

CYBER WARFARE

Prepared for: United Nations Security Council, ConnectMUN 2011
Director: Atiya Jaffar
Chair: Laith Sarhan
Crisis Director: Mike Koole

BACKGROUND

Cyber warfare has plagued information systems since the introduction of the World Wide Web in 1990. It involves offensive and defensive operations using information technology to attack other computers or networks. The perpetrators of these actions are generally people well versed in the intricacies of software programming, and their activities have the potential to be secretly protected or sanctioned by nation-state actors. Cyber attacks range from denial of services attacks, the use of viruses to gain access to confidential information, and

There are two primary categories of cyber attacks: cyber warfare and cyber terrorism. An act of cyber warfare has a defined target in a war that may be ideological or declared, while cyber terrorism is a means of instilling fear within everyone in a certain population.

A common form of cyber attacks is the interference with IT resources controlling critical national infrastructures, such as water supply, power grid, or air traffic, through manipulation of the SCADA (supervisory control and data acquisition) system. An example of such an attack occurred in 2000, when an offender hacked into Maroochy Shire, Australia's waste management control system and released millions of gallons of raw sewage into the town. Specific methods of cyber attacks include phishing, the practice of enticing a victim to visit a certain online website with the intention of stealing credentials, financial information such as bank accounts, or credit card number. Another form is DDOs which comes as a class of attacks that results in the exhaustion of computing or communications resources by engaging many intermediate computers to simultaneously request information from one victim.

In international and interstate politics, cyber conflicts have three major links to tangible conflicts. Firstly, physical attacks are generally followed by cyber attacks. Directly following the drowning of an American plane along the coast of China, both sides proceeded to launch cyber attacks against each other. Similarly,

in areas of on-going armistice but escalating tension, cyber warfare is also common; delegates are highly encouraged to research into tactics employed during the Pakistan/India conflict, the Israeli/Palestinian conflict and the Balkan War.

Cyber attacks on public institutions are often intended to represent high publicity value. Multinational corporations such as Microsoft, Boeing and Ford in the United States are top targets. Several measures can be exercised in order to prevent cyber attacks. Physical protection strategies include having certain information intensive areas off limits to unauthorized personnel, establishing barriers against the theft or destruction of sensitive IT equipment, and prevention of unauthorized reading of visual, acoustic or analog signals. Virus scanners and firewalls are deterrent forms of software. As well, screening employment is a strong organizational defense.

In contrast to attacks on national corporations, attacks on governments are usually kept quiet by government officials. Delegates are highly encouraged to read files released by Wikileaks (<http://www.telegraph.co.uk/news/wikileaks-files/china-wikileaks/>) to understand the conflict between China and the US regarding the security of satellites in space, which are responsible for relaying GPS, communication, and combat data. Attacks on these satellites would hinder the ability of the United States government to respond during armed conflicts.

There have been increasing incidences of high profile cyber attacks in the international community. In February 2011, the Canadian government released information about a cyber attack targeting the federal Department of Defense Research and Development. The hackers also were able to access highly classified federal information and forced the Financial Department and Treasury Board of Canada off the internet. Evidence traces the attacks to computer servers in Canada but it is still unclear whether it was perpetuated by the Chinese government. Later this year, Russia publicly alleged that the United States and Israel had launched the vicious Stuxnet virus to attack the Iranian nuclear program. Furthermore, in response to the publication of the so-called whistleblowing site, WikiLeaks in November 2010, many countries, most notably the United States, launched a DDOS campaign to prevent civilians from accessing data on the website.

Debate over cyber warfare is newly born in the United States and the United Kingdom and in foreign policy dialogue between the USA and Russia. However, the majority of this debate is considered highly sensitive and occurs primarily behind closed doors. Although there exists a committee to address the issue of cyber security, Industrial Automation and Control Systems Security (ISA 99), National and international understanding, strategy and means of implementing collaborative prevention remain undeveloped. A suggested deterrent has been establishing legal and diplomatic initiatives, both bilateral and multilateral, during

international conferences modeled after the naval disarmament conferences that took place in the 1920s and 1930s.

QUESTIONS TO CONSIDER

- 1) Should there be international institutions in place to police actively police potential acts of cyber crime?
- 2) What international agreements should be put in place when cyber crime is detected and proven?
- 3) What proofs are needed?
- 4) Should countries be responsible for tracking down hackers in their own countries?
- 5) Should cyber attacks be considered declarations of war?
- 6) Should countries construct alliances to act if one country is attacked by another?

SOURCES

Introduction to Cyber Warfare and Cyber Terrorism
In *Cyber Warfare and Cyber Terrorism* (Published 2007)
by Lech J. Janczewski and Andrew M. Colarik (eds)

Ch. V Infrastructures of Cyber Warfare
In *Cyber Warfare and Cyber Terrorism* (Published 2007)
by Lech J. Janczewski and Andrew M. Colarik (eds)

Cyber Warfare: Law and Governance Proposals for the US and Global Governance
by Stuart S. Malawer (Published 2010)

<http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf>

<http://www.cbc.ca/news/politics/story/2011/02/16/pol-weston-hacking.html>

<http://www.physorg.com/news/2011-09-russia-believes-israel-iran-worm.html>

<http://www.sciencedirect.com/science/article/pii/S175445481170002X>