Cyber
Reaching Critical Wil/WILPF

Background

Few subjects are as multi-dimensional or present as many unique challenges as "cyber". It constitutes an ever-widening spectrum of activities and concerns affecting individuals, private industry, society, and governments alike. The aspects most relevant to international security and disarmament are likely that of inter-state cyber conflict or cyber attacks. These concepts lack universal agreement on their meaning, but could be broken down to include activities such as mass espionage and surveillance, privacy intrusions, denial-of-service attacks, and ransomware or malware operations with the potential to negatively impact, disable, or destroy vital infrastructure or national or human security.

Potential impacts are vague but worrying. It is true that some cyber-attacks can have impacts similar to those of kinetic attacks, but these modes of conflict are as yet purely speculative. In practice, the majority of attacks have information security implications and no direct physical effects. The last twelve months have presented new challenges though, with growing evidence of digital interference in at least two national elections by a foreign power and unprecedented ransomware attacks.[1] In approaching these issues, it is important to be wary overinflating the threat and tacitly promoting militarisation. Given the dual-use nature of what constitutes "weapons" in this sphere, an unaddressed problem is how governments regulate the manufacturers of malicious technologies; an issue that the Hacking Team case illustrates well.[2] There could be lessons in how other dual-use materials are treated or if existing arms control regimes can continue to expand[3] to encompass digital weaponry—if, the international community views them as such—which is something that civil society encourages states to question vigorously. The Internet is now essentially civilian infrastructure and as such it should not be made the target of or the medium for attacks. States should establish the strongest norms against such actions and attacks and not drift into an acceptance or legitimation of problematic emerging practice.

Agreement that existing international law, including international human rights law and international humanitarian law (IHL), applies to activities in cyberspace provides a shared baseline, but this should not be taken to mean that the existing legal framework is sufficient. There is a lack of clarity regarding which legal framework should have primacy in relation to certain actions, and challenges to the application of legal frameworks, including in terms of accountability. Existing frameworks may not adequately reflect a wider social interest in developing and preserving the public space of the Internet as a shared, non-militarised resource.

The cyber realm also potentially intersects with issues of militarism and war in relation to surveillance, intelligence, and warfighting or the operation of specific weapon systems. The installations and cyber networks associated with the "Five Eyes" surveillance network, for example, are frequently also critical nodes in contributing to the US government's wars and military interventions abroad, including by targeting drone strikes or nuclear weapons. Given this complexity, cyberspace needs to be addressed on its own terms, with consideration of its specific characteristics.[4]

Current context

The United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE on ICTs) is the most immediately relevant UN forum covering cyber issues for First Committee delegates. The first GGE on ICT was established in 2004.

Following the fourth Group's adoption of what many called a groundbreaking report in 2015,[5] expectations were high for the fifth Group, but unfortunately it was not able to agree to a consensus report at its final meeting in June 2017. Reportedly a major point of contention concerns the applicability of IHL to the ICT environment. Some states feel strongly that doing so legitimises cyber space as an arena of war while others feel that omitting IHL is unacceptable. Another area of significant disagreement was around if a cyber attack can trigger Article 51 of the UN Charter. It's likely that both GGE-participating and non-participating states will express views on these subjects during the First Committee.

The failure to agree on a report means that the General Assembly has no guidance on how to continue engaging in this aspect of the cyber issue. Suggestions reportedly include establishing an open-ended working group, a UN entity or high representative, or relocating the issue to the International Telecommunications Union (ITU). During last year's First Committee, a growing number of states and civil society criticised the lack of transparency of the Group; this is an issue that must be resolved for future progress.[6] It's possible that new resolutions could be introduced with any of these suggestions or that a proposal will be included in the annual Russian-led cyber resolution. The chair of the fifth GGE will deliver a minimal report or debrief during the First Committee.

Beyond First Committee, an Arria-formula meeting on cyber security and international peace and security took place in November 2016. Participants discussed challenges resulting from the use of ICTs that can threaten international peace and security. Some common themes and concerns emerged included a shared concern about cyber attacks on critical infrastructure and the necessity of developing international norms and confidence building measures.

Another part of the UN system that considers cyber issues are human rights bodies, largely in the context of rights to privacy and freedom of expression. While those aspects are outside the purview of First Committee, it is good to have an awareness that such dialogues occur and related resolutions exist. There are also obvious linkages between cyber security and First Committee subjects such as nuclear safety, autonomous lethal weapons, and the networked systems through which drones operate.

At national levels, there continues to be a growth in the articulation of official cyber doctrines and the establishment of relevant bodies, units, or departments both offensive and defensive. First Committee is an ideal opportunity for states to provide updates on such measures; this could also be accomplished by submitting an annual report to the Secretary-General on national efforts—a practice in which too few countries engage.[7]

Recommendations

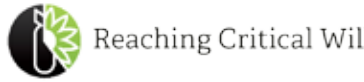
During First Committee, delegations should:

- Express concern about the risk of cyber attacks and the militarisation of cyberspace and promote a vision of the Internet as a shared public space that should not be the target of or medium for attacks;
- Work cooperatively to identify and establish an inclusive and transparent mechanism by which to continue work on behavioural norms in cyber space;
- Promote a fact-based discussion, avoiding language that over-inflates the threat and tacitly promotes militarisation;
- Advocate for common understandings within the international community around key terms and activities, in order to facilitate cooperation; and
- Commit to submit a report to the UN Secretary General

Beyond First Committee, states should:

- Uphold the behavioural norms that already enjoy broad support;
- Ensure information sharing between different international processes that address cyber issues, both within and outside of the UN system;
- Support technical capacity building initiatives; and
- Refrain from undertaking or facilitating any repression of human rights or freedoms through digital means.

Author: Allison Pytlak



1 Lily Hay Newman, "The biggest cyber security disasters of 2017 so far," *Wired*, 1 July 2017, https://www.wired.com/story/2017-biggest-hacks-so-far.

2 "Cyberwar for sale," *The New York Times*, 4 January 2017, https://www.nytimes.com/2017/01/04/magazine/cyberwar-for-sale.html.

3 "Wassenaar arrangement changes in multi-facated (digital) society," Tech and Law Center, 17 June 2015, http://techandlaw.net/wassenaar-arrangement-changes-in-multifaceted-digital-society.

4 For example, Menwith Hill in the United Kingdom, Pine Gap in Australia, and Waihopi in New Zealand/Aotearoa.

5 UN Doc A/70/174, available http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

6 Reporting on cyber issues during the 71st session of the UN First Committee was included several editions of in the 2016 *First Committee Monitor*, available online http://reachingcriticalwill.org/disarmament-fora/unga/2016/fcm.

7 Annual national reports are available on the UN Office of Disarmament Affairs website https://www.un.org/disarmament/topics/informationsecurity.