Civil society statement to First Committee on cyber, disarmament, and human security
28 October 2014, New York

The 21st century has seen increasing social and economic reliance on computer networks and interlinked networks of critical infrastructure. These networks provide significant advantages to human society.

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.

We recognise that amongst this broad spectrum of cyber activity, different sorts of cyber attacks may require different responses and restrictions. Indeed, 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.

Whilst some cyber attacks may create impacts similar to those of kinetic attacks in armed conflict and others may have direct military or security implications without having direct physical effects, many will have effects that are separate from the military or security realms. In any case, the complexity of networks can mean that the full impact is hard to predict and so control. Treating cyber attacks primarily as a military and security issue risks a reflexive response that can escalate incidents, including misunderstandings, into armed conflict.

It also risks adopting a legal 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.

States have a responsibility to provide security to their citizens, but state practice across this spectrum of cyber issues is already concerning. Privacy intrusions, denial-of-service attacks and malware operations have been linked to states, without those states accepting any responsibility. Transparency is sorely lacking around states’ cyber operations.

States must ensure a legal framework that prevents cyber attacks, whether undertaken by states, by private entities contracted by states or by other institutions or individuals. Discussion of norms on mercenaries and private military contractors provide an illustration that contracted services need to be brought under standards of control. Furthermore, the dual use nature of civilian infrastructures in cyber space should not be used an excuse to avoid strong rules to govern cyber operations by states.

We must recognise a wider responsibility amongst the public and institutions of all kinds to build resilience alongside reliance on computer networks. While we seek to prevent cyber attacks by adopting and enforcing clear standards, we must also develop the capacity to survive them and to mitigate the damage that they can do.

States should work towards adopting an effective international legal framework that will prevent cyber attacks and protect the networked infrastructure upon which societies rely for their wellbeing.

The GGE on ICT in the Context of International Security has allowed for initial discussions. As we move towards international action, wider discussions will be necessary in a variety of forums, open to all states and inclusive of civil society and other relevant actors. Including the voices of states from all regions, including low and middle income countries, will be crucial in this process.

Many delegations have noted the need to preserve the digital domain as a peaceful one. We share the goal of an Internet that is used only for peaceful purposes. We have an opportunity and a responsibility to act now, before we find ourselves locked in a new cyber arms race that could further destabilize our world.
This statement was drafted by Article 36 and has been endorsed by the following organisations:

Acronym Institute for Disarmament Diplomacy
Article 36
FundiPau (Fundacio per la Pau)
International Committee for Robot Arms Control
PAX
Peace Movement Aotearoa
Protection Against Armaments
Vertic
Women's International League for Peace and Freedom