The role of parliamentarians to advance disarmament in cyber space: a focus on cyber-warfare and peace

On 27 January 2021, the Geneva Centre for Security Policy (GCSP), the Inter-Parliamentary Union (IPU), the World Future Council (WFC) and Parliamentarians for Nuclear Non-proliferation and Disarmament (PNND) hosted a webinar on 'The role of parliamentarians to advance disarmament in cyber-space'. This event was held as a follow-up to the release in November 2020 of *Assuring our Common Future*, a parliamentary handbook on disarmament for security and sustainable development. The webinar brought together over 200 participants, including parliamentarians, leading experts on cybersecurity and disarmament, academics, students and members of civil society. In addition, the French edition of the parliamentary handbook was launched at the event, which took place in English with simultaneous French interpretation.

Marc Finaud, Head of Arms Proliferation at the GCSP, the moderator of this webinar, introduced the session, referring in particular to the parliamentary handbook's section on 'Disarmament for future generations' which includes the issues of cyberwarfare, and peace and disarmament in cyberspace. Mr. Finaud helped to clarify thinking on this issue by citing definitions and explanations of cyber-space, cyber-warfare and cyber-security. He noted that the webinar was timely as cyber insecurity is increasingly being recognised as a growing threat, with the World Economic Forum's Global Risks Report 2021 citing it as "among the highest likelihood risks of the next ten years" and the *Bulletin of Atomic Scientists* citing "destabilizing advances" in the development of cyber weapons as one of the reasons for the group's decision on 27 January 2021 to keep the Doomsday Clock at 100 seconds to midnight – indicating the highest level of existential threat to humanity yet.

Anda Filip, the IPU's Director for Member Parliaments and External Relations, introduced the French edition of the parliamentary handbook *Assuring our Common Future*. In her introduction, she emphasized the key role played by parliamentarians in advancing disarmament matters, and how parliaments are a key institutional component for change. Ms. Filip referred to the Handbook as a 'community document', as it was created with inputs from many partners including with the support of the UN Office for Disarmament Affairs. Ms. Filip also emphasized the good practices, policy models and concrete suggestions for actions put forward in the handbook and stressed the potential impact that it can have in supporting parliamentarians becoming "champions of the cause" in advancing the disarmament agenda.

Saber Chowdhury, Honorary President of the IPU, Vice-President of PNND and member of parliament in Bangladesh, recalled the IPU Resolution 'Cyber-warfare: A serious threat to peace and security', which was adopted at the 132nd IPU Assembly in Hanoi, Vietnam in 2015, the first IPU Assembly he had presided over as President. Mr. Chowdhury argued that the role of parliamentarians is being redefined, changed and challenged. In the context of these global issues, parliaments have to adopt a human security approach in order to balance the local perspective of their constituencies and the global perspective needed to tackle international issues. He added that because technological and cyber capabilities are progressing at a pace that governmental and multilateral action have been struggling to keep up with, there is an opportunity for legislators to lead on these issues and inform and show the way for such governmental cooperation. Mr. Chowdhury concluded with a hopeful note highlighting the potential for peaceful uses of cyberspace, and the expansion and promotion of a common understanding built through partnership and collaboration between parliaments and civil society.

A poll on the applicability of international law to cyberspace among participants showed that while some of the audience were pessimistic on the degree of applicability, the vast majority argued that international laws were applicable to the context of cyberspace.

Dr. Tilman Rodenhauser, legal adviser at the International Committee of the Red Cross (ICRC), followed up on the key question in the poll. Noting that the primary mandate of the ICRC is the application of International Humanitarian Law (IHL) to armed conflict, Dr. Rodenhauser affirmed that IHL applies in cyberspace and limits cyberwarfare. Addressing the first concern ('How is cyber technology currently being used in warfare?'), Dr. Rodenhauser explained that most states already use cyberspace in military operations, and many have already adopted cyber operations as a specific branch of their militaries, considering it to have an increasingly important role in offensive and defensive operations. He highlighted three possible types of application of cyberspace to modern warfare: as part of defensive operations (as systems get more digitalised, they will need to be protected from cyber-attacks); as deployed alongside kinetic operations (e.g. to disable enemy radar systems ahead of an attack); and in manners intended to cause physical harm.

Moving to the second concern ('What are the main humanitarian concerns and potential harmful consequences?'), Dr. Rodenhauser noted that the increasing dependency on and integration of digital systems in society multiplies the potential targets of cyber-attacks across every level of society. He gave examples of cyber-attacks on nuclear facilities (e.g. in Iran in 2010 and India in 2019) and electrical facilities (e.g. in Ukraine in 2017). Such attacks could cause harm to civilians and would be bound by the rules and norms of IHL, even if undertaken during wartime. He also noted the vulnerability of medical facilities to cyber-attack, an action that would undeniably violate IHL. Finally, in reinforcing the ICRC position that IHL applies to cyber operations, Dr. Rodenhauser noted that the International Court of Justice has confirmed this. He added that the UN Charter also prohibits the use of force in peacetime, and mandates States Parties to settle their conflicts peacefully. He added that Human Rights treaties also offer some protections, particularly in peacetime. He noted that IHL is best regarded as adding a layer of protection, complementing other international law applicable to cyber operations. Dr. Rodenhauser concluded his presentation by highlighting that there is still considerable uncertainty about the manifold applications of cyber capabilities in military operations. He stressed the fact that societies need to push governments to clarify how cyberspace is efficiently protected, and that MPs have a key role in this endeavour.

Ms. Anne-Marie Buzatu, Chief Operations Officer at the ICT4Peace Foundation, dedicated her intervention to discussing practical actions to neutralise some of the threats inherent to cyber operations (whether civilian or military). Ms. Buzatu focused on two concrete proposals. The first proposal revolves around the adoption of common norms and rules that govern operations in cyberspace. The potential of a cyber-attack on critical infrastructure is a concrete threat on which ICT4Peace focuses. It is an important issue, since digitalized critical infrastructure covers most essential services in modern societies. Accordingly, ICT4Peace calls on governments to commit to not conducting Offensive Cyber Operations against Critical infrastructure. Some of the norms that ICT4Peace has championed have been picked up and recognized by international processes designed to regulate conduct in cyber realms.

The second proposal is a Cyber state peer-review mechanism for state-conducted foreign cyber operations. Such a mechanism would attempt to (partially) fill the gap of some form of mechanism to hold states accountable for their cyber operations that affect other states through offering a cooperative process for state reporting, as well as facilitate the input of other stakeholders. Ms. Buzatu highlighted the positive impact that this could have by bringing together governments and the international community in an effort to promote norms, transparency and accountability. This is also a goal that MPs have the possibility to help implement and that could result in concrete steps towards safer and more peaceful use of cyberspace.

Mr. **Arthur Duforest**, research assistant for PNND and Master's student in Development of International Relations, introduced his presentation with a definition of cyber space, arguing that cyberspace is a "performative space" not defined by what it is (computers, networks, the internet) for that changes constantly, but rather by how it is used. It is the role of parliamentarians to ensure that this "how" remains peaceful. Mr. Duforest summarized a couple of aspects of the Parliamentary Handbook, more specifically the chapter on 'Disarmament for future generations', highlighting the usefulness of many of the resources brought forth in the handbook in securing peaceful use of cyberspace. He emphasized three aspects of the Tallinn Manual: (1) counter measure, which is a risky endeavour in cyberspace as it could hit the wrong target or spread to non-military aspects; (2) strong partnerships across nations and with the private sector, especially in the case of a rapidly evolving domain where it is hard to remain ahead of progress; and finally, (3) due diligence, as one of the core recommendations which demand a state not to launch cyber-attacks and furthermore not to allow states to be the launching ground of cyberattacks. Similarly, regarding the "non-first-use" policy for nuclear weapons, and echoing ICT4peace's call for restraint in using offensive force, Mr. Duforest stressed due diligence as a core aspect of the peaceful use of cyberspace. Mr. Duforest concluded with a reminder of the potential for positive change brough forth by the Handbook and encouraged MPs and all participants to use this resource as widely as possible.

During the question and answer session, some MPs took the floor to make comments and ask questions on various aspects of the topic. Some parliamentarians questioned the scope of responsibility and capacity of states to ensure that their infrastructure is not used for cyber-attacks, to which the speakers mentioned the notion of due diligence as a norm targeted at governments. A point was made regarding the vulnerabilities of nuclear command and control systems to cyber-attacks, which to this day remains a concern. Although such systems are not connected to the internet, the 'Trojan Horse' cyberattacks against Iran's nuclear energy plants in 2015 demonstrate the capability for cyber-attacks to be undertaken against systems that are off the net. The problem of (reliable) attribution of responsibility of cyber-attacks was addressed: according to the experts this still limits the discussion on accountability when a cyber-attack is carried out.

A point was raised on the possible use of the dark net to illicitly transfer arms and the responsibility of national governments in preventing this. Some parliamentarians commented on the need for a multilateral process leading to a treaty governing the state's cyber behaviours and responsibilities. One of the panellists responded that a governing treaty on cyberspace could only be formed from a multilateral perspective with collaboration and peaceful use of cyberspace in mind. A discussion about the diverging views (and consensus) among states on what norms and rules of international (humanitarian) law apply to cyber operations took place. Lastly, a question was raised on the roles of parliamentarians in protecting their constituents from cyber-crime. The handbook makes distinctions between cyber-security, cyber-crime and cyber-warfare, which are inter-related but not the same. The handbook deals primarily with cyber-warfare. However, many of the approaches to dealing with this are also applicable to cyber-security and cyber-crime.