Civil society statement on cyber and human security
UN General Assembly First Committee on Disarmament and International Security
17 October 2018

Check against delivery

I am delivering this statement on behalf of ten other organisations, many of whom represent larger constituencies, to express our views on cyber and human security.

The word "cyber" has come to represent an ever-widening spectrum of activities and concerns. Many of these have the ability to negatively impact, disable, or destroy vital physical infrastructure or national or human security. Cyber operations have become an effective tool for states seeking to disrupt or exercise power, and a primary method for the conduct of espionage.

This year at the First Committee, states will decide the mechanism through which they will work collectively to address many of these threats. It appears likely that agreement will be reached on creating a new Group of Governmental Experts (GGE) on the issue. Over the course of the General Debate, we have heard strong calls of support for reviving either this, or another, entity, yet this has included at times different views regarding mandate and composition.

It is imperative that a more transparent and inclusive entity be established. During a UN General Assembly high-level event on cyber security on 25 September, a strong case was made for the stake of developing countries in these discussions. Incorporating the views of the broader UN membership as a starting point, rather than as an after-thought, can only benefit the longer-term legitimacy and utility of any outcomes a future entity produces. There is also a very necessary role for civil society and the private sector in this work.

The organisations endorsing this statement are concerned about the growing militarisation of cyber space and supportive of solutions that move the global community closer to cyber peace. This militarisation is manifesting through the adoption of offensive strategies and doctrines; aggressive behaviours; or simply in the vocabulary used to describe this medium and actions within it. Accepting the militarisation of cyber space without question further risks adopting frameworks and guidelines that are more permissive of harm to the population than international law allows, and pushes the possibility of achieving cyber peace further away.

To counteract this trend, states should establish the strongest norms against such operations and not drift into an acceptance or legitimisation of problematic emerging practice. Agreement that existing international law, including international human rights law and international humanitarian law applies to activities in cyberspace provides a shared baseline. But this should not be taken to mean that the existing legal framework is sufficient.

Efforts need to also be made to reduce the motivation to pursue aggressive cyber capabilities and proactively advance cyber peace. To that end, the 2015 GGE report promoted a number of positive recommendations meant to diminish the utility of investing in offensive cyber capabilities, and to reduce the likelihood and likely harm of cyber attacks.

Positive recommendations are one way to challenge a militarised approach. Another is to put the human rights and the humanitarian impact of misused digital technologies at the centre of discussion. Treating cyber space and related actions in

a sanitised, faceless way risks institutionalising and taking for granted the broader idea of cyber conflict. It's vital that future UN discussions do not overlook the real-life repercussions that malicious intergovernmental operations can have on citizens; consider the 2017 WannaCry attacks, in which there were tangible and immediate impacts on hospital patients and the provision of urgent medical care in the UK. That said, better research and information gathering on the humanitarian impact of inter-governmental operations should be encouraged.

There is however, an ever-growing and highly credible evidence base illustrating the negative uses of digital technology in repressing human rights, notably the rights to freedom of expression, speech, assembly, and privacy. This is not a practice limited to just a handful of governments, but one that is practiced in many parts of the world. While the human rights part of the cyber agenda is rightly being pursued in other forums it cannot be separated entirely from discussions in the First Committee. Agreeing oversight and enforcement mechanisms to protect privacy and respect for freedom of expression online is important, as surveillance and censorship have repressed those rights. Doing so will contribute to a more secure cyber environment overall.

Statement prepared by the Women's International League for Peace and Freedom (WILPF)

Statement delivered by: Allison Pytlak, Reaching Critical Will of WILPF

Statement endorsed by:
Acronym Institute for Disarmament Diplomacy
Canadian Pugwash Group
Cyber Policy Institute
Environmentalists Against War
ICT4Peace
International Committee for Robot Arms Control
Project Ploughshares
PROTECTION
Seguridad Humana en Lationamerica y el Caribe (SEHLAC) Network
Women's International League for Peace and Freedom
World Beyond War