Edith Cowan University
Research Online

Australian Information Warfare and Security Conference

Security Research Institute Conferences

2010

International Relations and Cyber Attacks: Official and Unofficial Discourse

Kay Hearn
Edith Cowan University

Patricia A H Williams
Edith Cowan University

Rachel J. Mahncke
Edith Cowan University

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
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/isw/32

International Relations and Cyber Attacks: Official and Unofficial Discourse

Kay Hearn[1], Patricia A H Williams[2,3] & Rachel J Mahncke[3]
[1]School of Communication and Arts,
Edith Cowan University
Perth, Western Australia

[2]secau - Security Research Centre
School of Computer and Security Science
Edith Cowan University
Perth, Western Australia
Trish.williams@ecu.edu.au

[3]School of Computer and Security Science
Edith Cowan University
Perth, Western Australia

Abstract
The potential for cyberwarfare is vast and is of concern to all nations, and national security defence. It appears that many countries are actively trying to protect their computer networks, whilst looking for ways that might bring down the networks of other countries, although this is not officially acknowledged. Bringing down another nations computer networks could give the attacking national intelligence and control. These kinds of interactions are now a part of the way in which international relations are played out, and the internet is also a place in which international relations are contested. As such the internet plays a role in the visualisation and articulation of international relations both officially and unofficially, via official pronouncements and the activities of private citizens. What makes the internet different to other media forms is that the internet also represents a space in which international relations are contested in terms of cyber attacks and information warfare. This paper analyses official and unofficial discourses surrounding the way in which international relations in regards to cyber attacks have been played out via the internet, using North Korea and Stuxnet as case studies.

Keywords
Information warfare, cyber attack, information operations, North Korea, DPRK, Stuxnet.

INTRODUCTION

Nations around the globe are developing network intelligence gathering capabilities in an attempt to gain privileged intelligence, especially for military information. According to reports in the western media China and North Korea are leading in developing these intelligence networks and more covertly, in their hacking capabilities. "There is evidence to support the fact that the government of China knowingly allows hacking groups to prosper in the country" (USPatriot, 2007). Deibert and Rohozinski (2009) argue that "certainly Chinese cyber-espionage is a major global concern. Chinese authorities have made it clear that they consider cyberspace a strategic domain, one which helps redress the military imbalance between China and the rest of the world (particularly the United States)". The accusations against China have been well documented in the western media (Hearn, 2009).

The internet has transformed some aspects of warfare and has created a new space in which international relations are played out and contested. In the mid 1990's Libicki (1995) argued that new aspects of warfare were emerging and integrating with traditional facets. What was being transformed was command-and-control warfare, intelligence based warfare, electronic warfare, psychological operations, hackerwar, information economic warfare and cyberwar. Regardless of the naming of new information operation techniques fostered by the advances in technology and communications, the altered environment has become both a benefit and a vulnerability to nations, societies and economies. A virtual space that is included in defence of the realm, though a space in which private citizens have carried out attacks on other nations.

Any attack by state actors on other countries potentially incorporates multiple facets of information warfare. What distinguishes information warfare from simple criminal or attacks on information security is the motivation behind the attack. When offensive information operations are used by national and government entities (state actors) against other countries, be they state or non-state targets, the detection and defensive operations can be complex and impinge on often sensitive international relations. In apparently non-aggressive

conflict, the features that must be considered are potential attacks on critical infrastructure (most commonly now associated with cyber terrorism), espionage, intelligence operations and more recently hacking activities.

According to Wilson (2007, p.5) a Congressional Report in 2007 it was noted that:

> An Information Operations (IO) attack may take many forms, for example: (1) to slow adversary computers, the software may be disrupted by transmitting a virus or other malicious code; (2) to disable sophisticated adversary weapons, the computer circuitry may be overheated with directed high energy pulses; and (3) to misdirect enemy sensors, powerful signals may be broadcast to create false images. Other methods for IO attack may include psychological operations such as initiating TV and radio broadcasts to influence the opinions and actions of a target audience, or seizing control of network communications to disrupt an adversary's unity of command.

Traditional 'war' is openly declared and not covert, although its execution may be concealed. Yet, this line becomes blurred when we consider governments supporting and putting in place warfare tactics covertly and not under a declaration of aggression. As Giacomello (2003) points out the ability to create serious damage through a well coordinated attack, be it on commerce or critical systems, would need significant resources – usually not a characteristic of the non-state actor domain. Currently it appears that Al Qaeda is the only non-state actor that has the resources to coordinate large scale attacks.

The integration of technologies and advances in networking has seen unprecedented growth in online activities. This has included national, state based attacks on individual organisations and countries. One high profile example in 2010 was the report by Google that a well organised, sophisticated and targeted attack on its corporate information was launched in late 2009. It results in the theft of intellectual property. Whilst this is not an isolated case for major corporations, it highlights the growing problem of state support cyber activity from countries such as China. Indeed, the report to the US Congress by the US-China Economic and Security Review Commission cites that China has launched extensive malicious cyber attacks against US companies, the government and defence systems (USCC, 2009). It refers to the potential widespread damage to the US economy that is increasing in likelihood with more than 43,000 malevolent cyber incidents in the first six months of 2009 alone originating in China. Whilst some are traced back to private hacking groups others are clearly linked to state sponsored activities.

INTERNATIONAL RELATIONS

The internet forms a space in which international relations are played out at both official and unofficial level. Reports on hacking fall into two kinds, those that suggest the hacking has been officially sanctioned or hacking that is unofficial (Hearn, 2009). This paper draws on the work of John Hartely (1992), and Bendict Anderson (1993) to argue that the world stage is imagined and constructed via the media. Hartely argues in his book, The Politics of Pictures, that the public is imagined via images that circulate in the media. Benedict Anderson's notion of imagined communities poses a similar argument. Anderson argues that nations are imagined via the media, museums and rituals of the nation. We seek to extend these arguments to the imagining of the world stage. In this sense the world stage is imagined via the media as this is the space in which the rituals of international relations are played out in an official sense. The world stage is constructed via pictures and news stories of staged events, such as the G8, or APEC summits. The media is the space in which heads of state make foreign policy announcements and so it is in this sense that the world stage is constructed on an official level.

The internet allows for the participation of groups outside of governments to play a part in foreign relations at an unofficial level. For example the Spy Plane incident in 2001, when a Spy Plane from the USA was forced to make an emergency landing on Hainan Island following a mid air collision with a Chinese fighter jet. The spy plane was immediately confiscated by Chinese authorities and the crew were imprisoned. The repatriation of the plane and the crew was negotiated between the two governments and was played out in the media in both countries and on news websites. On the internet the incident was also communicated on official government websites on both sides. The incident was played virtually in a spate of 'tit for tat' hack attacks on government websites from private citizens in China and the USA (Wu, 2006).

It is against this back drop that we seek to analyse the interplay between the official and unofficial constructions of the world stage through the use of medium theory and in particular the work of Harold Innis (1951; Innis 1952; Innis 1972) and Ronald Deibert (1997). Both use medium theory to explore the shifts in political power that occur in relation to the development of new forms of communications technologies. Innis was interested in tracing these shifts in ancient times and Deibert focuses on the changes occurring following the development of the internet. Deibert (1997, p.204-205) argues that the internet "favours a complex diffusion of production across territorial/political boundaries by facilitating multilocational flexibility, transnational joint ventures, and both global and localization and "local" globalization –the latter best evidenced by the commercialization of the world wide web". Deibert uses the term ecological holism to examine media environments. By this Deibert

means that we need to look at the way in which societies adapt to changing media environments. It is against this back drop that the space on the internet is a media environment that encompasses the 'world stage' of politics. That is the internet as a media environment provides the space in which international relations are played out and a site at which it can be observed the ways in which different groups and governments have adapted to this changing media environment. One of the ways that international relations are played out is via information warfare.

NORTH KOREA CASE STUDY

One nation actively engaged in information warfare is the Democratic People's Republic of Korea's (DPRK), or North Korea. North Korea has a population of approximately 23 million people, where the majority earn low incomes (World Bank, 2008). In a study conducted in 2003 by Giacomello, Korea was ranked 10th out of 57 countries in their ability to launch information warfare type attacks. Communist North Korea, one of the most secretive countries in the world, has been lead by a military dictator Kim Jong-il of the Kim dynasty, since 1994. Kim Jong-il has a keen interest in information technology although computers and access to the internet are tightly controlled for the general public (Deibert, Palfrey, Rohozinski, & Zittrain, 2008).

It is often reported in the South Korean and western media that North Korea has carried out hack attacks on South Korea and as such, the relationship between North Korea and the international community is in part played out and visualised on the internet. For example in October 2010 the South Korean press accused North Korea of hacking into the South Korea water supply and drainage systems, and there were suggestions by government officials that it was an attempt to disrupt the November G20 Summit to be held in Seoul. A Korean Broadcasting System report also suggested that the government was investigating the abandonment by several members of a Chinese tour group and whether or not this was linked to terrorism ("NK Attempted to Hack Data on S.Korea's Water Supply" 2010). There seems to be little evidence to substantiate the claims, but what is significant is that the reports serve as an illustration of the relationship between North and South and the way in which that relationship is played out in the media and potentially on the internet via hacking activities.

North Korea is often reported in the media, to have trained computer hackers to launch cyber attacks against other countries such as the United States of America (USA) and South Korea (Security Focus, 2004). It is believed that cheap second hand computers that are capable of achieving Kim Jong-il 's aims are utilised (Mezei, n.d.). North Korea is believed to have a sanctioned budget for administering a cyberwarfare unit (Mezei, n.d.). This unit is believed to be responsible for hacking into USA and South Korean military networks to gather confidential information and disrupt service (Fox News, 2009). Hacking training begins as early as 10 years of age at the Mangyongdae Schoolchildren's Palace and that technology education continues into senior middle school, specifically at the Kumsong secondary schools (Madden, 2009a*)*. North Korea however, doesn't appear to be restricted by internal legal ramifications for hacking as are other nations.

North Korea is accused of launching global cyber attacks in an attempt to gain intelligence. North Korea however, has little infrastructure of interest or value for other nations to attack. Although, North Koreas' nuclear arms potential is a concern. Takahashi (2010) believes that North Korea could build a cyber army to attack and defeat the USA. He believes this could be achieved by launching malware to infect approximately 100 million computers distributed across the globe. Once infected, upon instruction this botnet could launch an attack on critical infrastructure. The cyber attack would be difficult to defend against as the attack would utilise dispersed computing power and bandwidth. Further once launched, it would be very difficult to determine exactly who the aggressor was.

The internet plays a role in the way in which North Korea's relationship with the international community is played out via online activities and this includes hacking and other forms of cyberwarfare. North Korea's foray into the digital world is not solely confined to hacking. The Korean Central News Agency has an online presence and there have been suggestions that North Korea has Facebook pages and Kim il Jong can also be found on Twitter, though Pyongyang denies this and claims it is a hoax (Buley, 2010). Either way the Pyongyang's relationship with the international community is visualised and played out via the media.

ISRAEL, THE USA AND STUXNET

The USA too is believed to be developing plans for cyberwarfare attacks. A 2007 report to Congress suggested that offensive action was not taken against Iraq's banking system, during the conflict, because Iraq's banking network was connected to financial communications networks in Europe (Wilson, 2007, p.9). In 2010 a form of malware known as Stuxnet emerged and is thought to have been developed by the USA or Israel.

Whilst free downloadable hacking software has been available for some time, the release of Stuxnet worm in June 2010 has introduced a new era of cyber warfare. The malware worm acts as a smart software bomb which is able to replicate itself from machine to machine until it infiltrates network control facilities to destroy them (Langner, 2010). Further, Stuxnet has the capability, once on a computer system, to hide its presence (ABC, 2010). "Stuxnet was tailored for Siemens supervisory control and data acquisition (SCADA) systems commonly

used to manage water supplies, oil rigs, power plants and other industrial facilities" (ABC, 2010). It is considered to be the most sophisticated malware ever created (ComputerWorld, 2010). "Welcome to cyber war," says Langner (2010), a cyber security expert in a post on his website.

In August Symantec reported that up to 60% of the computers infected with Stuxnet were located in Iran, and it has been suggested that Iran's nuclear power plants were the target (ComputerWorld, 2010; Thakur, 2010). There continues to be much speculation about the origins of Stuxnet and media reports in the *New York Times, The Guardian* and the *BBC* suggest that it is Israel or the USA who has developed the Stuxnet worm (Fildes, 2010; Halliday, 2010; Markoff & Sanger, 2010). The clues as to the origins are based on instructions in the Stuxnet code that appear to exempt Israel from an attack (ComputerWorld, 2010). "Stuxnet's complex design and SCADA target has led many to conclude that it was the work of a state-backed group of hackers" (ComputerWorld, 2010). What is concerning is that this software toolkit can be downloaded from the internet and adapted as part of any countries cyber weaponry.

All governments appear to be investing in both network protection and destruction. It seems likely that Stuxnet has been developed by a government given the complexity of the malware and the financial resources required to create software with that degree of sophistication. It is not just a concern that China and North Korea could get hold of the technology, but what is really happening is that there is a kind of virtual arms race going on, and it is played out on the internet, rather than being just confined to conventional warfare technology. Globally therefore, governments will need to commit resources to maintaining their cyber security efforts. If this is not done, then attacking nations may develop new technologies and methods of infiltration that could be difficult to defend against (USPatriot, 2007). It may be that a catastrophic cyber event may soon occur.

This case study on Stuxnet also serves as an illustration in the ways in which the internet acts as a site in which international relations are played out and can be visualised. Despite the fact that no country has officially claimed responsibility for the development and the deploying of Stuxnet, the reporting of the spread and the locations that it has been found in paint a picture of some of the more clandestine aspects of international relations.

CONCLUSION

The potential for information warfare is vast and is of concern to all nations and national security defence. The internet plays a role in the visualisation and articulation of international relations both officially and unofficially. North Korea's relationship with the international community can be best viewed in the space of the internet. Because of the secretive nature of North Korea and their antagonistic relationship with the international community, the internet becomes one of a limited number, of mediums in which the countries relationship with the rest of the world can be viewed and well documented in the Western press. This paper also discusses emerging cyber weaponry such as Stuxnet, a malware worm released in June 2010 which targets and destroys critical network infrastructure such as water supplies, oil rigs, power plants and other industrial facilities. The massive infections in Iran indicated that that country's infrastructure, possibly its nuclear facilities, was the intended target of Stuxnet. Future battles therefore, will be conducted in both 'real' space and cyberspace. However, North Korea is not the only country to actively engage in cyber warfare. It appears that most countries are actively trying to protect networks, while potentially looking for ways to bring down the networks of other countries, and this is not officially acknowledged.

REFERENCES

ABC. (2010). Software smart bomb aimed at Iran: experts. Retrieved October 4, 2010 from http://www.abc.net.au/science/articles/2010/09/24/3021334.htm

Anderson, B. (2006). *Imagined Communites Reflections on the Origin and Spread of Nationalism* (Revised ed.). London: Verso.

Buley, T. (2010). North Korea Tells Forbes That It Is Not Using Twitter, Facebook Or YouTube. *Journal*. Retrieved from http://blogs.forbes.com/taylorbuley/2010/08/23/north-korea-tells-forbes-that-its-not-using-twitter-facebook-or-youtube/

ComputerWorld. (2010). Stuxnet code hints at possible Israeli origin, researchers say. Retrieved November 11, 2010 from http://www.computerworld.com/s/article/9188982/Stuxnet_code_hints_at_possible_Israeli_origin_researchers_say

Deibert, R. J. (1997). *Parchment, Printing, and Hypermedia Communication in World Order Transformation*. New York: Columbia University Press.

Deibert, R. J., & Rohozinski, R. (2009). *Tracking GhostNet: Investigating a Cyber Espionage Network*: Information Warfare Monitor. Retrieved November 11, 2010 from http://www.infowar-monitor.net/2009/09/tracking-ghostnet-investigating-a-cyber-espionage-network/

Deibert, R. J., Palfrey, J. G., Rohozinski, R., & Zittrain, J. (Eds.). (2008). *Access Denied. The Practice and Policy of Global Internet Filtering*. Cambridge: The MIT Press.

Fildes, J. (2010). Stuxnet worm 'targeted high-value Iranian assets'. *Journal*. Retrieved from http://www.bbc.co.uk/news/technology-11388018

Fox News, Associated Press. (2009). Report: N. Korea Attempting to Hack U.S. Networks. Retrieved September 21, 2010 from http://www.foxnews.com/story/0,2933,518915,00.html

Giacomello, G. (2003). Measuring 'Digital Wars': Learning from the experience of peace research and arms control. Infocon Magazine, 1 (Oct). Retrieved from http://www.iwar.org/infocon/

Halliday, J. (2010). Stuxnet worm is the 'work of a national government agency'. *Journal*. Retrieved from http://www.guardian.co.uk/technology/2010/sep/24/stuxnet-wormnational-agency

Hartley, J. (1992). *The Politics of Pictures: The creation of the public in the age of popular media*. London: Routledge.

Hearn, K. (2009). *Circumnavigating the Great Firewall* in Chong A., & Bin Yahya, F. (eds) *Alterity between Online and Offline Politics forth coming.* International Convention of Asia Scholars 6 (ICAS6). August 6 – 9, 2009 / Daejeon Convention Center, Korea.

Innis, H. A. (1951). *The Bias of Communication*. Toronto: University of Toronto Press.

Innis, H. A. (1952). *Changing concepts of time*. Toronto: University of Toronto Press.

Innis, H. A. (1972). *Empire and Communication* (2 ed.). Toronto: University of Toronto Press.

Kim Jong-il: Encyclopedia. Retrieved September 27, 2010 from http://www.associatepublisher.com/e/k/ki/kim_jong-il.htm

Langner, R. (2010). Stuxnet is targeted attack - Hack of the decade. Retrieved October 4, 2010 from http://translate.google.com.au/translate?hl=en&sl=de&u=http://www.langner.com/&ei=TGCpTKCYDozQcbmgneQN&sa=X&oi=translate&ct=result&resnum=1&ved=0CBwQ7gEwAA&prev=/search%3Fq%3DRalph%2BLangner%26hl%3Den%26rls%3Dcom. microsoft:en-us:IE-SearchBox%26prmd%3Do

Libicki, M. (1995). What is information warfare? *Strategic Forum 28* (May). Washington DC: National Defense University.

Listverse. (2010). 10 "facts" about Kim Jong Il, as reported by the media . http://listverse.com/2010/05/30/top-10-crazy-facts-about-kim-jong-il/

Madden, M. (2009a). Hacking at an Early Age. Retrieved September 21, 2010 from http://nkleadershipwatch.wordpress.com/2009/10/24/hacking-at-an-early-age/

Madden, M. (2009b). NK's PR Cyber Blitz in South Korea. Retrieved September 27, 2010 from http://nkleadershipwatch.wordpress.com/category/cyber-warfare/

Markoff, J., & Sanger, D. E. (2010). In a Computer Worm, a Possible Biblical Clue. *Journal,* (September 29, 2010). Retrieved from http://www.nytimes.com/2010/09/30/world/middleeast/30worm.html?_r=3&hpw=&pagewanted=print>

Mezei, A. D. (n.d.). North Korea Blues - More On Those Secret Cyber Attacks. Retrieved September 27, 2010 from http://therealadm.posterous.com/north-korea-blues-more-onthose- secret-cyber

NK Attempted to Hack Data on S.Korea's Water Supply'. (2010, 2010-10-20 08:11:24). from http://world.kbs.co.kr/english/news/news_Dm_detail.htm?No=76502

PLA. (2002). *Full text of China's defense white paper in 2002*. Retrieved 18/10/07. From http://news.xinhuanet.com/english/2002-12/10/content_654851.htm.

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

Security Focus. (2004). North Korea has 600 computer hackers, South Korea claims. Retrieved September 21, 2010 from http://www.securityfocus.com/news/9649

Steiden, B. (2010). N. Korea succession awaited: One of the most secretive and controversial nations in the world could be close to a change in leadership. The Atlanta Journal – Constitution, 16. Retrieved September 27, 2010 from ProQuest Database.

Takahashi, D. (2010). How North Korea could build a cyber army to defeat the U.S. Retrieved October 6, 2010 from http://venturebeat.com/2010/07/31/how-north-koreacould- build-a-cyber-army-to-defeat-the-u-s/

Thakur, V. (2010). W32.Stuxnet — Network Information. *Journal*. Retrieved from http://www.symantec.com/connect/blogs/w32stuxnet-network-information

The Official Webpage of The Democratic People's Republic of Korea (DPRK). Retrieved September 20, 2010 from http://www.korea-dpr.com/

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

USPatriot. (2007). China and North Korea Hacking. Retrieved September 21, 2010 from http://www.usmilitary.com/blogs/975/china-and-north-korea-hacking/

Widnall, S.E., & Fogelman, R.R. (1997). Cornerstones of information warfare.USAF publication. Retrieved from http://www.dtic.mil/cgibin/ GetTRDoc?AD=ADA323807&Location=U2&doc=GetTRDoc.pdf

Williams, M. (2010). North Korea opens up Internet for national anniversary. *Journal*. Retrieved from http://www.computerworld.com/s/article/9190238/North_Korea_opens_up_Internet_for_national_anniversary?taxonomyId=18&pageNumber=2

Williams, M. (2010). North Korean hackers probe South, say reports. *Journal*. Retrieved from http://www.northkoreatech.org/2010/10/21/north-korean-hackers-probe-south-say-reports/

Wilson, C. (2007). *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*: Congressional Research Service.

World Bank. (2008). World Development Indicators by Country. Retrieved October 5, 2010 from http://data.worldbank.org/country/korea-democratic-republic

Wu, X. (2006). Chinese Cyber Nationalism: evolution characteristics and implications.