



FIRST GENERAL ASSEMBLY

**Questioning the Threat to International Security Posed by
Cyber Attacks**

BACKGROUND PAPER

**Mark Loong
Reece Milburn**

Committee and Mandate

The 1st General Assembly of the United Nations (UN) is a subsidiary committee of the UN General Assembly that deals with issues of disarmament and international security not already covered by the Security Council. The Assembly is a space for States to discuss positions and to forge resolutions on issues such as minimising weapons spending, maximising global security (through non-proliferating methods), and reducing arms trade, production, and stockpiles.

As a delegate in this committee you will represent your designated country and its interests as the international community seeks to understand the scope of cyber warfare and limit its potential as an international security threat. There are also multiple facets to cyber warfare that need to be addressed, being that the difficulties in differentiating state based cyber attacks from those of non-state actors result in the need for not only international cooperation in the prevention of cyber warfare but also state based measure to prevent non-state actors within their borders from engaging in hostile cyber activity.

A Brief Overview of Cyber Attacks

General

Cyber-warfare presents an unprecedented paradigm and threat to international peace and security. Cyber-warfare attacks on military infrastructure, government, communications systems, and financial markets pose a rapidly growing decisive weapon of choice in present and future conflicts between states. Hostile governments potentially have the capability to hide behind rapidly advancing technology to launch attacks undetected. And unlike conventional and nuclear arms, there are no agreed international controls on the use of cyber weapons. Further to this, cyber-warfare re-ignites questions of morality and freedom of access to information which have traditionally jaded the proliferation of global information communication technology. Now, ineffective multi-lateral answers to these questions present very real human consequences.

Over 1.7 billion people use the internet, or roughly 25% of the global population. In the developed world well over 50% of the population use the internet (IWS 2009). Financially, major banks all offer internet based banking and security and are interconnected via online networks. Economically, share markets and other trade platforms all utilise the internet as the primary means of information transfer. Civilian infrastructure is also heavily dependant on the internet, with advanced power plants and water treatment facilities allowing for remote monitoring and control. The military use the internet not just for restricted data but also for the operation of next-generation battle systems. This widespread use of the internet shows just how reliant the world is becoming on the internet, and how vulnerable it is to internet based attacks.

Cyber Warfare

Cyber warfare is a new form of conflict where, as the name suggests, belligerents engage in conflict primarily through telecommunication and virtual avenues to inflict damage to civilian and military systems or to extract restricted information. This method of conflict offers the advantage of being deniable and relatively non-destructive. The actions involved in cyber attacks are difficult to prove, and ever harder to pin-point blame (Lewis 2009:1). Past attacks that have appeared to be state based have been denied and blamed on freelance groups.

The inability to discern between government attacks and those conducted by freelance groups or individuals provides states with a cloak to hide aggressive actions. In addition to being deniable, as the actions are primarily information based, the physical impact and harm is far less than what would be experienced in a conventional attack of the same scale. Someone shutting down a power station or taking a government database off-line will result in minimal condemnation, if any, and avoids the military response that blowing up a power station or physically destroying government offices may result in. Given the strong appeal of using cyber warfare, rather than conventional means, to achieve strategic goals, it is important for the international community to create and implement measures that can prevent an escalation of this new style of conflict.

Cyber Terror

The use of cyber space for conducting campaigns is not just limited to states, individuals and groups are also capable of conducting attacks. For ideologically driven organisations the internet is used primarily for propaganda and misinformation purposes (Stohl 2007: 9) however the anonymous nature of cyber space has allowed groups to mount a variety of attacks both against opposing organisations as well as governments with the intention of silencing their communications or disrupting their ability to function normally.

There is also the use of the Internet to create purely psychological harm, rather than only attacking infrastructure. International video servers have been utilised by a diverse array of groups to post not just their ideological messages but also footage of the preparation of equipment for coming physical attacks but also the beheading of captives and the firing of rockets into Israel (Stohl 2007: 9)

Points to Consider

This topic provides a large amount of freedom within committee sessions. Unlike the majority of issues discussed by the 1st General Assembly, cyber attacks are still relatively new and such there has been very little formal debate on how the international community should respond. This gives you, the honourable delegates, the opportunity to find creative solutions to this complex problem without the constraints of past measures. This opportunity, however, comes with the responsibility to anticipate future developments and to draft a resolution that can pre-empt potential problems.

Some important questions to consider when drafting a resolution:

- What actions would your country support?
- What measures could realistically be taken to prevent cyber attacks?
- Who would be responsible for these measures?
- Should actions taken by states be dealt with differently from the actions taken by non-state actors?
- Who is responsible for responding to cyber attacks?
- Is Internet security a national or international responsibility?

Recommended Research Avenues

These resources offer further information regarding the development, use and implications of cyber attacks.

The Centre for Strategic and International Studies (CSIS) has a section devoted to cyber security. We have also noted two publications here that are especially relevant to the committee. A special thank you to our Under Secretary General for Committees for finding these resources.

<http://csis.org/category/topics/technology/cybersecurity>

http://csis.org/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_Conflict.pdf

http://csis.org/files/publication/100120_CyberEventsSince2006.pdf

Additionally, the forthcoming issue of *UQ's United Nations Student Association* publication, *Contribute*, features an in-depth analysis of Cyber Warfare. The article addresses cyber warfare in a Clausewitzian sense, scrutinising the use of cyber attacks as politics by other means". We highly recommend you read this article (and the rest of *Contribute*, which is a fantastic International Relations analysis resource) as a part of your preparations for BrizMUN 2010.



Reference List

Stohl, Michael. 2006. 'Cyber Terrorism: a Clear and Present Danger, the Aum of all Fears, Breaking Point or Patriot Games?' *Crime Law and Social Change* 24 (4-5).

Internet World Statistics (IWS). 2009. Internet World Statistics: Usage and Population statistics. Accessed 25 March 2010.
Available at: <http://www.internetworldstats.com>

Lewis, James. 2009. 'The "Korean" Cyber Attacks and Their Implications for Cyber Conflict'. *Center for Strategic and International Studies*.