Statement on cyberspace and human security
UN General Assembly First Committee on Disarmament and International Security
12 October 2016

Over the last year, the public imagination has continued to be seized with the concept of cyber conflict. This is increasingly reflected in policy discussions at multiple levels and in multiple fora as well of course in popular media. Cyber attacks present a broad spectrum of risks to individuals and societies. Such attacks can include contraventions of individual or corporate privacy and mass espionage and surveillance up to the disabling or destruction of infrastructures vital to the general population and the manipulation of elements of civilian infrastructure in order to use them as weapons.

In the context of the United Nations, cyber security has been addressed primarily in the context of the Group of Governmental Experts on Information and Communication Technologies, which has continued its work in 2016. At national levels, there continues to be a growth in the articulation of cyber doctrines and the establishment of relevant bodies, units, or departments. In some instances these relate to potential cyber conflict and in others they are established to manage issues of cybercrime, espionage or security more broadly.

These many initiatives are welcome and demonstrate the increasing salience of the issue area. However they also demonstrate that "cyber" encompasses a broad spectrum of activities that will require different approaches. Some activities are relevant to the purpose and objectives of the First Committee, while others are being taken up in other spaces including beyond the UN. Forging connections between these initiatives and agreeing on common definitions and understanding are critical for progress in this area, as the rate of technological change rapidly outpaces that of diplomatic negotiation. The GGE has served as a helpful place to explore the issue but does not have the mandate or ability to actualize the behavioural norms it is discussing.

There are two further points that we want especially to underscore in this statement.

The first relates to the assumption of cyber space as being a militarized one. Treating cyber primarily as a military and security issue risks institutionalising the broad idea of cyber conflict. This may lead to preparations that escalate the threat, and responses that unnecessarily escalate incidents, including misunderstandings, into armed conflict. It also risks adopting a 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. In approaching these issues, it is therefore important to be wary of overinflating the threat, and in doing so promoting militarisation and escalation. We should remember that the Internet is essentially civilian infrastructure and should not be made the target of or the medium for attacks.

Second, we have seen an increase in negative use of cyber technology by state actors in the repression of human rights, notably the right to freedom of expression, and cracking down on the ability of civilians to communicate electronically or access email, news, or social media platforms. 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 and at the Human Rights Council, but should not be completely divorced from how delegates in First Committee approach this subject.

If normative progress is to be made in this area, states will need to go beyond a reiteration of existing, general rules and recognise that cyberspace needs to be addressed on its own terms, with consideration of its specific characteristics.

Recommendations

During First Committee, delegations should express concern about the risk of cyber attacks and the militarisation of cyberspace, and they should promote a vision of the Internet as a shared public space that should not be the target of or medium for attacks.

Delegations should also indicate support for the current GGE to develop concrete recommendations on preventing the development, deployment, and use of cyber weapons, cyber attacks or other intrusions or interference.

Beyond First Committee, states should seek to establish new avenues for wider discussions on these issues open to all states and inclusive of civil society and other relevant actors, noting that including the voices of states from all regions, including low and middle income countries, will be crucial in this process. This should include discussions on an effective international legal framework that will prevent cyber attacks and protect the networked infrastructure upon which societies rely for their wellbeing.

States must refrain from any repression of human rights or freedoms through digital means; and work towards adopting an effective international legal framework that will prevent cyber attacks, intrusions, or interference and protect the networked infrastructure upon which societies rely for their wellbeing.

This statement has been endorsed by the following organisations:

Article 36

International Committee for Robot Arms Control

Nonviolence International Canada

PAX

Women's International League for Peace and Freedom