Chinese government is actively recruiting cyber-skilled hackers for information warfare activities.

Cyber terrorism and hackivism

Using the Internet and other global networks is a viable weapon for cyberterrorist attacks when used to attack critical infrastructure and communication and transport systems that also directly affect society (Collin, 2008; Denning 2001). This differs from initial definitions that suggested that "Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives" (Denning, 2000). Where previously the ability of state and non-state actors to affect such attacks was remote, today they are a possibility. This is particularly in view of the insecurities that still in exist in SCADA systems. (Woodward & Valli, 2008).

Attacks on internet and social networking sites highlights the use of hacking as an information warfare tool to disrupt communications and promote political ideologies. An emerging trend is hacktivism, where *citizen-based warfare demonstrates a powerful weapon, has seen electronic civil disobedience and* digital culture jamming (Hearn, Mahncke & Williams, 2009). This focus for information warfare in this field has been multinational corporations, targeting their practices in globalization, and freedom of a society voice as during the Iranian protests in June 2009 where the Internet and specifically Facebook, Twitter and You Tube were critical in communicating messages to organise the protests ("Iran blocks Facebook", 2009). Such hacktivist activities challenge international relations. Conway (2007) suggests that increasingly there is a shrinking gap between the hacktivist and the cyberterrorist.

Electronic Warfare and Digitization

With its basis in the electromagnetic spectrum, the purpose of electronic warfare was traditionally to corrupt an adversary's ability in this spectrum and clearly directed at the physical layer activity in a network (Frater and Ryan, 2001, p. 219). Today this focus has altered to include attacks on services which support the physical layer activities. Integrated network systems are more vulnerable to attack. Whilst the military still maintains separate tactical communication systems, the commercial world has opted for increased seamless integration as is demonstrated by the use of the Internet for voice communications. This integration also applies to mobile and ad hoc networks. This cyberwar position poses significant problems for the military.

Integration of Technology and Individual Warfare

The assimilation of technologies has seen new vulnerabilities unconsidered in the early 2000's. The interconnectedness of technologies has seen a growing vulnerability to personal information warfare attacks. With the use of mobile devices such personal digital assistants and mobile phones, and internet enabled home devices such as televisions and game consoles there is an increased opportunity for targeted attacks on individuals using cyberspace. With this convergence of technology comes greater freedom and greater threat. Personal information warfare attacks have come to the fore with more individual connections to broadband and integration of technologies. It is not that people are connected to a particular domain, it is that they are connected the majority of the time to one network or another through multiple devices. The 'on and accessible all the time' mentality means that individuals are more vulnerable to information warfare attacks (Valli, 2002).It may not be individuals that are the target of the attack; it is more conceivable the resources the individual has access to and usually controls is the target. Our individual dependence on the technology means that any attack on the technology or the use of the technology for other more nefarious ends, is possible and highly likely. The vulnerability of non-military individual technology users is high. The disruption to people's lives is a consequence of such attacks (Cronin & Crawford, 1999). Home and individual attacks in information warfare stem from the 'always on' availability of home PC and networks. Whilst the methods of attack have been through malware and phishing, the use of home networks for botnet activity or individual collection of information is an increasing threat to society (Wolfe, 2007)

Space Wars

There are some new topics in information warfare emerging such as the concept of space war. Our dependency on satellite technology and the potential to create havoc in the space environment has prompted the US to

introduce the National Space Policy (Shiga, 2010). The problem is not restricted to space weapon systems, it also involves the impact that uncontrolled satellites and satellite debris could have in space. It has already been proven that anti-satellite capabilities are a reality by both China in 2007 and the US in 2008. Unfortunately as with most security technologies, whilst the technology is designed to protect and repair satellites it could also be used to interfere with them. The idea of a malicious satellite may seem far fetched but is indeed a reality. Another aspect of space war more in the domain of information warfare is that of incepted and altered satellite signalling.

DISCUSSION

Perhaps what is lost in the recognition of redefining the discipline is that of the original doctrine and strategy that underpinned information warfare's early years. Whilst there is still a place for this in military education of information warfare, it is perhaps less important in teaching information warfare as part of an overall perspective on security to non-military based courses. This is open to debate and personnel working in the armed forces in information operations and signals intelligence roles would certainly need such background. What has changed even since the early 2000's, is the connectivity and its uses, together with the increasing reliance on computer controlled systems.

Cyber Warfare as the Fifth Domain

Cyber warfare uses the Internet and global networks for political; military and economic actions including espionage and crime (Carr, 2010). Increasing cyber warfare is focusing on critical infrastructure vulnerability. It has been, arguably, labelled as the fifth domain for warfare after air, land, sea and space. It includes state and non state actors. Despite the term having been around for ten years, it is still not clearly defined legally or ideologically.

It is clear that information warfare is now on the global agenda with countries such as the US, Australia, United Kingdom, South Korea and China, and NATO setting up dedicated cyber-security centres. This has been in response to the war threat in the 'fifth domain'. Commentators suggest that the threats of information warfare cannot be dealt with without the assistance and involvement of the corporate area (Johnstone, 2010). In traditional information warfare this was not the case. The military operations were separate in objective and operation. Physical protection of the nation and people were the primary concern. The new perspective needs to have a stronger focus on critical infrastructure in order to protect the nation, society and people. This includes our economic systems as well as communications and essential services. An example of this need and the potential disruption was evident in the Russian attacks on Estonia in 2007 (REF). What has altered is the reliance on and rapid adoption of integrated technologies such as iPhones, social networking, shared services cloud computing. The change from the 2001 definition of information warfare (Hutchinson & Warren, 2001) is the risk management required for supply chains; the integration and reliance of society on technology; and the increasingly dynamic defence requirements.

Categorisations of information warfare

There is no doubt that to make any curriculum and discipline relevant to today's society it must reflect relevance to international, national, economic organisational and personal security. It has to encompass the techniques in information warfare, the defences and countermeasures, and the potential impact in reality, in law and ethically. In order to give the broadest picture, education must be mindful of the strategic implications of information operations and how these can be harnessed to assist in defence and in policy making. This is particularly important in consideration of increasing terrorist activity and the potential vulnerabilities in critical infrastructure.

Perhaps new perspectives on how information warfare is positioned, reflecting both military and organisational constructions, would be on the operational, tactical and strategic levels. The association with these levels would allow particularly those with non-military backgrounds to comprehend the associated impact of information warfare at each level. Strategic information warfare is aimed at influencing decisions and subsequently actions, whilst the operational level supports the strategic by affecting an adversary's ability to make those decisions (Szafranski, 1995). What is clear is that the area of cyber warfare is adding both opportunities and challenges for organisations defence. This is creating a shift in the position of information warfare to include an increasing overlap with computer network operations - defensive, exploitative and as an attack mechanism.

Another categorization would be to link with the spheres in which information warfare is executed. These are essentially the military, corporate/economic, community/social, and personal environments. Indeed the impact and multiple aspects of information warfare would have differing impact and perspectives. However, such a categorisation may assist the relevancy of information warfare to be understood more clearly in terms of legal, ethical and potential impact viewpoints.

Dependency on technology means that targets for information warfare are abundant from telecommunications and space based systems, though critical infrastructure automated control and finance systems, to the construction of society and its cultural systems. Increasingly the targets for information warfare are the operational level networked systems, and as these expand global vulnerability occurs. The impact on individuals and society has changed dramatically from information warfare's inception. To date information warfare, under the discipline of security, has not explored these impacts in any depth.

The explosion of channels for extremist and socio-political groups to disseminate their message means that the motivation of such groups necessitates exploration, together with a wider appreciation of the potential effect of the use of technology in this activity. Contemporary information warfare needs to acknowledge the increasing use and influence of activists and extremists in this space.

Information strategists versus information specialists

Developing a strategic viewpoint in contemporary information warfare as applied to their sphere of reality (for whom the majority is not the military environment). Indeed, arguable some of today's student cohort will be the future strategists who advise governments on national security behaviour. This will include corporate involvement in critical infrastructure protection and economic protection of society.

As with other areas of information use in society, the danger that now exists, and increases daily, is that of information and data overload. The problem, particularly for military scenarios, is sorting out the relevant from irrelevant information. In the past fifteen years since the acknowledgment that harnessing technology in information warfare would be possible; the world has changed dramatically (DiNardo & Hughes 1995). No longer is it sufficient to be just an information specialist whose role is to acquire, evaluate and search for information. What are required now are information strategists who can align information strategy (proactively) with corporate and military strategic goals. This role is not merely content based, it is to analyse that information to best meet deliberate objectives.

CONCLUSION

Information warfare emerged in the 1980's as a significant feature of modern warfare. An increase in the volume and access to information began to transform society. Teaching the content and significance of information warfare in the curriculum of security relies increasingly on linking it to today's society and world. Demonstration of this context helps create meaning. This is particular important for the younger generation of students who have only ever experienced the conflict of war through a television screen or through electronic games. Thus information warfare needs a new perspective on how it can use applied in the broader social and economic community.

This paper is a platform for discussion of the application of information warfare in a contemporary economic. The discipline is becoming increasingly integrated with other parts of the computer security disciplines. What is the place of information warfare in this changing structure? Current research at Edith Cowan University is looking at creating a new topology for information warfare and its place in information security. This project is assessing student views on information warfare and how it can be made sense of in various ways and using various categorisations. Information warfare is an essential constituent of the gamut of security. It allows students and disciplinarians to make sense of multiple warfare and security techniques in the context of modern society as well as the military. If information warfare is to continue to be a discipline stream in its own right, and not become subsumed by information security, it must be clear and articulate its unique aspects and applications.

REFERENCES

Borden, A. (1999). What is information warfare? *Air & Space Power Journal*. Retrieved from http://www.airpower.au.af.mil/airchronicles/cc/borden.html

Callon, J. D. (1996). *Competitive advantage through information technology* (International Ed.). Singapore: McGraw-Hill.

Carr, J. (2010). *Inside cyber warfare.* Sebastopol, CA: O'Reilly Media.

Clarke, R.A. and Knake, R.K. (2010). *Cyber war: The next threat to national security and what to do about it.* New York: HarperCollins.

Collin, B.C. (2008). The future of cyberterrorism. Where the physical and virtual worlds converge. Proceedings of the *11th Annual International Symposium on Criminal Justice Issues.* Retrieved from http://afgen.com/terrorism1.html

Conway, M. (2007). Cyberterrorism: Hype and reality. In E.L. Armistead (ed) *Information warfare*. Virginia, ,USA: Potomac Books.

Crilley. K. (2001). Information warfare: New battlefields terrorists, propaganda and the Internet. *Aslib Proceedings Bradford: Jul/Aug 2001, 53*(7), 250-264.

Cronin, B and Crawford, H. (1999). Information Warfare: It's Application in Military and Civilian Contexts. *The Information Society*, *15*, 257–263,

Denning, D. (2000). *Cyberterrorism.* Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services, US House of Representatives, 23 May 2000.Retrieved from http://www.cs.georgetown.edu/~denning/infosec/cyberter ror.html.

Denning, D. (2001). Is Cyber Terror Next? In *Understanding September 11* edited by C. Calhoun, P. Price, and A. Timmer, PP, New York: The New Press. Retrieved from http://www.ssrc.org/sept11/essays/denning.htm

DiNardo, R. L. and Hughes, D.J. (1995). Some Cautionary Thoughts on Information Warfare. *Airpower Journal - Winter 1995*. Retrieved from http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/win95_files/dinardo.htm

Frater, M. R., & Ryan, M. (2001). *Electronic warfare for the digitized battlefield*. Boston: Artech House.

Hearn, K., Mahncke, R.J. and Williams, P. A. H. (2009). Culture jamming: from activism to hacktivism. In P.A.H. Williams (Ed.) *Proceedings of the 10th Australian Information Warfare and Security Conference*, (pp.13-17), SECAU Security Research Centre, Edith Cowan University, Perth, WA.

Hutchinson, W., & Warren, M. (2001). Principles of Information Warfare. *Journal of Information Warfare, 1*(1),1-6.

Iran blocks Facebook. (2009, Sunday, 24 May 2009, 11:17). Sunday, 24 May 2009, 11:17. Retrieved Oct, 14 2009, 2009, from http://www.theinquirer.net/inquirer/news/1137462/iran-blocks-facebook

ITU. (2005). A comparative analysis of cybersecurity initiatives worldwide. WSIS Thematic Meeting on Cybersecurity, Geneva 28 June – 1 July, 2005.

IWS. (n.d.). The Information Warfare Site. Retrieved Oct 26, 2009, from http://www.iwar.org.uk/iwar/

Johnstone, P.D. (2010). Why we must fear the threat of the fifth domain. *Weekend Australian*, October 23-24, 2010, Defence Section p.11.

Kuehl, D. (2007). Introduction: "Brother, can you spare me a DIME?". In E. L. Armistead (Ed.) *Information Warfare-Separating hype from reality*. Washington, D.C.: Potomac Books.

Marakas, G.M. (2003). *Decision support systems in the 21st century. (2nd ed.).* Upper Saddle River: Prentice Hall

Macdonald, S. (2007). *Propaganda and Information Warfare in the Twenty-First Century: Altered Images and deception operations.* London: Routledge.

McCathy, J.A., Burrow, C., Dion, M. and Pacheco, O. (2009). Cyberpower and critical infrastructure protection: A critical assessment of federal efforts. In F.D. Kramer, S.H. Starr and L.K. Wendz (eds.) *Cyberpower and national security,* pp. 543-556. Washington D.C.: National Defense University Press.

Rowe, N, C. And Rothstein, H.S. (2004). Two taxonomies of deception for attacks on information systems. Retrieved from http://www.cs.nps.navy.mil/people/faculty/rowe/mildec.htm.

Schneier, B. (2000). *Secrets and lies: Digital security in a networked world*. New York: John Wiley & Sons.

Shiga, D. (2010). No space for war. *New Scientist,*10 July2010.

StrategyPage.com. (2007). *Japanese Propaganda and American Mass Media*. Retrieved from http://www.strategypage.com/print.aspx?sec=htmw&bi=htiw&fn=20070629

Szafranski, R. (1995). A theory of information warfare: *Airpower Journal*, (Spring), 56-65.

USCC. (2009). *2009 Report to Congress on the U.S.-China Economic and Security Review Commission: Chapter 2. Section 4 China's cyber activities that target the United States and the resulting impacts on U.S. National Security*. Retrieved from http://www.uscc.gov/annual_report/2009/chapter2_section_4.pdf

Wilson, C. (2009). Cyber crime. In F.D. Kramer, S.H. Starr and L.K. Wendz (eds.) *Cyberpower and national security,* pp.415-436. Washington D.C.: National Defense University Press.

Wolfe, D. (2007). Information operations and the average citizen. In E.L. Armistead (ed) *Information warfare*. Virginia: USA: Potomac Books.

Wooward, A. & Valli, C. (2008). Issues common to Australian critical infrastructure providers SCADA networks discovered through computer and network vulnerability analysis. *Proceedings of the 6th Australian Digital Forensics Conference*, pp-206-210. Perth: SECAU- Security Research Centre. .

Valli, C. (2002). Personalised information warfare - The new homeland defense. *Journal of Information Warfare, 2*(1).