Civil society statement on cyber

UN General Assembly First Committee on Disarmament and International Security

10 October 2017

Headlines and journals abound with examples of cyber-based attacks, threats and problems. Between probable election interference by foreign powers in multiple national elections, an unprecedented rise in the use of ransomware, and hacking into vital information hubs, it’s clear that the threats in cyber space are only growing. It is also very clear that international law and policy is not keeping up with the pace of technological change.

The civil society groups that support this statement regret that the most recent UN Group of Governmental Experts (GGE) has not been able to identify a path forward. The deadlock within the group signifies that there are still deep global divisions and misunderstandings around key concepts concerning cyber security, which are likely to plague any multilateral efforts on cyber.

We believe that the GGE suffered from significant defects in terms of transparency, access, and mandate. The myth that only economically developed and technologically sophisticated countries are at risk of cyber attack is just that, a myth. Developing countries equally have a stake in these discussions, particularly as they rapidly “leap frog” forward in their technological modernisation. Technical, policy, and academic experts must also be included in discussion. Those with such expertise are best placed to help policymakers foresee what a “cyber attack” actually looks like, or what so-called “cyber weapons” are truly made of. To be effective in the real world and viewed as legitimate any future UN body that deliberates on cyber security must include all such stakeholders and be open about its work.

Given this impasse in UN discussions, we believe it’s an opportune moment to put forward a few basic questions: how much more militarised are we going to allow cyberspace to become? When and under whose authority did it pass from a civilian domain to the so-called “fifth domain” of conflict, and how was that allowed to happen? Most importantly: what are the repercussions? By treating “cyber” primarily as a military and security issue we risk institutionalising and taking for granted the broad idea of cyber conflict. This may lead to preparations that inflate threat perceptions or to responses that unnecessarily escalate incidents into armed conflict in the kinetic, or offline world. The cyber realm also potentially intersects with issues of militarism and war in relation to surveillance, intelligence, and war fighting or the operation of specific weapon systems. 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.

This is one area where it’s not too late to turn back the clock. States can choose to elaborate methods to preserve cyber peace, rather than resign themselves to formulating the norms of cyber war.

We also wish to register our concern about the use of cyber technologies in the repression of human rights. From Thailand to Myanmar to Venezuela to Mexico to Egypt, among other countries, there has been an increase in the negative use of cyber technology by state actors in the repression of human rights, notably the right to freedom of expression. The technologies through which this happens are being
manufactured and sold by companies that exploit their dual-use nature. The human rights part of the cyber agenda is rightly being pursued in other forums, including in the Third Committee and at the Human Rights Council, but it is relevant to the First Committee if in fact, states consider software, malware, and other technology to be a form of armament and therefore subject to control. We encourage states to better consider how to protect the digital rights of people everywhere by improving regulation and standards for control over such items. It is a human rights imperative to protect privacy and respect for Internet freedoms.

As we move into thematic debate, we urge First Committee delegates to take into account, and respond to, the points and questions raised here — but we also support moving the debate forward in forums beyond the First Committee. Few subjects are as multi-dimensional or present as many unique challenges as cyber. Given its complexity, cyberspace needs to be addressed on its own terms, with consideration of its specific characteristics, including its overwhelmingly civilian nature.

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

**Statement delivered by** Allison Pytlak of the Women’s International League for Peace and Freedom (WILPF)

**Statement endorsed by:**

- Article 36
- International Committee for Robot Arms Control
- Protection Against Armaments and Conflict
- Niskanen Center
- Nuclear Age Peace Foundation
- PAX
- Women’s International League for Peace and Freedom


Paul Meyer, Adjunct Professor of International Studies, Simon Fraser University, and Chair, Canadian Pugwash Group