Civil society statement to First Committee on cyber, disarmament, and human security
16 October 2015, New York

We are speaking as a group of civil society organisations concerned to avoid harm from the militarisation of cyberspace, to avoid the build up of offensive cyber capabilities, and to ensure human rights and freedom of expression whilst promoting cyber protection. With the 2015 report of the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, we have already seen cyber issues receiving greater attention at First Committee this year.

Cyber presents a diverse range of concerns – including the development of problematic state practices that suggest a lack of effective international legal and policy constraint. Privacy intrusions, mass surveillance, denial-of-service attacks and malware operations have been linked to states, often without those states accepting any responsibility.

Potential impacts from such activities include impairment of government administration, damage to critical infrastructure and the undermining of human rights. But in approaching these issues we should be wary of responses that overinflate the threat, and in doing so promote militarisation, or facilitate policies of escalation. Furthermore, protecting privacy and respect for freedom of expression online is a human rights imperative. Surveillance and censorship have repressed those rights, and concerns regarding the risks of cyber conflict in the future must not justify attacks on those rights in the present.

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. In particular, we should avoid focusing debate primarily within the framework of international humanitarian law, a legal framework more permissive of harm to the general public than is ordinarily allowed and where the practical implementation of rules is anyway disputed.

While there are valuable recommendations in the 2015 GGE report, those aimed at constraining offensive behaviour tend to be framed in subservience to existing law in a way that may render them hollow. 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 in its own terms, with consideration of its specific characteristics. The Internet is essentially civilian infrastructure. As such it should not be made the target or the medium for attacks. States should establish the strongest norms against such attacks and not drift into an acceptance or legitimation of established practice. To this end, we see merit in the negotiation of new principles, procedures, rules, and norms.

Alongside further developing norms against cyber attacks and intrusions, efforts should be made to curtail the likely effectiveness of such attacks and so reduce the motivation to pursue aggressive capabilities. This can be done through effective cyber-protection. In this area, the recent GGE report promotes a number of positive recommendations to diminish the utility of investing in offensive cyber capabilities, and to reduce the likelihood and likely harm of cyber attacks. These include testing to identify vulnerabilities in vital networks; the timely, comprehensive, and responsible disclosure of such vulnerabilities; the strengthening of capacity amongst response teams; and the promotion of international cooperation.

Apart from discussion in the GGE, States have been meeting in other forums. These have included the Global Conference on Cyberspace hosted by the Netherlands in April, as well as the Global Cooperation in Cyberspace Initiative, and discussions at regional or bilateral levels. We urge that further work to develop a stronger policy and legal framework be open to all states and inclusive of civil society and other relevant stakeholders. Our shared reliance on the structures of cyberspace means that inclusivity will be vital to credible and effective international action in this area.

In conclusion, as states develop further the international policy and legal framework they should pursue an approach that works against cyber attacks and intrusions, whether in crime or conflict; that requires and promotes the actions necessary to reduce opportunities for attacks and to mitigate any harm they might cause; and that ensures the protection of human rights. Such a framework should promote an Internet that is used for peaceful purposes, and that resists the current drift towards normalising offensive capabilities. The cyber domain provides a unique tool for our collective social development: as such it deserves policy and legal protections that respect this vital role.

This statement has been endorsed by the following organisations: