Cyber

Women's International League for Peace and Freedom

Background

The word "cyber" has come to represent an ever-widening spectrum of activities and concerns encompassing espionage, surveillance, privacy intrusions, denial-of-service attacks, and ransomware or malware operations. Many of these activities have the ability to negatively impact, disable, or destroy vital physical infrastructure or national or human security as well as constitute criminal activity. Cyber operations have become an effective tool for states seeking to disrupt or exercise power. Digital tools have also added new means by which states can control or repress their citizens while the "dark web" enables illicit arms trafficking. The cyber realm also potentially intersects with issues of militarism and war in relation to surveillance, intelligence, and the operation of specific weapon systems.

Since the first instances of malicious cyber operations between states were uncovered, there has been a growing pre-supposition of cyber space as a militarised one. This is a dangerous path for states to continue down, given the civilian and dual-use nature of cyberspace and digital networks. Such militarisation is evidenced in the increasingly formalised role of digital operations in military doctrine and strategy, as well as in the language used to depict activity in this arena, such as "cyber weapon," "cyber war," or "cyber bomb". By treating this primarily as a military and security issue, states and other actors risk institutionalising and taking for granted the broad idea of cyber conflict. In the on-going discussions about norms of responsible behaviour in cyberspace, it's essential that such norms are viewed as obligatory commitments and that space is also given to articulating a vision of cyber peace.

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.[1] The first GGE on ICT was established in 2004 and included experts from 15 nations, with a general purpose of examining existing and potential threats in cyberspace and possible cooperative measures to address them. Subsequent groups expanded the membership and worked to develop behavioural norms for actions in cyberspace. Following the fourth Group's adoption of what was generally regarded as a "groundbreaking" report in 2015,[2] expectations were high for the fifth Group, but it was unable to agree to a consensus report. Major points of contention were the applicability of international humanitarian law and Article

51 of the UN Charter to the ICT environment, over which the majority of participating Western states had views different to that of China, Russia, and Cuba.

The inability of the fifth GGE to agree on a report meant that there was also not sufficient agreement among states at the 2017 First Committee to adopt a mandate for a new Group to continue work on this issue. Governmental and expert statements in 2017 expressed frustration over the "collapse" of the GGE, reaffirmed commitments to abide by the norms established by past GGEs, or set out ideas for how best to pursue this subject in future. UNGA resolution A/72/404, "Developments in the field of information and telecommunications in the context of international security," was a procedural resolution introduced by Russia and adopted in 2017 by a vote of 185-0-1.[3] It ensured that the issue remains on the agenda in 2018. While formal work in the context of the UN General Assembly (UNGA) has stalled over the last year, some states have continued to push ahead in search of solutions for the stalemate. Germany, Switzerland, and Mexico have produced a non-paper titled that outlines various proposals that have been suggested. The non-paper ultimately proposes the establishment of a subsidiary body of the UNGA mandated to "build common understanding and provide guidance on how existing international law, non-binding norms of responsible State behavior, confidence-building and capacity-building measures can be implemented." The proposal is for the 15-member body to begin work in 2019 for a two-year period, consult with the wider UN membership, and report back to the General Assembly. It is expected that non-paper's proposal will be put forward as a resolution.

Pine Gap in Northern Territory, Australia. Run by the CIA and NSA, the facility is part of the Five Eyes surveillance network
© Kristian Laemmle-Ruff

It is also expected that Russia will introduce its annual resolution on ICTs, but with a recommendation to reconstitute the GGE. The draft resolution will also include language from Russia's draft International Code of Conduct for Information Security, meant as a basis for discussion in the new GGE. The draft Code was first introduced in 2011[4] and then updated in 2015[5] but has never gained significant political traction. The US will table a resolution calling for a new GGE, to base its discussions agreements reached by the most recent Group.

Recommendations

During First Committee, delegations should:

- Speak out against hostile and provocative actions in, and the militarisation of, cyberspace;
- Work cooperatively to identify and establish an inclusive and transparent mechanism by which to continue work on behavioural norms in cyber space and to promote a cyber peace approach; and
- Express concern about unlawful surveillance and digital censorship activities that violate human rights.

Beyond First Committee, states should:

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

Author: Allison Pytlak

1 For additional background, see the UN Office of Disarmament Affair's Fact Sheet, available https://s3.amazonaws.com/unoda-web/wp-content/uploads/2018/07/Information-Security-Fact-Sheet-July2018.pdf.

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

3 Voting record available at http://reachingcriticalwill.org/images/documents/Disarmament-fora/1com/1com17/votes/404.pdf.

4 UN Doc, A/66/359, available https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf.

5 UN Doc, A/69/723, https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf.