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.02

11 September 2019

Photo by ev 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

CAPACITY, CONFIDENCE-BUILDING, AND CONSULTATION—THE WORK OF THE OEWG BEGINS

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

Around 70 delegations participated in the general exchange that occurred over the first two days of the Open-ended Working Group's first session. Statements covered wide ground, setting expectations and priorities on substantive and procedural issues, and sharing of national and regional experience. It is evident that there is appetite and support for this process and a collective sense of concern about the implications of a deteriorating global security environment in a digital and highly networked and interconnected world.

A strong message reinforced by virtually all is that the OEWG is not "starting from scratch" and that outcomes from the prior Groups of Governmental Experts (GGEs) on ICTs are the basis for further work and cannot be discounted or replaced. In fact, several statements urged better examination of how the behavioural norms recommended by the GGEs and endorsed by the UN General Assembly are—or are not—being implemented. For some, this means exchanging in greater detail about policies and practice. Others, like Nigeria, the Philippines, Malaysia, and ICT4Peace emphasised the need to develop better attribution mechanisms as a way to foster accountability and compliance. A few states spoke frankly about their concern about aggressive cyber policies or actions; Luxembourg, for example, stated that it is not optional for "digital heavyweights to not respect international law". The Netherlands observed that while almost all countries present have said they are against malicious state behaviour, it is still occurring all the time which indicates a need to "practice what we preach."

There were more overt warnings against weaponising technology and militarisation of cyber space than have been heard in First Committee statements on the subject of cyber to date. Albeit in varying forms, this point was made by the Non-Aligned Movement (NAM), Liechtenstein, Morocco, Peru, the Netherlands, Iran, and China, among others. Switzerland said it concerned by increased power projection within cyber space. Australia acknowledged its own offensive cyber capabilities and argued that this does not contribute to militarisation because they are transparent about their programmes. The Netherlands also spoke out strongly in favour of a human-centric approach to cyber security that puts the safety of citizens first.

WILPF understands the militarisation of cyber space as an expansion of the same patriarchal structures of power that perpetuate violence and repression in the offline world. While this precise gender analysis was not articulated during the general exchange, Sweden, Canada, the Association for Progressive Communications, and WILPF highlighted the unique challenges of online gender-based violence and Australia and New Zealand called for stronger participation of women in ICT-related discussions. This builds on the upsurge of gender sensitivity occurring in other parts of the disarmament system.

There were more overt warnings against the weaponisation of technology and militarisation of cyber space.

While the majority of delegations welcomed the OEWG's transparency and openness, it was acknowledged that this is not yet perfect. Statements from governments and civil society organisations together, and the High Representative for Disarmament Affairs, regretted specifically that non-ECOSOC organisations were prevented from participating in this session. Many others stressed the importance of a multi-stakeholder process writ large, whether to take advantage of technical knowledge and expertise or to bridge political and conceptual divides. Doing so would be "an essential part of a solution to a deteriorating environment in cyber space," noted Portugal. As this publication argued in its preview edition, opening up the discussion to more voices

and perspectives can help to dilute and diffuse some of the tensions described above but only if the OEWG can escape same power dynamics that have come to characterise so many other UN security bodies lately, in which the voices of a global majority are stifled by a powerful few. In this vein, it was noticeable that not all global regions were equally represented in the opening days of the session, which may have an impact later in the OEWG process.

On Wednesday, the thematic debate will begin with six half-day sessions focusing on threats; international law; rules, norms, and principles; institutional dialogue; confidence-building measures; and capacity building. Each will open with an expert presentation. In some of these areas we've already been given a preview of what to expect through general exchange statements. For example, the applicability of international law to cyber space was widely reinforced and a few states highlighted specific (if at times divergent) views on the necessity of new international law. The applicability of international humanitarian and human rights law was widely supported during statements made in the general exchange, but we know from past discussions that this is a sensitive issue. The importance of proper capacity building and dialogue were referenced in nearly every statement and quite a lot of countries have indicated already what they see as the biggest threats.

Yet, there is variation in the level of detail being put forward and sometimes key terms or jargon are being used without precision. This also speaks to the broader problem of differing understandings and lack of clear definitions in this issue area. Different views are emerging on where to focus the OEWG's work with some highlighting cyber crime, others cyber terrorism, and yet some others preferring to focus on state-sponsored cyber operations. There are also certainly diverse priorities and baseline understandings of cyber and information security that will need to be resolved in order to get to the practical outcomes and support sought by most member states—but that is also why it has been illustrative and useful to have this kind of a session and hear the views of all, in order to better understand where the gaps and needs really are.

It is often said in the UN that "nothing is agreed until everything is agreed" in reference to the process of adopting resolutions, reports, and other documents. While states do not have to negotiate a report just yet, the phrase does sum up well the interconnectedness of the six areas of work awaiting their attention this week. Threat reduction—or its escalation—is heavily dependent on the strength and success of confidence-building measures and dialogue promotion. Law relates to norms, rules, and principles. These six areas of work are a very good blue print for forward progress. Each requires focused time and study but ultimately cannot be considered in complete isolation from one another.

> Just as digital networks bind our world together and have created shared vulnerabilities, the solutions can likewise feel like a tangled web

Just as digital networks bind our world together, and have created shared vulnerabilities, the solutions can likewise feel like a tangled web. They require comprehensive approaches that take into consideration the unique contours of cyber space and employ a broader range of tools and tactics and players than may be the norm in traditional disarmament and arms control. As one delegation noted, any cyber security regime is only as strong as its weakest link.

NEWS IN BRIEF

Danielle Samler | Reaching Critical Will, Women's International League for Peace and Freedom

The News in Brief is not a comprehensive recording of all statements and positions but meant to capture key points from discussions.

Process

- Nearly every delegation stressed that the current Group of Governmental Experts (GGE) and the OEWG should work in tandem with one another and avoid overlap or contradiction in content and outcomes.

- Russia noted that the focus of this substantive session on the presentation by states of their political positions and concrete proposals is what constitutes the chief distinction between the OEWG and the GGE. It further noted that the outcome of the OEWG will be judged on its concrete result.

- Russia emphasised the importance of producing a concrete draft report sooner than later. The NAM strongly encouraged the early circulation of substantive recommendations. Kazakhstan said it expects the final OEWG report to include recommendations on how to practically deal with threats.

- Pakistan noted that the Conference on Disarmament is an appropriate venue for multilateral work on strengthening security in the cyber domain.

- New Zealand reminded that the purpose of this OEWG is to discuss responsible state use of ICTs and therefore the scope should be limited to state use of ICTs and not cyber crime or cyber terrorism as there are other more appropriate forums for that discussion. This was supported by the Netherlands.

- Numerous delegations reinforced the value and necessity of a multi-stakeholder approach and/or consultation with experts, academics, or civil society. The United Nations Office on Drugs and Crime (UNODC) noted that continuous stakeholder engagement is the essence of the OEWG.

- The High Rep for Disarmament Affairs and Canada expressed disappointment in the fact that only ECOSOC accredited organisations were allowed to formally participate in this OEWG.

Threats

- India, Colombia, the Philippines, Costa Rica, Spain, France, Turkey, Morocco, Kenya, Mauritius, and the UNODC highlighted cyber crime as a threat and area of concern. Morocco and Peru described internal steps taken to address cyber crime. The Caribbean Community (CARICOM) spoke of the impact of financial cyber crime in the region and how this hampers development.

- CARICOM, Thailand, Liechtenstein, Australia, Nicaragua, Bangladesh, Norway, Qatar, and Algeria noted the importance of protecting critical infrastructure. The International Committee of the Red Cross (ICRC) further described the impact on civilians when vital infrastructures like hospitals are attacked.

- Other delegations variously referenced concerning activities such as disinformation (Nicaragua), government destabilisation (Nicaragua), fake news (China), social media (Iraq), hacking (Sri Lanka, Philippines) and defacement (Philippines).

- Belarus, Syria, China, Iraq, Guatemala, and Peru referenced the risks of cyber terrorism or terrorists. India urged states to not let their territory be used for cybercrime and cyber terrorism.

- Switzerland referenced the "increasing diversification and professionalisation" of perpetrators conducting malicious cyber acts and also of the increased use of cyber space as

a space to project power.

- Nigeria, Iran, Australia, Liechtenstein, Algeria, and China expressed concern over the militarisation and weaponisation of the cyber domain; Algeria also highlighted the potential for cyber space to become a new theatre of warfare.

- The Netherlands noted that while the majority of states say they are against the malicious use of information and communication technologies (ICTs), it is still occurring. It urged states to "practice what they preach" regarding the malicious use of ICTs in order to foster a peaceful cyber security environment.

International law

- The applicability of existing international law to cyber space was reinforced by a significant numberof delegations.

- The NAM argued that the OEWG should use existing international laws and regulations as a reference point for developing further legal regulations for the use of ICTs.

- States such as Nigeria, Algeria, and Qatar voiced hope that the OEWG will lead to the creation of a legally binding instrument to enforce international norms.

- CARICOM welcomed the OEWG as means to develop a legally-binding framework that can consider the concerns and perspectives of all states.

- Egypt said the OEWG process provides an excellent platform to codify rules on the appropriate uses of ICTs.

- Belgium, Estonia, Bulgaria, and the Netherlands would not support the creation of new legal frameworks. The EU stated that while it is generally agreed that international law should apply in its entirety to the use of ICTs it is important that the OEWG not create a new body of law to apply to cyber space that would risk undermining ongoing practical efforts. Indonesia suggested giving priority to existing law and not creating new law. It further noted that at an early stage legally binding norms can serve as a reference to fill the gap of ungoverned issues in cyber space.

- Liechtenstein and others urged updating or harmonising laws to ensure their relevance in cyber space.

- Pakistan suggested a cautious interpretation of international law with respect to cyber space, given its complexity.

- The International Committee of the Red Cross (ICRC) explained that by asserting the applicability of IHL it is not encouraging the militarisation of cyber space or legitimising cyber warfare. It noted that cyber operations do raise a number of issues regarding how IHL is interpreted.

- Kenya expressed that development of inclusive and cooperative frameworks at national, regional and international levels to detect, prevent, and respond to various threats in the cyber space is a priority.

- Czech Republic stated that government action in cyber space should be subject to independent judicial oversight.

Rules, norms, and principles

- Most delegations reinforced the importance of achieving better understanding and implementation of the norms, rules, and principles that were set out in the 2013 and 2015 reports of the GGEs.

- Germany said that widespread understanding and clear definitions of the norms are essential.

- France, Poland, the UK, and Indonesia, among others, spoke to the importance of ensuring that already agreed norms are being implemented and abided by.

- The United States (US) specified that the 11 voluntary non-binding norms should be strengthened but noted that these should remain voluntary and non-binding.

- Costa Rica suggested sharing codes of conduct to assist in understanding how these norms and principles are being understood, as a starting point in discussions.

- Nigeria urged the OEWG to develop proposals to address attribution, such as through establishing an international framework, and the role of artificial intelligence. The Philippines and ICT4Peace also urged more attention be given to attribution.

Capacity building

- More than half of all statements highlighted the importance of capacity building, with some urging it to be a central consideration for the OEWG. Nicaragua advocated for it to be an essential component of discussions, and Ireland called for sustainable capacity building.

- Kenya said it believes that necessary international financial infrastructure for funding capacity building need to be put in place and that such funding mechanism should prioritise those states that are furthest behind. South Africa urged incentives to be put in place so that capacity building through un-ear-marked financial assistance can occur. New Zealand spoke to increasing the capacity of Pacific Island states in particular. Iraq suggested the creation of international partnerships to bolster capacity building efforts.

- Canada asked how can states speak of the implementation of standards without raising the question of resources and tools and described some of its recent capacity building efforts within the Organization of American States and Organisation internationale de la Francophonie.

- The Netherlands said it is committed to investing in capacity building measures whether it be financially or politically. It also stated its hope that this OEWG will result in better application of capacity building measures.

- The UNODC expressed the importance of capacity building in achieving the goal of cyber peace and security and highlighted its own work in this regard.

- The International Telecommunications Union (ITU) described its technical work with states in the development of national cyber security strategies and deployment of international security standards.

Confidence-building measures (CBMs)

- Statements from Singapore, the Philippines, Australia, Estonia, Japan, Finland, Ireland, Austria, Peru, Ecuador, the US, and the Netherlands, among others, urged the importance of trust and cooperation, including through the establishment of CBMs. Japan referenced CBMs as an important pillar and Ireland described them as essential for avoiding conflict in cyberspace, "by increasing predictability of state behaviour and reducing the risks of misinterpretation and escalation."

Gender

- Australia noted that women are under-represented in the cyber domain and highlighted how few women had delivered statements in this meeting.

- New Zealand also expressed the importance of increasing women's participation in the discussion on ICTs.

- Canada suggested establishing links between this OEWG and the Women, Peace and Security agenda as well as the importance of women's role and voice in discussions around cyber security.

- The Association for Progressive Communications (APC) stated the importance of looking at ICTs through a gendered lens acknowledging that gender-based violence creates differential threats which affect the ability for some to use and benefit from ICTs because of their gender.

- The Women's International League for Peace and Freedom (WILPF) also recognised the

importance of taking gender into consideration when discussing cyber peace and security, explaining that online gender-based violence is often directed at those who break from traditional gender norms.

Human rights and human security

- States including Luxembourg, Norway, Sweden, Costa Rica, Liechtenstein, the UK, Czech Republic, Portugal, Canada, and Iraq, among others, expressed support for the respect of digital human rights. Some of these states, as well as APC and Igarape Institute, further explained the relationship between these rights and international cyber security.

- The Netherlands outlined its view on the use of ICTs in international security as a human-centric approach, primarily focused on the responsibility of the protection of citizens.

- Colombia urged it as fundamental to tackle the challenges related to digital identify, protection, and privacy.

Development

- Some delegations highlighted the positive economic benefits of ICTs and the importance of preserving the right to the peaceful uses of ICTs while also combating the malicious use of ICTs. The NAM in particular emphasised that a legally binding framework shall not affect the inalienable rights of states to develop and use ICTs for peaceful purposes.

- Nicaragua and the Netherlands referenced how better cyber security could lead to the achievement of Sustainable Development Goal (SDG) 9.

- Sweden noted that around 50 per cent of the world's population is still offline and urged increased meaningful access be a priority given the declining rate of new internet users in recent years.

- Iraq stated that the peaceful use of ICTs are a main pillar for promoting sustainable development and achieving economic growth.

- Kenya described positive benefits of ICTs such as business development but noted also the related increase in vulnerability. It explained domestic measures it is taking to protect and promote e-commerce and e-government services.

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. 02
11 September 2019

Editor: Allison Pytlak
disarm@wilpf.org

The views expressed in this publication are not necessarily those of WILPF or Reaching Critical Will.