Cyberspace, disarmament, and human security

Article 36 and Reaching Critical Will

Background

The 21st century has seen increasing social and economic reliance on computer networks and interlinked networks of critical infrastructure. These networks provide significant advantages to human society.

Cyber attacks present a broad spectrum of risks to individuals and societies. Such attacks can range from contraventions of individual or corporate privacy, mass espionage and surveillance, up to the disabling or destruction of infrastructures vital to the general population or the manipulation of elements of civilian infrastructure in order to use them as weapons.

Within this broad spectrum of cyber activity, different sorts of cyber attacks may require different responses and restrictions. It is a human rights imperative to protect privacy and respect for Internet freedoms. This part of the agenda is rightly being pursued in other forums, including in the Third Committee.

Whilst some cyber attacks may create impacts similar to those of kinetic attacks in armed conflict and others may have direct military or security implications without having direct physical effects, many will have effects that are separate from the military or security realms. In any case, the complexity of networks can mean that the full impact is hard to predict and so control. Treating cyber attacks primarily as a military and security issue risks a reflexive response that can escalate incidents, including misunderstandings, into armed conflict.

It also risks adopting a legal framework that is more permissive of harm to the population than international human rights law allows. In working to prevent cyber attacks, states should consider the full range of impacts on human rights, international humanitarian law, protection of civilians and state responsibility.

Current context

States have a responsibility to provide security to their citizens, but state practice across this spectrum of cyber issues is already concerning. Privacy intrusions, denial-of-service attacks and malware operations have been linked to states, without those states accepting any responsibility. Transparency is sorely lacking around states' cyber operations.

Within First Committee, work on cyber issues has been undertaken in four groups of governmental experts (GGEs). The first failed

CREDIT: FLICKR/YURI SAMOILOV

to reach consensus in 2005; however, the 2010, and 2013 groups issued substantive consensus reports. Many delegations were pleased with the consensus outcome of the 2013 GGE, noting the affirmation of existing international law, but also emphasised that further study of the application of norms is needed and that additional norms could be developed over time. Another GGE of 20 experts commenced its work in July 2014 with Brazil in the chair. It has the mandate of examining how international law applies to the use of information and communication technologies (ICTs), which requires identifying how technological features of ICTs affect the functioning of legal rules. This discussion reveals the differences between states in their competition for influence and power in cyberspace and beyond. "This context," notes a Council on Foreign Relations writer, "means that GGE discussions involve political sub-texts, particularly between the United States and China, that involve more than ICTs and that will make reaching anything more than superficial consensus difficult."[1]

It will be important for states to reach common understandings of the concepts they are debating. Likewise, understanding how existing laws, either national or international, can be applied to the cyber framework will be crucial. But all of this must be done with the objective of developing a legal framework that prevents cyber attacks, whether undertaken by states, by private entities contracted by states or by other institutions or individuals. Discussion of norms on mercenaries and private military contractors provide an illustration that contracted services need to be brought under standards of control. Furthermore, the dual use nature of civilian infrastructures in cyber space should not be used

an excuse to avoid strong rules to govern cyber operations by states.

We must also recognise a wider responsibility amongst the public and institutions of all kinds to build resilience alongside reliance on computer networks. While we seek to prevent cyber attacks by adopting and enforcing clear standards, we must also develop the capacity to survive them and to mitigate the damage that they can do.

Many delegations have noted the need to preserve the digital domain as a peaceful one. We share the goal of an Internet that is used only for peaceful purposes. We have an opportunity and a responsibility to act now, before we find ourselves locked in a new cyber arms race that could further destabilise our world.

Recommendations for governments

During First Committee:

- Delegations should express concern about the risk of cyber attacks and the militarisation of cyberspace.
- They should indicate support for the current GGE to develop concrete recommendations on preventing the development, deployment, and use of cyber weapons.
- They should also seek to establish new avenues for wider discussions open to all states and inclusive of civil society and other relevant actors. Including the voices of states from all regions, including low and middle income countries, will be crucial in this process.

Beyond First Committee:

- States should work towards adopting an effective international legal framework that will prevent cyber attacks and protect the networked infrastructure upon which societies rely for their wellbeing.

Article36

Reaching Critical Will

1 David Fidler, "How International Law Applies to Cyberspace," Net Politics, Council on Foreign Relations, 14 April 2015, http://blogs.cfr.org/cyber/2015/04/14/the-un-gge-on-cyber-issues-how-international-law-applies-to-cyberspace/.