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.03

16 September 2019

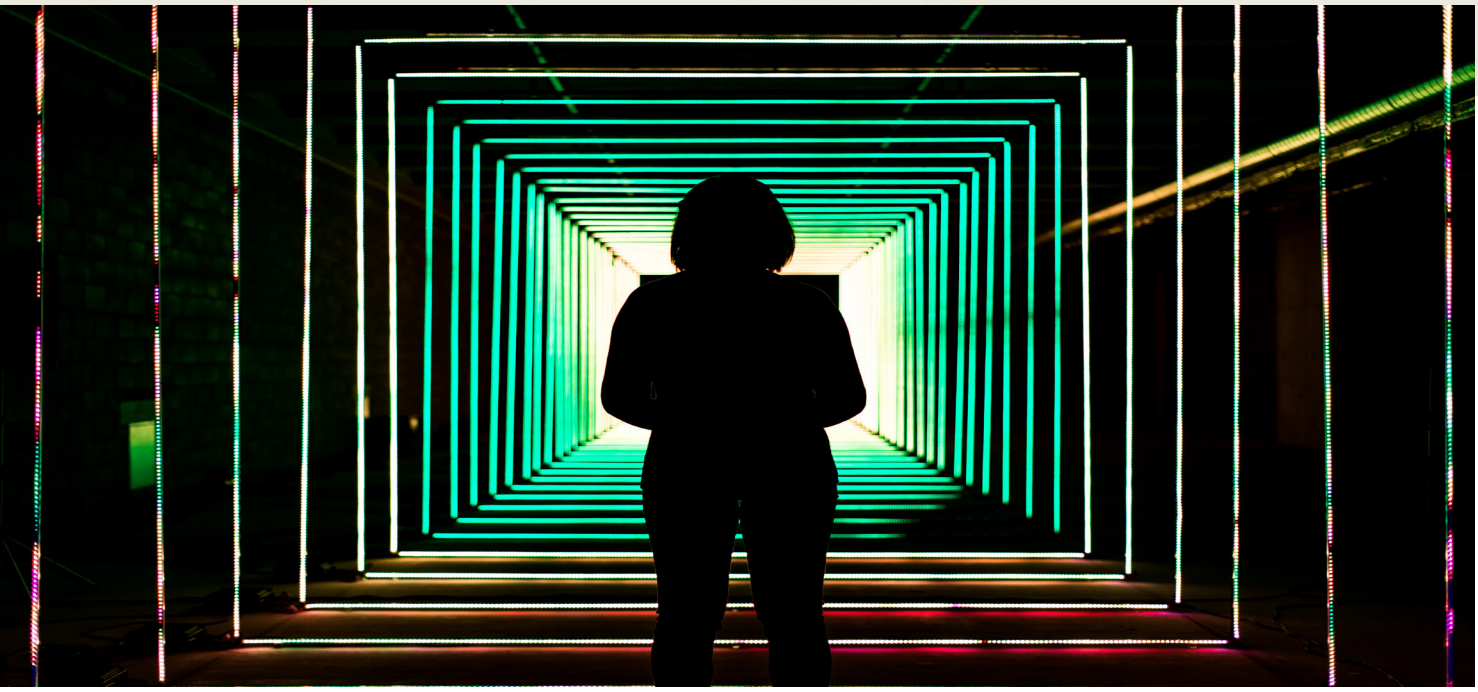

Photo by Bit Cloud Photography

IN THIS ISSUE

Reaching Critical Will

www.reachingcriticalwill.org

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

www.wilpf.org

EDITORIAL: NOT STARTING FROM SCRATCH MEANS BUILDING ON HUMANITARIAN DISARMAMENT

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

"We are not starting from scratch" might just be the motto of the first substantive session of the UN's new Open-ended working group (OEWG) on developments in the field of information and telecommunications in the context of international security. States and regional groupings alike used these words in order to acknowledge the significant work and dialogue that has already occurred or is presently underway in the area of international cyber security. It was made in reference to external, non-UN dialogue processes as well as regional and national projects spanning prior discussions about the applicability of international law to cyber space, to confidence and capacity building measures. Yet most often, what this equaled was a re-endorsement of the outputs of the UN's five Groups of Governmental Experts (GGEs) in this issue area (a sixth GGE will begin work later this year). This is not insignificant, for while the outputs of those groups were formally endorsed by the UN General Assembly, they were developed in closed settings which later came under criticism and the fifth GGE broke down owing to fundamental differences of opinion. The near universal reaffirmation of those GGE outputs was a strong indicator that the majority of member states do not want to undo what has already been agreed.

A second point highlighted by many delegations was one of practicality, and urgings to avoid more ambitious, yet politically-charged and possibly unproductive avenues of discussion in future OEWG sessions. This point surfaced across all six thematic areas that were discussed during the session and included suggestions to create various guidance or compilation documents, or recognition of the value of the OEWG as an on-going forum for institutional dialogue and information exchange. Some states used working papers or proposals to advance their ideas; Mexico, for example, submitted a proposal for the periodic submission of national reports to the Secretariat (UNODA), within the framework "on the implementation of rules, norms and principles previously agreed upon", including challenges or difficulties. The Canadian paper suggests that the "OEWG focus should now be on proposing practical measures to disseminate, apply, and implement existing agreed norms and confidence-building measures (CBMs)."

This desire to focus on practical activity was reinforced and enhanced by the session's tone. Overall, it was marked with a refreshing atmosphere of good will and positive exchange, which is surprising given the heated context through which it was established. In some of the meetings, delegations discarded prepared statements in favour of honest discussion, in which they asked clarifying questions of one another and responded to points and ideas raised by others. While this sounds like an obvious manifestation of what is meant by the words 'dialogue' and 'debate', it's surprising how rare this has become in UN disarmament and arms control fora.

The session was marked with a refreshing atmosphere of good will and positive exchange, surprising given the heated context in which it was established.

At the same time, it is already clear which topics do not enjoy consensus and will become more challenging as states move toward issuing the OEWG's report, due in 2020. The applicability of international humanitarian law (IHL) is one, where countries like China and Cuba were clear in their refusal to accept this premise and are unlikely to change their minds about this anytime soon. As explained in greater detail within our News in Brief section, this hangs largely on the premise that accepting IHL legitimises conflict in cyber space, which China says it is keen to avoid, stating more than once that a cyber war "cannot be won and must never be fought", a quote borrowed from

Ronald Reagan regarding nuclear war. Moreover, some states maintain that existing international law of any nature is insufficient to regulate cyber space or information and communication technologies (ICTs) and propose the establishment of new laws and conventions. There were also sufficiently divergent views put forward around human rights, human rights law, and social media content regulation that one can anticipate as a future problem, even if states did not engage in prolonged or overt disagreement during this first session. A majority of countries believe that the OEWG should focus on state behaviour in cyber space, while a smaller grouping of others emphasised that non-state actor behaviour must also be scrutinised.

None of this is surprising. It is now an open secret that the applicability of law and IHL is among the subjects that prevented members of the fifth GGE from reaching consensus in 2017. It is also well-known that some countries would like to see the establishment of a new legal convention on cyber space and that space for human rights considerations within First Committee-mandated bodies is not always welcome.

What states now face is a decision on whether or not to play it safe in the OEWG. They could use the forum to focus on outcomes that would lead to practical implementation of past agreements, and potentially diffuse tensions between certain countries. Or they could seek to put forward more ambitious—yet politically fraught—decisions and recommendations. This approach has merit and could help the UN catch up with and contribute to some of the more technical work of international cyber security that occurs through regional bodies and national computer emergency response teams (CERTs). Yet some of the primary assets of UN-based discussions are its convening power and capacity for norm setting, so to discard the opportunity to work through as of yet unresolved issues in an open and equal space like the OEWG should not be lost.

The extent to which geo-political realities would influence the OEWG session was something that this publication speculated about in its preview edition. The chair, whose own positive energy and coordination contributed to the good atmosphere in conference room four, outlined that he intends to have another round of open discussion on these same topics during the OEWG's second session in February, and will then have informal consultations to begin reviewing a pre-draft of a draft final report ahead of the third and final session in July. Egypt said in response that it hopes even if states cannot resolve major areas of disagreement, that the report will at least record what those differences are, and why they exist, so as to inform future work in this area.

What states now face is a decision on whether or not to play it safe in the OEWG.

What will also happen between now and July is that the sixth GGE will begin its meeting cycle, and while it has various input mechanisms for the wider UN membership and non-governmental stakeholders, the GGE is a closed group and the focus of their deliberations largely unknown as of yet, at least to non-insiders. It may become the venue to resolve these politically challenging questions or progress further the articulation of rules, norms, and principles—although its lack of transparency could raise the eyebrows of non-members who are shut out from that conversation. The necessity for complementarity between the two bodies has been widely reinforced (only a few states have said they do not support the GGE at all) but it is important that the more open OEWG not be treated as less politically significant in any way or become a space that is merely left to implement or interpret the decisions made by the smaller GGEs. This will not be politically viable in the long term nor lead to the type of two-way capacity and confidence-building stressed by so many states during the OEWG session. It is somewhat concerning that OEWG participation was uneven, with fewer states from the Caribbean, Africa, and the Pacific attending. In fact, the states who contributed most actively to the first OEWG session are also largely those who are GGE members and can therefore dominate both spaces, while hinting also at capacity issues that may prevent others from participating.

Along similar lines, it is imperative that the OEWG's

intersessional meeting in December be organised in a way that allows for meaningful input from private industry and civil society organisations, the two groups named as the session's target participants. This will mean meeting formats that permit and encourage interactive engagement and move away from tokenistic presentations delivered from the back of the room. It was encouraging to hear dozens of delegations refer to the importance of non-governmental participation and contributions throughout the week, and that several regretted that 18 such groups were denied access to this session of the OEWG without explanation or clarity on if they could attend future sessions. The intersessional should not, in theory, have the same restrictions for attendance yet all the same, anxieties around inclusivity remain, as do question marks about how the inputs of these diverse other stakeholders will be formally taken on board.

In its preview edition, this publication warned of the continued unchecked militarisation of cyber space. It was troubling to hear from states such as Australia and the Netherlands, and to a lesser extent France and Denmark, that it is okay to develop offensive cyber capabilities provided that this is done with transparency and restraint. This publication also urged states participating in the OEWG to take a more human-centric approach to international cyber security and move away from sanitised discussions that focus on infrastructure over individuals. In this regard, it was positive to hear more statements than expected in this direction throughout the week. Although, it was confusing to hear some of the same states that support the build-up of offensive capabilities simutaneously championing this view. Canada and Australia, for example, spoke to the disproportionate impact of cyber security threats on marginalised groups, including women, and encouraged better awareness of this and gender balanced participation. The UK highlighted the stark lack of gender diversity in the conference room. The Netherlands spoke out strongly in favour of a human-centric approach to cyber security that puts the safety of citizens first, a point echoed by some other delegations. References to the positive role of technology and ICTs in socio-economic development and bridging digital divides were frequent.

If we are not starting from scratch then that must also mean taking into account the principles and successes of humanitarian disarmament. Humanitarian disarmament, which is people-centred both in process and in substance, aims to prevent and to remediate human suffering and environmental degradation and is inclusive. A disarmament approach of any kind should not be taken as a pass on allowing cyber space to become militarised in the first instance, but presents a framework through which to challenge what has already occurred and is occurring in cyber space, in a way that can better orient us to human-centric cyber peace.

> If we are not starting from scratch then that must also include humanitarian disarmament, which is people-centred in process and substance.

NEWS IN BRIEF

Danielle Samler and Allison Pytlak | 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.

Existing and emerging threats

- There was some disagreement among delegates as to whether or not the issue of non-state actors using information and communications technologies (ICTs) in a malicious manner is part of the mandate set forth by resolution 73/27. Egypt, China, India, Singapore, Spain, and Syria supported that responding to non-state actor activities would be relevant. Syria recognized that while states can and do use ICTs in a malicious manner, they are not the sole perpetrators and non-state actors must be considered, particularly when dealing with the use of ICTs to incite, promote, and spread terrorism.

- Australia reminded that the mandate is to deal with responsible state behaviour, not that of non-state actors or terrorists as there are already bodies of work and groups working on that specific area. Australia also noted that it cannot be discounted that sometimes states use non-state actors to cover up their own malicious use of ICTs. This point was supported by Brazil, who recognised that states can use terrorists and non-state actors as surrogates or proxies for their own irresponsible use of ICTs. New Zealand also stressed the importance of the focus remaining on state behaviour and state-sponsored actors.

- Another point of debate was whether or not the norms agreed upon by this OEWG should be legally binding, or voluntary. At the outset, Egypt and Syria advocated for a legally binding instrument regulating state behavior whereas Japan noted that a legally binding instrument would take too long to develop and would not be able to keep up with the rapid pace of developments in ICTs. The United States (US) also advocated for voluntary norms, but on the basis that implementing legally binding norms poses a risk of hindering the ability for development in ICTs, a concern which was shared by the Russian Federation.

- The US and Russia expressed that delegates should be wary of overregulating ICTs and hindering their peaceful use. Egypt made clear that the issue at hand is to regulate behaviour and not technology. Mexico referred to the fact that just as it is not nuclear energy in and of itself that is a threat, but rather the creation of nuclear weapons, it is not cyber space or ICTs themselves that pose a risk, but the criminal use of them.

- Freedom of expression was also raised as a debate topic in this session. Syria questioned the delegates who supported the protection of freedom of expression as to whether or not that protection extends to online activities aimed at inciting or promoting terrorism. France made note that protection of the freedom of expression does not extend to online terrorist activities, but that the protection of human rights and freedom of expression is separate from international law issues. Argentina, the Netherlands, Iran, Finland, and Switzerland also stressed the importance of protecting fundamental human freedoms such as the freedom of expression.

- There was a common theme that transparency is of the utmost importance when discussing state capabilities in the cyber realm. The Netherlands, Denmark, Australia, and France all emphasised that states have the right to defend themselves against existing and potential threats. The Netherlands stated that states have the right not only to build defensive capacities, but offensive ones as well. The Netherlands also noted that while states are concerned about the threats that malicious use of ICTs, it is also important to recognise that states themselves are part of the threat. For this reason, it is of critical importance

that a state's abilities and intentions with ICT capabilities must be communicated in the international community so as not to cause misattribution, miscalculation, or misinformation. Denmark and France agreed that states must practice restraint and transparency when outlining their defensive and offensive ICT capabilities.

- Attacks on critical infrastructure was identified as a concern by Egypt, Argentina, Australia, Austria, Poland, Singapore, Botswana, Cuba, China, and the Netherlands. India also mentioned the potential threats that financially motivated fraud can pose to the financial banking system and the economy. The Netherlands pointed out that ICTs can be used to undermine a states' democracy and interfere with elections. The spread of malware, private data theft, infringement on states' sovereignty, the use of ICTs to promote hate speech via social media, and the militarisation and weaponisation of ICTs were also mentioned by states.

- Canada highlighted the differentiated impacts of ICTs on marginalised groups. In particular, they stressed the fact that ICTs affect these groups differently and this must be taken into consideration when assessing potential threats, which can include women, human rights defenders, and advocates.

International law

- The majority of states that spoke in this session reiterated that international law is applicable in cyber space. Some others, like Cuba, Israel, Pakistan, Syria, Malaysia, India, and Iran indicated doubts or reservations, owing either to the fact that law has so far not prevented malicious cyber operations or because of cyber space has unique and specific characteristics that may not align well or require further study.

- Some states with reservations also expressed support for or want to examine establishing new international law, such as through a legally binding instrument. Iran and Syria noted that existing law doesn't seem to be sufficient because cyber conflict, or attacks, continue to occur. Russia queried what happens when each state interprets international law differently and favours adapting international law to the realities of the cyber landscape. Egypt sees a gap in how existing law is being implemented.

- Russia set out five circumstances that prevent the application of existing international law: no main understanding of how to practically apply it; no overall understanding on what instruments are applicable; not all states recognise cyber attacks as armed attacks; there are contradictions between binding law and voluntary norms; and preventive cyber strike doctrines are incentives.

- France supports the application of existing law but noted that something more is needed, and Colombia referenced a need for something binding. Australia explained that in its view, existing law is both satisfactory and already binding, and states should avoiding picking and choosing from existing bodies of law, thereby undermining or reducing their quality. Russia suggested either a new instrument or standing legal body.

- There was significant discussion about the need to examine more precisely how international law applies, which kinds of law, and what legal bodies or agreements are relevant. Chile highlighted that the International Court of Justice (ICJ) has ruled on cases relating to what constitutes a cyber attack and around use of force in this space. Liechtenstein described its current project to review how the Rome Statute applies to cyber warfare. Many states referenced the UN Charter, per the recommendations of earlier GGEs. Australia cited the laws of state responsibility and on the use of force, as well as the UN Security Council as a body to review applications. The applicability of human rights law was reiterated by Australia, India, Liechtenstein, United States, and Estonia.

- There was significant discussion about the applicability of international humanitarian law (IHL). Some countries, such as China and Cuba, maintained that to affirm the applicability of IHL would legitimise conflict in this domain

and/or encourage its militarisation. China further explained that it has practical questions about how to apply IHL, given the challenges of distinguishing peace time from war time in cyber space, or military from civilian targets and actors, and if IHL principles of distinction and proportionality could be properly observed, not least because of attribution. It also urged a focus on cyber conflict prevention, rather than planning for it by developing laws for conflict there.

- Switzerland, Liechtenstein, US, Netherlands, Chile, Australia, France, the United Kingdom (UK), Mexico, Estonia, and Brazil, among others asserted that IHL does apply and would not become a justification for or encourage conflict. Australia responded to China's concerns to say that it too wants to prevent conflict, but a back-up plan is needed for when it does to protect civilians. Others made analogies to traffic and driving laws as existing but not encouraging accidents.

- Switzerland and Costa Rica acknowledged that attribution presents unique challenges for applying and enforcing law, per the points raised by China and others. The United States believes that further work on capacity building will help to address these concerns.

- India expressed that more work on definitions for key terms and concepts, like "attack" is needed. Australia explained that it has developed its own definitions for clarity and transparency that guides its national policy and Singapore indicated similarly.

- Malaysia said that the use of proxies is complicated for law; the Republic of Korea and the United States feel that the GGE outcomes and existing law address that.

- There were practical and action-oriented proposals for how the OEWG could focus its work in this area. Liechtenstein suggested that the OEWG could further delineate how international law specifically and concretely applies to cyber space. Egypt urged the OEWG to focus on operationalisation and universalisation of existing and agreed norms. Canada encouraged states to submit position papers to this conference and annual submissions to the UN Secretary-General's report on ICTs as ways to elaborate their views, and to also build on parallel discussions in the GGE. It said it would like to hear from states in the OEWG about their legal capacity building needs. Its suggestions were noted by Australia and Costa Rica. The Netherlands requested a legal opinion or explanatory note for the next session that explore the difference between cyber conflict and cyber competition, noting that most hostile cyber activities occur below a threshold of armed attack. Russia proposed to create a standing body of legal experts to assist the OEWG or the First Committee with thorny legal issues, which Iran supported.

Rules, norms, and principles

- There was much agreement that there needs to be a set of norms, rules, and principles that states abide by in cyberspace. There was disagreement on whether those rules and norms should become binding or remain voluntary. Egypt and Syria advocated for a binding instrument. Egypt pointed out that non-binding norms can reduce the risk of conflict in the short term, but in the long term there needs to be established binding rules and norms around ICTs. The US, Australia, Japan, Switzerland, and Israel prefer non-binding voluntary norms as a means of regulating state behaviour surrounding ICTs.

- A further point of contention was on whether or not the OEWG should have the ability to create new norms apart from the 11 that were set out in the 2015 GGE report. Singapore, Spain, Brazil, Switzerland, India, Malaysia, and the US, among others, adamantly expressed that there is no need to create new norms or rules on this issue, but rather the 11 voluntary non-binding norms established in the 2015 GGE are sufficient and the focus should be placed on the understanding of and implementation of these norms. Malaysia in particular mentioned the importance of establishing a mechanism to operationalise these norms in a practical manner. States such as Chile, Mexico, France, Cuba, and Iran on the other hand made

clear that the OEWG should not discount the possibility that new norms and rules may need to be established. All states agreed however that the 11 norms established by the 2015 GGE report should act as a basis for discussion regarding norms, rules, and principles.

- States also agreed on the importance of implementing the norms established. It was noted by Chile, the US, Malaysia, Japan, Egypt, Switzerland, the European Union (EU), India, Canada, Mexico, the Netherlands, the UK, Brazil, and Singapore that implementation mechanisms are needed. While not all of them support the move to something legally binding, many observed that the existence of these norms and principles is not enough in and of itself. Implementation and operationalisation measures need to be taken in order to turn these norms into practical instruments.

- Malaysia, Singapore, the UK, Belarus, Guatemala, Mexico, Austria, and Colombia shared their regional commitment to implementing these norms by mentioning practices their countries are already doing to ensure implementation of the norms and principles. Mexico proposed that states share among themselves the regional initiatives already under way.

- Canada urged the OEWG to consider how the specific needs of women and other vulnerable constituencies are met. They also advocated for a larger participation of women within entitites like the OEWG, computer emergency response teams (CERTs), and other bodies to advance gender equality in this field. This point was seconded by the UK who expressed disappointment at the lack of gender diversity in cyber security discussions.

- Mexico and Austria highlighted that the mere implementation of norms is not enough to guarantee peace and security in cyber space, but rather it is the combination of implementing norms, establishing confidence-building measures, capacity building measures, and the rule of law.

Institutional dialogue

- Views on this topic tended to downplay the need to establish new institutions and mechanisms, stressing instead that the OEWG should relate and engage with existing ones. In general there was wide support for dialogue, including among states or between states and other entities, for purposes of cooperation, capacity building, and transparency and also in relation to the pace of ICT development. France described such dialogue as necessary to create channels to de-escalate situations.

- France, New Zealand, Poland, the Netherlands, Guatemala, Poland, Estonia, and Canada expressed reservations about the need to establish new mechanisms or institutions because of a lack of clarity around what purpose it would serve or how to ensure results and felt that this would be premature without knowing what such a body would do. "Form follows function" noted Australia, Finland, Germany, and Brazil, in this regard while supporting the broader importance of dialogue.

- Russia argued that it is not premature to be talking about this, noting that if we want to think about the future then we must think about it now. It suggested that the continuing the format of this Group, and the GGEs, is part of institutional dialogue. It, along with Syria, Iran, Australia, and Norway highlighted that this OEWG is in and of itself a form of institutional dialogue and should continue to be in the future regardless of whether or not this group achieves success.

- Syria said that the OWEG is not here to just affirm what was previously agreed in earlier GGEs. It prefers to not link the work of the OEWG with the current (sixth) GGE. Iran had some criticisms of the closed nature of the GGEs and urged to establish an inclusive intergovernmental body to continue dialogue on this subject, by 2020. Australia reminded that the recommendations of the GGEs have been endorsed by the full UN membership.

- Mexico presented its proposal to initiate a new process of regular reporting to the UN Office of Disarmament Affairs, on the implementation of rules, norms and principles previously

agreed upon, and other related measures at the national level. It emphasised that this was designed with practicality in mind and would not incur any additional costs. Ireland suggested a creating paper or overview of existing mechanisms that within the UN system that are relevant to the work for the OEWG for the second substantive session.

- Estonia highlighted high levels of bilateral and regional cooperation already occurring in the area of implementing the recommendations of the 2015 GGE report. Canada referenced work happening through the Organization of American States (OAS) and urged that OEWG discussions strengthen regional work. New Zealand urged developing regional mechanisms and cooperation. Syria felt that any proposals to replace dialogue with regional arrangements would be too limiting.

- The necessity of including civil society and other stakeholders in regular institutional dialogue was a point made by a number of delegates such as India, New Zealand, France, Canada, the Netherlands, Poland, Finland, Estonia, Iran, and Australia. Germany noted it would be important to bring in the "wider UN cyber ecosystem" and also reminded that private companies own large parts of the internet, making them a stakeholder too.

Confidence building measures (CBMs)

- There was general agreement that CBMs are necessary to achieve a peaceful and secure ICT environment. The key goals of transparency, predictability, and cooperation were emphasised as being key instruments to avoid misperception, miscalculation, and escalation between countries.

- The success of regional cooperation, particularly current practices of the Organsation for Security and Cooperation in Europe (OSCE), the OAS, and the ASEAN Regional Forum (ARF), among others, were highlighted as an important first step in building confidence by a number of countries, namely Singapore, Japan, Malaysia, Switzerland, the Netherlands, Syria, Belgium, Spain, Germany, Australia, Estonia, the EU, Austria, India, Korea, Canada, and the UK.

- There was a strong focus by many states on how CBMs need to be translated into practical operationalisation. Malaysia, New Zealand, Germany, the EU, Austria, Montenegro, India, Canada, and the UK all supported practical confidence building measures rather than ideological norms, rules and principles. It was also noted that CBMs must be concrete and tangible, with examples including the identification of points of contact, information sharing through dissemination of reports, and dialogues such as this one.

- Cuba, Syria, and Ecuador noted that while CBMs are essential for international peace and security in the ICT environment, these confidence building measures should in no way act as a replacement for a legally binding instrument. Cuba also noted that regional confidence building measures remain subject to the nature of the region and the composition of regional organisation. For this reason, it is important to make CBMs more inclusive but note that there is still the need for a legally binding instrument but that CBMs contribute to the codification of norms, rules, and principles.

- The US defined the three different categories of confidence building as transparency measures, cooperative measures, and confidence building security measures. To this end, the US proposed the publication and sharing of strategy, doctrine, and white papers by states for the edification of all other member states. They also suggested establishing not only technology point of contact in the context of CERTs, but also the establishment of policy points of contact. Lastly, the US posited that confidence building security measures based on restraint would be an important confidence building measure so that states are more aware of other states' intentions and capabilities in the field of ICT.

- Iran identified the monopolisation of ICTs as a main source of mistrust between states. It said that the use of digital sanctions by states is alarming and has a negative impact on other confidence building measures and argued

that CBMs should not be limited to critical infrastructure, but should encompass national security, sabotage, economic crisis, and crypto currencies as well.

- Another point of discussion was the role that the private sector should play in confidence building measures. Chile highlighted that the private sector in smaller and middle countries have a greater capacity for preventing cyber attacks. In these instances, their inclusion in CBMs is crucial to build trust and avoid miscalculation, misperception, and escalation. Belgium welcomed the idea of including the private sector in confidence building measures and was open to developing it further.

Capacity building

- Capacity building described by all as of the utmost importance to the success of the OEWG and the establishment of a safe, secure, and peaceful cyber space. Many noted that capacity building is a "two way street" and is about more than developed states assisting developing states. Capacity building is about building trust, confidence, technological ability, skill, and ensuring that every country has the ability to make their voice heard and to take advantage of the benefits that ICTs can provide.

- Iran and Cuba focused on the fact that capacity building must not restrict ICT access for smaller states, in particular the monopolisation of technologies by more developed countries and the use of digital sanctions against smaller states by more developed states. Iran argued that sanctions and restrictive measures exerted by more developed states can have negative impacts on existing capacities. Iran also noted that the regional capacity building measures already in place are a step in the right direction, but they still leave some countries out. Therefore, new capacity building measures need to be under the auspices of the UN to ensure that no member state is left behind.

- There was a lot of endorsement for the specific capacity building measures that have already been put in place by various groups, countries, and organisations. Japan, Korea, New Zealand, Australia, Singapore, Israel, the UK, and Estonia all outlined specific capacity building measures they have implemented in their region and funds they've contributed, for activities ranging from such as CERT training, education, cyber security exercises, establishing measurement mechanisms to assess effectiveness.

- The UK defined a few specific areas that it hopes the OEWG report will address with regards to capacity building. They are cyber skills, strategy development, legislation support, cyber security culture, training, cyber exercises, law enforcement support, and CERT support. They asked that these specific areas be addressed in concrete ways moving forward so that the ideation of capacity building measures can be actualised in practical ways.

- The Pacific Island Forum spoke of the record connectivity they have experienced because of ICTs and the benefits it has brought. They noted though, that these benefits must be supported by security and the rule of law. The Pacific Island Forum also stressed the importance of taking a national cyber security approach to capacity building, meaning that as the region becomes more cyber secure, these capacity building partnerships can and should be used to address threats as well.

- The need to create a resilient cyber security system was noted by the EU and the Republic of Korea, who noted that despite its has faced serious cyber threats despite being a technologically advanced country and have been forced to improve their resiliency.

- The EU, the UK, Greece, Costa Rica, New Zealand, Algeria, and Egypt all stressed the importance of sharing best practices between states so as to build confidence and trust between states and to build capacities and knowledge around the globe.

- Ms. Katherine Getao, the Chief Executive Officer of ICT Authority of Kenya remarked that we are only as strong as our weakest link, and this was repeated by Australia and Canada. In order to secure a peaceful, open, and free

cyber space there needs to be international cooperation to strengthen one another and to ensure that all states are not only able to participate in the economic and social benefits of ICTs, but are equipped with the tools to protect and secure ICTs. This means not only developed countries giving resources and assistance to developing countries, but also requires developed countries to continuously improve their practices and technology know-how.

- Several states highlighted the importance of education, including to build technological skills alongside about the safe and proper use of ICTs. Estonia, Japan, the United States, and expert speaker Katherine Getao all highlighted the important role that education has for capacity building measures. Ms. Getao made the point that there is a pressing need for more jobs in this field and more people with the skills to execute those jobs. Education is an essential component of this and will tremendously help capacity building efforts.

- Egypt, Mexico, Bangladesh, and The Pacific Island Forum stressed the importance of tailored capacity building measures, noting that each country and region is unique and capacity building measures must be specific for that regions' particular needs. Blanket capacity building measures will not be effective for every region.

- Canada and Mexico encouraged gender to be taken into consideration when dealing with capacity building measures. Increasing the number of women and other marginalised groups into the field of ICTs will greatly improve capacity, confidence, and allow more voices to be heard.

Want to follow this issue at the 2019 UNGA First Committee?

Visit www.reachingcriticalwill.org

for statements, documents, and analysis published

through our *2019 First Committee briefing book* and

First Committee Monitor

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. 03
16 September 2019

Editor: Allison Pytlak
disarm@wilpf.org