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*

Follow this and additional works at: [https://ro.ecu.edu.au/isw](https://ro.ecu.edu.au/isw)

Part of the Information Security Commons

DOI: 10.4225/75/57a82cadaa0e0

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.
International Relations and Cyber Attacks: Official and Unofficial Discourse

Kay Hearn¹, Patricia A H Williams²,³ & Rachel J Mahncke³

¹School of Communication and Arts, Edith Cowan University
Perth, Western Australia

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

³School 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 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 Benedict 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 incident was played virtually in a spate of ‘tit for tat’ hack attacks on 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 multilocal 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
June 2010 has introduced a new era of cyber warfare. The malware worm acts as a smart software bomb which whilst free downloadable hacking software has been available for some time, the release of Stuxnet worm in 2010 a form of malware known as Stuxnet emerged and is thought to have been developed by the USA or Israel. Whilst offensive action was not taken against Iraq's banking system, during the conflict, because Iraq's 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 Jong-il 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). 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


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.


