Cyberpeace and the militarization of the Internet

Women’s International League for Peace and Freedom

Background

Given the impact of Edward Snowden’s revelations, the debate around the issue of cyber security and the resolution on “Developments in the field of information and telecommunications in the context of international security,” first introduced by Russia in 1998, will be an interesting one this year.

The resolution currently expresses concern about potential misuse and exploitation of information and communications technologies that would affect the military and civilian security of states; calls for multilateral consideration of measures to limit existing and potential threats; and calls on the Secretary General to compile a report based on member state views.

The resolution has been the mechanism through which four Groups of Governmental Experts (GGEs) have been established on this issue. The first failed to reach consensus in 2005; however, the 2010, and 2013 efforts were able to issue substantive consensus reports. Another GGE of 20 experts was established in 2013 and commenced its work in July 2014 with Brazil in the chair.

The text has changed only slightly over the years, thankfully replacing “mankind” with “humankind” in 2002, adding references to the World Summit on the Information Society (WSIS) as that process unfolded in 2003 and 2005, and issuing an annual thanks to UNIDIR for an expert group meeting in 1999. For the first time in 2013, and in the wake of Snowden’s revelations, the resolution noted the importance of respect for human rights and fundamental freedoms in the use of information and communications technologies.

The resolution has been adopted without a vote each year, except when the United States cast a sole negative vote from 2005 to 2008.

Many delegations were pleased with the consensus outcome of the 2013 GGE, noting the affirmation of existing international law, but also emphasized that further study of the application of norms is needed and that additional norms could be developed over time.

Current context

The last report was issued two weeks after the Snowden revelations came to light. Since then, the debate may have shifted, but policy has not. The language on the development and deployment of cyber weapons was struck from the NetMundial meeting hosted by Brazil in

April 2014 and similar language put in the "too hard" basket and erased from the document issued by the WSIS + 10 High Level Event in June. All

While it is generally accepted that "existing law applies," information security or cybersecurity is a very broad and untested spectrum, with particular difficulties faced in defining a weapon or attack. When do code-borne instruments of harm become weapons? When they damage a country's infrastructure systems and networks that result in physical damage to property, people and loss of life? While attacks could include denial of service that make websites inoperable, malware and viruses, financial fraud, stealing patents, identities, and information, are these really weapons? Depending on who does the attack and what it impacts, some attacks could have the effect of weapons, or spill over into physical armed conflict, while others would be unlawful, but not themselves weapons that cause physical damage human beings or to property through an attack on infrastructure, water supply, energy etc.

Deciding what comprises a threat, an instrument and act of violence in the context of cyber attacks is ongoing. As Harvard Fellow Camille Francois has asked, "The 2007 attacks in Estonia, the 2008 attacks in Georgia, the Stuxnet malware that targeted an Iranian uranium enrichment centrifuge in 2009 have given political urgency to this legal debate: How does the law address States attacking one another through cyber means?"[1] (emphasis added)

But there is not enough urgency to categorize and scrutinize the cyber weapons that are currently being developed and deployed by up to 100 countries, which in turn incentivize an expanding commercial market for the research and development of offensive cyber weaponry. Snowden has revealed that the NSA carried out over 230 offensive cyber operations in just one year (2011).[2] Perhaps the most dangerous parts of the surveillance that Snowden has revealed are the 50,000 Computer Network Exploitations (CNE),[3] software implants in other countries' telecoms networks that have the ability not only to tap into the data streams of these networks but also to disable them, armed and activated with a single command.

Bruce Schneier, one of the world's leading security experts has written[4] on the need for a treaty banning cyberwar: "We're in the early years of a cyberwar arms race. It's expensive, it's destabilizing, and it threatens the very fabric of the Internet we use every day. Cyberwar treaties, as imperfect as they might be, are the only way to contain the threat."

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 address Snowden's revelations in this regard and the development of concrete recommendations on preventing the development, deployment, and use of cyber weapons.

Beyond First Committee:

- States should seek to develop commitments and instruments to prevent the militarisation of cyber space, including a treaty banning cyber warfare.

[1] Camille François, "A Roadmap to Cyberpeace," 11 March 2012, http://cyber.law.harvard.edu/events/luncheon/2014/03/francois.

[2] Barton Gellman and Ellen Nakashima, "U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show," The Washington Post, 30 August 2013, http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html.

[3] Nathan Mattise, "Report: NSA-planted malware spans five continents, 50,000 computer networks," Ars Technica, 24 November 2013, http://arstechnica.com/tech-policy/2013/11/report-nsa-planted-malware-spans-five-continents-50000-computer-networks/.

[4] Bruce Schneier, Cyberwar Treaties, https://www.schneier.com/crypto-gram-1206.html#2.