CYBER PEACE & SECURITY MONITOR

Civil society perspectives on the Open-ended working group on developments in the field of information and telecommunications in the context of international security

VOL.01 NO.04

02 December 2019

Photo by Ana Flávia on Unsplash

IN THIS ISSUE

Reaching Critical Will

www.reachingcriticalwill.org

A PROGRAMME OF THE WOMEN'S INTERNATIONAL LEAGUE FOR PEACE & FREEDOM

www.wilpf.org

EDITORIAL: THE VALUE OF MULTI-STAKEHOLDERISM

Allison Pytlak | Reaching Critical Will, Women's International League for Peace and Freedom

As noted in the last edition of this Monitor, "not starting from scratch" was the overarching message from the first session of the Open-ended Working Group (OEWG) on "developments in the field of information and telecommunications technologies in the context of international security." The phrase was one that states and regional groupings used consistently throughout the September session to acknowledge and re-affirm the value of the past and current work, dialogue, and commitments in the area of international cyber peace and security.

This informal intersessional meeting of the OEWG is a way to support, but also test, that resolve.

The meeting is organised around six substantive sessions that roughly reflect the same topics addressed in formal meetings of the OEWG. Each will begin with "scene-setting remarks" after which participants are invited to provide brief interventions that respond to a set of proposed framing questions. The chair of the meeting, Mr. David Koh of the Cyber Security Agency of Singapore, and Swiss Ambassador Jürg Lauber, the OEWG chair, have both emphasised their hope for an interactive dialogue and exchange throughout. Member states will participate to ask questions and respond but not deliver national statements.

Over 100 organisations have registered for the intersessional meeting and represent an extremely broad diversity of stakeholders. There are non-governmental organisations (NGOs) coming from the areas of advocacy, policy, and awareness-raising with expertise in disarmament, peace, security, human rights, and international law. There are private cyber security and software firms, both large and small. There are independent academic researchers, technologists, lawyers, and policy research institutes. Some approach cyber security with a human-centric and human rights-first approach; and others view this solely as an issue of national defence and international affairs.

Multiple global regions will be represented and the possibility to deliver video statements has been made available to those not able to attend in person. The meeting will be webcast.

Such a diversity of participants can support the "not starting from scratch" approach by bringing to the fore and highlighting in detail the breadth of work occurring in the pursuit of peace in cyber space; a basis that can be built on by the OEWG. Through the framing questions, participants have been invited to bring examples of actual capacity- and confidence-building measures, for example, or to provide views on how the malicious use of information and communications technologies (ICTs) negatively affect socio-economic development and pose other threats—all of which could move the conversation from blanket descriptions of harm to evidence-based information sharing.

The framing questions also make specific reference to other normative fora like the Cybersecurity Tech Accord and the Paris Call, and ask for views on how to reconcile the overlapping outputs of those processes with the UN's cyber activities, which is a very real question that has not yet been adequately addressed. Participants are further invited to outline what role we see for ourselves in supporting the implementation of the voluntary non-binding norms of responsible state behaviour contained set out by the UN Group of Governmental Experts (GGE) in 2015, and what we view as the main threats to critical infrastructure and critical information infrastructure. Thoughts on the way forward will also be taken up.

This all should, in theory, provide states with the specialised information and insight to help steer the OEWG toward concrete and technically sound outcomes when it resumes formal discussions in February 2020. Many states emphasised that the OEWG should aim for such concrete and practical outcomes, possibly as one way to distinguish its outputs from those of the GGE that is meeting concurrently within the UN and has its first session next week. Stakeholder input could also serve to provide clarity on some of the thornier or more controversial questions that member states are

wrestling with or lift up dimensions of the issue that are under-explored, such as the gendered impacts of cyber operations.

Stakeholder diversity can also be a healthy test, however, as undoubtedly there will be criticisms and concerns raised about state behaviour in cyber space that some countries may prefer to not hear—but that need to be accounted for if we are indeed not starting from scratch and want to have a dialogue that is rooted in reality. It's evident that the pace and severity of malicious operations in cyber space have increased noticeably. The use of cyber technologies as tools of or targets for aggression is becoming more regular and, as a result, normalised by a larger number of states. The last year has seen a spike in data breaches, malware attacks, disinformation campaigns, and continued use of proxies by states. Governments use digital technologies and spaces to restrict human rights, such as through surveillance, hacking, censorship, and intentional disruption of internet services and access.

It was presumably a desire to avoid criticism about just these kinds of activities that prompted some member states to block access to the September OEWG session for any organisation that does not hold ECOSOC status at the UN; a very rare occurrence in UN disarmament and arms control fora and one that sets a dangerous precedent. Ironically, some of the same member states who may have played in role in that blockage are also those who spoke at length during the 2019 First Committee about the importance of having a cyber security body at the United Nations that is open and accessible to all. That is why the high turn-out and participation for this consultative meeting is so significant and can stand to demonstrate what non-governmental stakeholders collectively offer to this work and integral role in implementing state-agreed norms, but it shouldn't come at a cost of critical and honest discussion.

Shutting out critical discussion does a disservice to both the concept of multi-stakeholderism and the spirit of multilateralism and equality that the United Nations is meant to embody. The same concerns that civil society may rightfully raise about the abuse of human rights online or flouting of agreed norms when states attack critical infrastructure should also be the concerns of the entire international community, including governments, because they threaten our collective peace and security, and undermine the rules-based international order.

"This is the first time in the history of UN ICT discussions in the context of international security that such an inclusive and global multi-stakeholder meeting is held to discuss cyber threats and challenges and how to address them," notes a joint letter from the two chairpersons. What will be important going forward is how the expertise and information provided at this meeting is used by states in the formal work of the OEWG. This convening of a meeting like this was mandated in the same UN General Assembly resolution that created the OEWG, but it does have an informal status and is being independently and voluntarily resourced and chaired. A report of this meeting will be presented from the chair during the OEWG's next formal session in February 2020, at which non-governmental participation could again be restricted. This publication will produce a final report at the end of the intersessional to capture the diversity of expertise, views, and concerns presented. The hope is that this is the start, and not the end, of a more robustly inclusive UN dialogue on cyber security writ large. The ubiquity of ICTs in each of our lives, and relatedly our shared vulnerability, makes us all stakeholders in their protection.

The hope is that this is the start, and the not the end, of a more robustly inclusive UN dialogue on cyber security writ large.

CYBER OPERATIONS DURING ARMED CONFLICT: HUMAN COST AND LEGAL FRAMEWORK

Laurent Gisel and Tilman Rodenhäuser | International Committee of the Red Cross

Indeed, digital technology is advancing quickly. During armed conflict, cyber operations have been used in support of or alongside kinetic military operations. They have the potential to help achieve military aims without harming civilians or causing physical damage to civilian infrastructure. However, recent cyber operations also reveal that sophisticated actors have the capability to disrupt the provision of essential services to the civilian population.

By means of cyber operations, a variety of "targets" in the real world—such as industries, infrastructure, telecommunications, transport, or governmental and financial systems—can be disrupted, altered or damaged. Experts see the potential human costs of cyber operations.[1] For instance, the health care sector appears to be particularly vulnerable to both direct cyber attacks and incidental harm from such attacks directed elsewhere. In addition, there is an increased frequency of cyber attacks against industrial control systems, such as those used to operate critical civilian services, including water and sanitation facilities.

In light of this evolving digital environment, hostile cyber operations are high on the agenda of the international community. Next week, the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) will hold an intersessional consultation, and the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (GGE) will convene for a first time in New York. Both groups are mandated to study "how international law applies to the use of information and communications technologies by States". One important field in the context of international security—and a point of contention in past discussion on information and telecommunication technologies—is international humanitarian law (IHL).

For many years, the International Committee of the Red Cross (ICRC), also known as the guardian of IHL, has engaged with states and other actors on the question of existing principles and rules of IHL apply to cyber operations during armed conflicts. This week, the ICRC published a position paper on cyber operations and IHL and submitted it to both groups.

In a succinct blog post, we have summarised the five key messages of the position paper, namely:

- Cyber operations can cause human harm
- IHL applies to, and therefore limits, cyber operations during armed conflict
- IHL provides essential rules protecting civilian populations against the effects of cyber attacks
- States must act now to clarify how key IHL notions and rules apply in cyberspace
- Any development of law or norms needs to build upon re-affirmed existing rules

The full position paper is available here: https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts.

1. *See https://www.icrc.org/en/document/potential-human-cost-cyber-operations.*

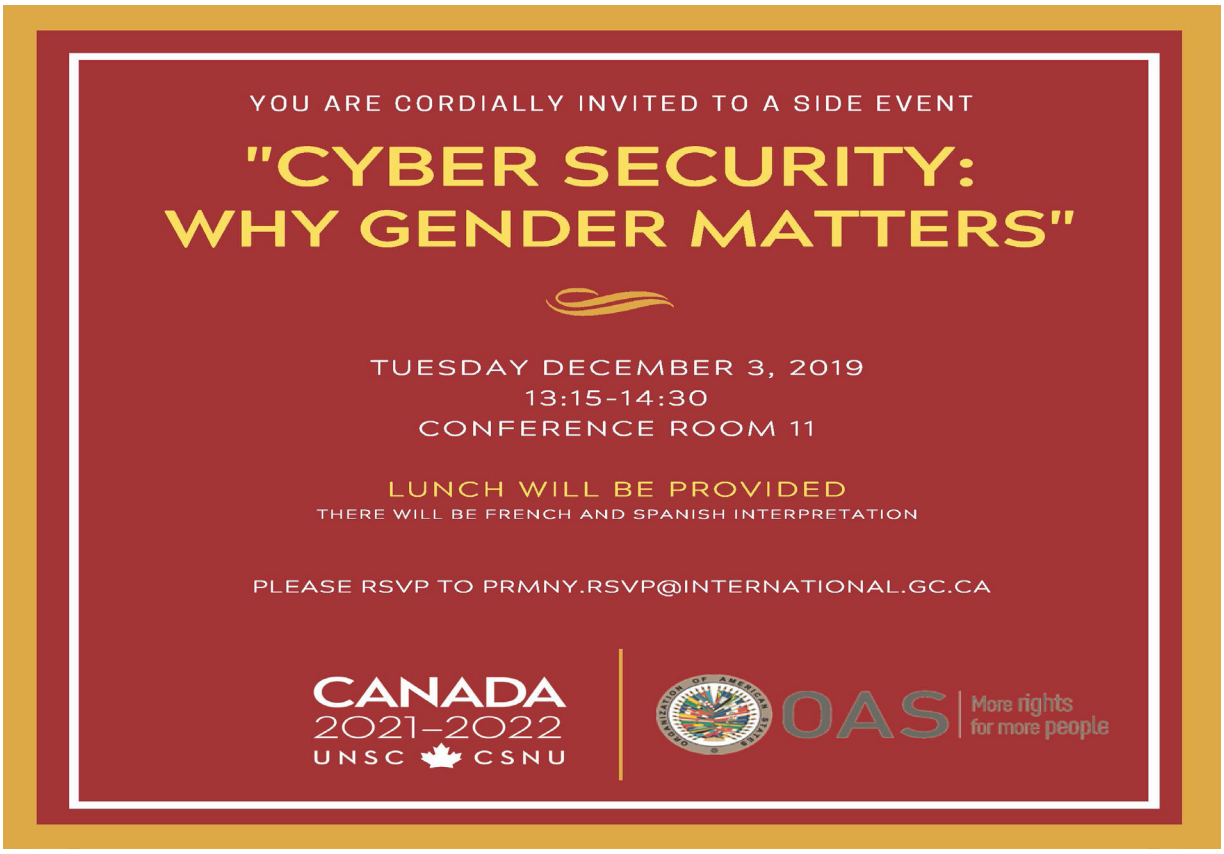
UNPACKING THE GGE'S FRAMEWORK ON RESPONSIBLE STATE BEHAVIOUR

Sheetal Kumar | Global Partners Digital

At the UN First Committee, two processes—the UN Group of Governmental Experts (GGE) and the Open-ended Working Group (OEWG)—are currently exploring the same question: responsible state behaviour in cyberspace. This term comes from a 2015 report by the previous GGE, which defines it according to a framework of four components:

- norms, rules and principles;
- confidence-building measures;
- capacity-building;
- the application of international law in cyberspace.

Understanding these components is crucial to engaging effectively at the GGE and OEWG. Global Partners Digital (GPD) is publishing a series entitled "Unpacking the GGE's framework on responsible state behaviour" which looks at each component in turn—looking at what they mean, how they have been defined, and their relevance to human rights. Each brief is authored by GPD and external experts. So far, two briefs have been published: the first on capacity-building and the second on confidence-building measures. They can be found on GPD's dedicated information hub for the First Committee, which also includes a range of other resources: https://www.gp-digital.org/event/unga-first-committee-hub/.



CYBER PEACE & SECURITY MONITOR

Reaching Critical Will is the disarmament programme of the Women's International League for Peace and Freedom (WILPF), the oldest women's peace organisation in the world. Reaching Critical Will works for disarmament and the prohibition of many different weapon systems; confronting militarism and military spending; and exposing gendered aspects of the impact of weapons and disarmament processes with a feminist lens. Reaching Critical Will also monitors and analyses international disarmament processes, providing primary resources, reporting, and civil society coordination at various UN-related forums.

Reaching Critical Will

www.reachingcriticalwill.org

www.wilpf.org

The Cyber Peace & Security Monitor is produced by the Reaching Critical Will programme of the Women's International League for Peace and Freedom (WILPF) during relevant UN meetings.

CYBER PEACE & SECURITY MONITOR

Vol. 01, No. 04
02 December 2019

Editor: Allison Pytlak
disarm@wilpf.org