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.07

18 February 2020

Photo by Steven Lelham, 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: CYBER SECURITY—A TEAM SPORT

Allison Pytlak | Women's International League for Peace and Freedom

The second substantive session of the UN's Open-ended working group (OEWG) on developments in the field of information and telecommunications in the context of international security was replete with analogies, inside jokes, and catch phrases covering everything from handwashing to weakest links. Yet the one that resonates the most is the notion of cyber security as a team sport. While this was first articulated in reference to the inclusion and role of non-governmental stakeholders at the OEWG and more practically in cyber security activities, the analogy has applicability for the Group as a whole—and with its Chair as the referee, as one state joked in its closing remarks. If member states can "play" together as a team through the final stretch and agree on a consensus report with good substance, then everyone wins, because there will be benefits for the international community. If members of the team start missing passes from their teammates, running the other way, or incurring penalties for bad behaviour—then we all lose out.

Multiplicities of views

Coming off of the second session, the team spirit feels strong. On-going positive dynamics, engaging leadership, and an ever-growing number of substantive proposals have managed to transform a process with an auspicious beginning into something that might just deliver on practical outcomes that could improve international cyber security in fundamental ways.

This is not to say that there are not differences in positions. There are, and significant ones at that. The largest discrepancies are clearly in the area of law, and in the context of norms and principles. The vast majority of states affirm that international law, especially the UN Charter, applies to state behaviour in cyber space—but there are a few outliers, particularly to point that that international humanitarian law (IHL) applies. Differences exist regarding the voluntary norms for state behaviour that were agreed by a UN Group of Governmental Experts (GGE) in 2015 and later adopted by the entire UN membership. Most states defend the existing norms as an important baseline and point to a lack of their implementation as the problem in stopping digital threats. Others feel that the norms don't speak to certain national or regional realities or that new ones are needed, a view supported by some civil society groups and international organisations. Some believe the voluntary status of the norms is insufficient to impact behaviour.

> On-going positive dynamics, engaging leadership, and an ever-growing number of substantative proposals have managed to transform a process with an auspicious beginning into something that might just deliver on practical outcomes that could improve international cyber security in fundamental ways.

Relatedly, some countries have called in past for a legally binding instrument, or a "cyber treaty" and have indicated that the OEWG should be laying the groundwork for its negotiation. As that appears unlikely at this juncture, frustration on this point could lead to resistance on other aspects of the report. There were rumours throughout this session of a pending working paper from the Non-Aligned Movement that (reportedly) contained proposals for the OEWG to endorse work on a cyber treaty, among other things. This is a point which right now is supported by a minority of states on the floor, but if passed within the bloc—even if it goes against the stated national positions of some of its members—then those proposals would enjoy a numerical advantage, and be harder to not account for in a final report and push the issue to the fore.

That aside, a temporary work-around to accommodate these different perspectives on legal and normative aspects could be to agree that while the 2015 norms are an agreed baseline and should be maintained, they do require some unpacking, better promotion, or maybe even some minor tweaking to be impactful in different contexts. An agreement in the report to allocate time, and resources, to do that as a first step before attempting to negotiate new norms, or a treaty, might temporarily allay frustrations and also serve to reveal where the real gaps are among the norms. The same could be said for international law, in that a blanket statement about its applicability can sound daunting. Initiatives like the Australian case studies which illustrate in more detail which laws apply in what contexts, and how, are useful both politically and practically. The suggestion for the OEWG to recommend that member states share how they interpret international law in this regard, or apply the norms, would be a solid first step, as is a forthcoming Mexican proposal to invite the International Law Commission to undertake an impartial and complementary study in this regard.

Differences of opinion on the way forward, as addressed under the topic of "regular institutional dialogue," were more pronounced in this second session. Russia, with support from others, has proposed extending the OEWG into the future. Some states, like Estonia, expressed reservations about doing this or establishing any dialogue platform, given the multiplicity of other normative fora on international cyber security that exist within, and beyond, the UN. Several other states, like Canada, New Zealand, and Finland, among others, expressed they are open to the establishment of "something" but it's too soon to know the form it should take, and functions need to first be delineated. This isn't necessarily problematic but outlining the functions of a new OEWG could be something for its supporters to then prioritise, given the time remaining in the process.

Apart from a future dialogue platform, there were multiple suggestions for bodies and mechanisms that could be established to support work across any of the six topics. Ideas floated so far range from a mechanism to improve global coordination of capacity building and matching resources, to a follow-up implementation mechanism. Involving relevant stakeholders in this work was expressed as an important pre-requisite to success by many governments, many of whom also spoke out against non-ECOSOC organisations having been blocked from attending this session.

The areas of agreement are largely found in the discussions about the threat landscape, and in relation to confidence and capacity building. For example, many states are encouraging better global coordination of capacity building efforts and recognise the importance of building from existing regional initiatives, which also applies to CBMs; and agree that capacity building should be politically neutral and guided by widely accepted principles—the elaboration of which could be a future task for a future OEWG or other body. These and other aspects of the conversation are outlined in the News in Brief section of this edition, as are the numerous concrete ideas proposed across all the six topics.

Unpacking human-centric

Since the first substantive session in September, there is ever-growing support for a human-centric approach to international cyber security, possibly buoyed along by inputs of this nature from many non-governmental stakeholders during the informal meeting in December. It has been particularly encouraging to hear more states articulating that there is a role for human rights within discussions on international cyber security and a sense that while the OEWG focuses on state behaviour, the impact of that behaviour on people, and their rights, cannot be overlooked. A new statement from the Freedom Online Coalition that was referenced often in this second session has helped to elaborate on the human rights-based approach to cybersecurity in conjunction with other resources from civil society groups.

Yet this is not a universal sentiment with some viewing this as beyond the purview of the OEWG and the UN General Assembly's First Committee, despite a track record of humanitarian disarmament initiatives within the Committee and a 2015 norm on human rights. This may be a point that becomes challenging to agree on in the report.

In its remarks to the second session, WILPF encouraged states to think more concretely about what human-centric means practically and advocated that a gendered approach would be central to that. As reported on separately in this edition, numerous states have indicated in their statements that the OEWG must take gender into account in its final report, possibly through recommendations on participation and representation, or to find synergy with national action plans on Women, Peace and Security, or in accounting for gender-differentiated impacts of cyber operations and incidents.

WILPF, along with ICT4Peace, also spoke to the question posed by the Chair about if the OEWG could ask members states "to unilaterally declare to refrain from militarisation/offensive use of ICTs?" There hasn't been an honest conversation in the OEWG, or anywhere, about the proliferation of states with offensive cyber capabilities and policies. It's something has been happening slowly in the last few years, and as WILPF noted, it sometimes feels as if that the international community has given up on trying to prevent the militarisation of cyber space and is rather focused on outlining how to do damage control by focusing on responsible state behaviour and rules of the road. Some states speak out against militarisation in their statements—but some of them are known to have run significant offensive operations. In the second session, countries like Denmark, Australia, and the United Kingdom outlined their reasons for going this route, which included the precision that a cyber operation can offer as well as feeling incentivised to pursue an offensive capability or policy because other countries have. Their frankness and uptake on this point was welcome in lieu of prior non-engagement; but more discussion and holding to account on this point is needed within the OEWG process, and the outside world.

The next round

The OEWG is fast approaching a turning point as the Chair will now develop a pre-draft of the final report that must be agreed by consensus at the third and final session in July.

The final report will be structured in a way to indicate areas of agreement; areas of disagreement; and then recommendations and conclusions under each of the six substantive topics that the OEWG considers. This format should be palatable for most because it leaves space to show all views when there is not agreement. The Chair reminded delegates that while the report will be organised under the six topics, these different sections are connected and impact one another.

This is often where even the most positive processes can turn ugly or become difficult. Given the breakdown of multilateralism in so many other security forums and recent late-night negotiations in processes on small arms and autonomous weapons, hoping for the adoption of a strong report without controversy can feel naïve. The problem with consensus-based decision making is that it only takes one spoiler to bring down a meeting.

Yet, the genuine goodwill and efforts to listen to one another are real. As more than a few delegations have stressed, "Let's focus on the 80 per cent of things where we have agreement, rather than the 20 per cent where we do not."

Since the first session, most member states have urged one another to focus on practical and achievable outcomes rather than trying to tackle the more politically challenging questions that have deadlocked other UN bodies on this subject. If the OEWG could make concrete recommendations in the areas of CBMs or confidence building or help to advance shared understanding on legal or normative interpretations, then those are successes that can help advance resilience and security in real ways.

"The urgency is real, and is felt by everyone around the world," Ambassador Lauber, the OEWG Chair reflected as he closed the session.

Apt words as this team advances into the next round.

NEWS IN BRIEF

Danielle Samler and Allison Pytlak | Lawyer’s Committee on Nuclear Policy and the Women’s International League for Peace and Freedom

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

Existing and emerging threats

- A common concern among states was the potential damage that can be done to critical infrastructure through the malicious use of information and communications technologies (ICTs). States agreed that protecting critical infrastructure is crucial, especially in an increasingly interdependent and digitised society. The Philippines suggested mapping what constitutes critical infrastructure and identifying which elements should be prioritised.

- The Netherlands pointed out that critical infrastructure is no longer confined to national borders. It used energy grids, international financial systems, and the internet itself as examples. Singapore built upon this point by stressing the importance of protecting supranational critical infrastructure because of how many states depend on them. It gave Amadeus, an international system used for flight ticket purchasing, and Swift, used for international banking, as examples. It said that these systems along with others must be strongly protected because of their international nature.

- Malaysia, the Republic of Korea (ROK), Switzerland, Canada, Singapore, New Zealand, Pakistan, Brazil, Peru, Iran, Kenya, the Philippines, the Czech Republic, China, Indonesia, and Chile identified the technical threats that will develop in parallel with technological development. The technical threats they identified were; the Internet of Things (IOT), artificial intelligence, big data, intellectual property theft, quantum computing, supply chain integrity, and block chain.

- The risks posed by cyber autonomous weapons was highlighted by Kenya and the Netherlands. The Netherlands expressed concern that once launched, these autonomous cyber weapons are not under human control and therefore cannot be trusted to abide by international laws posing a serious risk to international peace and security.

- The Netherlands, Malaysia, New Zealand, Indonesia, Switzerland, the United Kingdom, Australia, the United States (US), Germany, and Finland all stressed the need to approach existing and emerging threats in cyber space in a tech-neutral way. These states emphasised that it is not the existence of the technology itself that poses a threat to international peace and security, but the ways in which the technologies are used that can pose a risk. Australia, among others, noted that having a tech-neutral approach will ensure that the OEWG’s work remains relevant as technology further develops.

- Canada, Slovenia, Chile, Italy, Uruguay, and Bangladesh highlighted the need to promote comprehensive gender mainstreaming when discussing information and communications technologies (ICTs). Canada noted that different groups are affected differently by ICTs and this is certainly true for men and women. Incorporating a gender perspective will not only allow states to have a comprehensive understanding of the threat landscape, but will also aid in the implementation of UN Security Council Resolution 1325.

- South Africa, Algeria, ROK, and Russia urged delegates to not use the OEWG to list every possible existing or emerging threat, but to develop practical solutions to combat those threats. Russia expressed concern with having a discussion that gets too abstract or theoretical and encouraged the OEWG to focus on completing its “group homework assignment” and come up with solutions and practical steps forward.

- Argentina, Israel, South Africa, Colombia, Cameroon, the United Kingdom (UK), Brazil, Uruguay, Germany, Pakistan, and Kenya, among others, noted that the digital divide and varying capacity among states is a threat in and of itself as cyber security is an international issues and states are only as strong as the "weakest link". Kenya proposed installing a mechanism to increase resilience among countries who lack resources.

Rules, norms, and principles

- The implementation and operationalisation of pre-existing norms was brought to the forefront of the norms discussion. The Pacific Islands Forum (PIF), Singapore, the Czech Republic, Bangladesh, Canada, the Netherlands, Bangladesh, EU, Sweden, Lao PDR, Switzerland, Indonesia, Colombia, ROK, Japan, Belgium, France, New Zealand, Canada, Malaysia, Israel, Austria, Egypt, Chile, Pakistan, Croatia, UK, Australia, Denmark, Ireland, Kenya, Malawi, and Nigeria all made statements to this end.

- The Netherlands called upon the OEWG to find appropriate language in the norms, rules, and principles cluster that has complementarity between international security and individual human rights.

- Sweden stated that there have been many references to critical infrastructure, but the OEWG should clarify what counts as critical infrastructure (i.e. power supply, water and food supply, telecommunication, transport, etc.) Malaysia called for linking norms with practical and concrete initiatives.

- The Czech Republic noted that the implementation and operationalisation of norms should be a shared responsibility for all stakeholders as major security risks arise form cross-border breaches.

- Canada noted that the current norms are not widely observed even by those who have undertaken the commitment to operationalise them. New Zealand also highlighted that cyber stability is not threatened by the absence of norms or the lack of a framework, but it is threatened by the fact that some states are not abiding by the commitments they made.

- Mexico proposed presenting national reports on a voluntary basis to the UN Office of Disarmament Affairs (UNODA) on implementation of norms, rules, and principles in order to determine progress and the challenges that states have faced. This would allow for a general and focused analysis on where states are with regards to cyber security and identify work that still needs to be done. This proposal was welcomed by Austria, Australia, Norway, and Argentina, among others. Indonesia also suggested a reporting mechanism or an action plan to identify implementation gaps and challenges in different states and regions.

- India, Iran, Pakistan, Ecuador, Kenya, Cuba, Egypt, South Africa, and China called on states to refrain from developing offensive cyber capabilities so as to avoid the militarisation of cyberspace. Iran proposed that this be an additional norm to be put forth in the OEWG report.

- Australia, Denmark, UK, and Norway alluded to the fact that many states are already developing offensive cyber capabilities and there is no way to prevent it from happening. The UK highlighted that states have every right to develop these capabilities as long as they are transparent about their capabilities and their intentions. Australia seconded this notion by stating that states have the right to develop such technologies so long as they are consistent with international law. It also noted the precision granted by cyber "weapons" over kinetic ones.

- Most delegations spoke to the importance of including civil society, the private sector, public sector, academia, and all other stakeholders in these discussions.

- Australia, Canada, Norway, Finland, Germany, Ireland, and Japan, among others, expressed concern that non-ECOSOC accredited organisations were unable to participate in this session as their contributions in the intersessional meeting in December were useful. Norway said that the inclusion of non-ECOSOC organisations would have been an opportunity to demonstrate the open and multi-stakeholder approach.

- Iran said that stakeholders must held accountable for their activities.

- The role that regional groups and organisations can and should play in norm implementation efforts was highlighted by a number of states. Egypt noted the practical guidance that regional groups can provide by giving context to a region's specific cyber security needs. This was reiterated by Austria, India, the United Kingdom, Ireland, and Jordan. Among states there was general agreement that these regional organisations can better raise awareness of norms in their regions and are best equipped to give other states a solid understanding of the differing circumstances of their specific region and can better assess what resources, knowledge, or tools they need to implement the agreed upon norms.

- Jordan went further to say that other UN organisations should be included in discussions on cyber security and capacity building (CB) measures. They suggested incorporating UN organisations dealing with food security, water security, health services, and any other area that could be affected by malicious use of ICTs.

- Belgium pointed out that currently, the international community lacks specific mechanisms to manage crises and capacities and more effort should be made to establish crisis management mechanisms. It also noted that it is not only the responsibility of states to implement and understand norms—corporations and private actors also have the responsibility to share information and abide by their obligations.

- CB more generally was identified as a key element in states' ability to implement and operationalise the norms. Japan said that it is important to work on CB in parallel with raising awareness of norms. New Zealand, India, Chile, Jordan, Australia, and Kenya all stressed the importance of capacity building as it relates to norm implementation, understanding, and operationalisation.

- Bangladesh highlighted the fact that there are already accepted values and principles regarding the creation and operationalisation of cyber norms. They said that it is important to identify gaps in existing international norms not only of relevance by also of applicability.

- Switzerland noted that raising awareness of existing norms is of crucial importance and the universalisation of such norms should be a priority of the OEWG. It also stressed the importance of having a clear distinction between legally binding obligations and voluntary norms. Finland agreed, stating that the OEWG must ensure that the norms developed or elaborated upon are consistent with international law and do not cause confusion. Norway also made statements to this end.

- Iran commended the fact that the OEWG is the first and sole intergovernmental body that has provided countries with an opportunity to contribute to rules, norms and principles of responsible state behavior in cyber space. It also expressed that before discussion on raising awareness of norms and operationalisation, there must be an agreed upon list of norms that is more comprehensive than the norms in the 2015 GGE report. Iran proposed to structure the discussion on the norms around issues of ambiguities, terminology, introduction of changes, and elaboration of additional norms.

- Croatia stressed the need to clarify possible misinterpretation of norms and principles and how they should be implemented. It advocated for a guideline or a road map to help raise awareness and understand among states.

- Estonia highlighted the need for a resilient cyber space and universal norms that allow predictability—this can foster more stable development of economies and societies. The European Union (EU) also expressed the need for a resilient cyber space that revolves around effective implementation of agreed upon standards.

- Lao PDR encouraged promoting of dialogue across states and across sectors. It also advocated for building on existing norms, rules, and principles and perhaps exploring additional ones if necessary.

- Syria expressed disappointment with the fact that many states do not wish to create additional norms. They noted that the OEWG is tasked with developing rules, norms, and principles to guide the behaviour of states and that the world does not stop at the stage of the 2015 GGE report—cyber space is rapidly developing and the norms need to be elaborated upon and new ones need to be created as well.

- Australia discussed the complementarity between voluntary norms and legally binding obligations. It explained that these voluntary norms do not relieve states of their legally binding obligations under international law, but serve to complement it. It stated that if a violation of a norm is of sufficient gravity, it can also be inconsistent with principles of existing binding law.

International law

- All states agreed that international law and the UN Charter in its entirety apply in cyber space with the exception of Syria.

- States disagreed on whether or not there needs to be a legally binding instrument to govern and regulate state behaviour in cyber space. Egypt, Iran, Syria, Cuba, Indonesia, Pakistan, Philippines, and Venezuela argued for a legally binding instrument. Australia, Belgium, Austria, Colombia, Estonia, US, UK, Japan, the Czech Republic, Switzerland, and Italy argued against a legally binding instrument.

- Those in favour of a legally binding instrument argued that the voluntary norms are not sufficient enough to ensure that states act responsibly in cyberspace. Egypt noted that while the voluntary norms are a good step, they need to be complemented with politically binding commitments. Syria argued that the absence of a legally binding instrument, allows other states to behave irresponsibly and develop cyber capabilities that can be used against other states. Venezuela argued that a legally binding instrument could provide the "teeth".

- Australia clarified its argument against a legally binding instrument by reminding delegates that the agreed upon norms in the GGE reports sit alongside existing international law which is binding. They argued that while norms are voluntary, laws are not and the voluntary nature of those norms does not replace binding legal obligations.

- Bangladesh, South Africa, and Singapore took the middle ground when it came to whether or not a legally binding instrument is necessary at this juncture. Singapore recognised that while there could be benefits in having a legally binding instrument, cyber space is developing at a very rapid pace and requires immediate response and negotiations on a legally binding treaty would take a long time.

- A large number of states recognised that human rights and fundamental freedoms must be protected online just as they are offline. States paid particular attention to freedom of expression, freedom of association, and freedom of speech. The Czech Republic, Norway, Australia, Ghana, Liechtenstein, Finland, Switzerland, France, Chile, Italy, Argentina, Uruguay, the Netherlands, Bangladesh, Germany, Slovenia, and Canada, the Media Foundation for West Africa, the Association for Progressive Communications (APC), and Access Now, among others argued that the protection and promotion of human rights online must be a key pillar of responsible state behaviour in cyber space.

- Iran agreed with the fact that human rights must be protected online, but they also said those human rights should reinforce societal rights, values, morals, and the security of societies. They also argued that the protection of individual human rights in an ICT environment should not be used as a disguise for violating the rights of states.

- The Netherlands called on the OEWG to find appropriate language in its report to indicate complementarity between international security and individual human rights. Italy also stressed the importance of protecting human rights online.

- Norway, Ghana, Finland, Switzerland, Canada, UK, the Netherlands, and Germany all supported the most recent Freedom Online Coalition statement.

- Russia raised many practical questions about the applicability of international law in cyber space. For example, it asked what specific laws are applicable in cyber space; what instruments of international law can and should be invoked when there is a breach; what international arbitration body will deal with cyber incidents; what kind of cyber-attack would constitute an armed attack therefore allowing a state to invoke Article 51 of the UN Charter, etc. It argued that Article 51 is not always applicable in all scenarios; therefore the OEWG needs to identify specifically what constitutes an armed attack in cyber space.

- Egypt expressed disbelief that the guidelines of how international law applies are unclear. It said that in most cases, the recommendations on how international law applies in cyber space are quite clear, especially with regards to the negative recommendations of what states should not do.

- The Czech Republic suggested that cyber operations causing death or injury, damage and disruption to national security, damage to essential data, and disrupting government functions could reach the threshold of the use of force.

- Mexico recognised the need for practical steps forward with regards to the applicability of international law in cyber space. It suggested involving the International Law Commission (ILC) to conduct a study and specifically and concretely determine which laws apply and provide examples of how that law would be implemented or adhered to. South Africa agreed with this proposal and further suggested that the ILC could provide guidance on identification of customary international law through state practice. It challenged states that have publicly attributed cyber attacks to cite which specific international laws that have been violated.

- The applicability of international humanitarian law (IHL) in cyber space was recognised by a number of delegations including the Czech Republic, Pakistan, New Zealand, Ecuador, Estonia, Uruguay, Australia, Chile, Finland, Switzerland, Italy, Austria, Poland, Mexico, the International Committee of the Red Cross (ICRC), and APC.

- Austria noted that states are obliged to spare innocent civilians because IHL demands it. It noted that a targeted state can seek reparation and react through proportionate counter measures, but that must not justify abuses of sovereignty.

- The ICRC highlighted that malware used against a military objective may have collateral damage on civilians, but it is the states' responsibility to ensure that damage to civilians is not excessive.

- The Czech Republic, ICRC, and Estonia all noted that the applicability of IHL does not legitimise cyber warfare or the militarisation of cyber space. ICT4Peace called on states to publicly state that they will refrain from offensive cyber operations that target critical infrastructure

- WILPF compared the militarisation of cyber space to an arms race, citing the argument that states are developing offensive cyber capabilities because everyone else is. It expressed concern over this rationalisation and noted that every deliberate and conscious effort "to use digital technologies as a tool or as a medium for harm or for violence is another step along a path toward greater and greater militarisation of relevant technologies."

- Cuba argued that the alleged applicability of IHL would create conditions that could justify cyberwar and other attacks on states.

- Pakistan pointed out that IHL, the state's right to self-defense, and lack of clarity surrounding the rules of engagement in the ICT context raises concern for states. India highlighted challenges presented by a lack of consensus on definitions, terminology, and the threshold for the use of force—all of which makes the application of IHL in cyber space difficult. It highlighted core questions, such as what counts as a military object, and what counts as a civilian object?

- The US highlighted the lack of clarity about what constitutes use of force in the cyber domain. It recognised that information technology can be used as a weapon of sorts across a spectrum of lethality from everyday peacetime disruptions to activities above the threshold of the use of force.

- Belarus, Iran, Mauritius, the Czech Republic, Morocco, Singapore, Austria, Iraq, South Africa, Cuba, the Philippines, Switzerland, among others expressed the importance of upholding the principles of sovereignty, sovereign equality, and non-interference in cyber space. The Philippines noted that while it could support a legally binding instrument, there are questions about how that instrument would address state sovereignty and the imperatives of existing domestic laws.

Confidence building measures

- Globalisation of regional confidence building measures (CBMs) was an idea supported by a number of delegations, in response to questions provided by the Chair. States agreed that in order to build confidence, it is important to draw on the expertise, experience, and context that regional bodies can provide. States identified that regional bodies can assist with the implementation of norms because they are better equipped to identify the needs of a particular region and can build confidence regionally, which can then be expanded globally.

- New Zealand pointed out that not all states are part of a regional organisation which makes it also important to continue discussions on the global level in order to achieve full participation by all member states.

- Many states recognised that confidence building and CB are interlinked and heavily rely on each other for success. States recognised the importance of addressing these issues simultaneously.

- Mexico pointed out that different countries and regions have differing degrees of ability for development and therefore cannot implement confidence building measures equally. It suggested that states in the OEWG will need to acknowledge those differences and understand that some countries will need more support to implement standards and apply regional CBMs.

- Colombia, the PIF, Chile, Ghana, France, Australia, Russia, and Malaysia all endorsed the suggestion of establishing a global repository of existing CBMs and best practices.

- Australia suggested that the repository could be published using the UNIDIR Cyber Portal or the UN Secretary-General's annual call for submissions. Russia expressed concern that this global repository could fall into the wrong hands and urged that before creating a global repository of any kind, states decide who will have access to the repository, where it will be published, and other security measures.

- Egypt supported Mexico's proposal for periodic reporting and information sharing, arguing that it would be an influential tool for confidence building. It also noted that these voluntary confidence building measures are not sufficient and will not be fully actualised unless they sit alongside binding commitments.

- Colombia, Austria, Chile, New Zealand, Mexico, the United Kingdom, Australia, Canada, France, Russia, Ghana, Estonia, Ecuador, Slovenia, and Argentina, among others, supported the suggestion of establishing a list of points of contact.

- Australia stressed the importance of establishing diplomatic points of contact so as not to duplicate the existing list of computer emergency response team (CERT) points of contact that exist. Canada also warned delegates of duplicating existing lists, although they saw the added value of having such a list.

- Russia, France, and Canada all supported having a consolidated list of points of contact, however they put an emphasis on how that list is used. Russia noted that creating a list of contact points alone is insufficient, saying that states need specific rules and procedures to regulate how the contact points are to interact with one another.

- Canada and France highlighted that how the list is used is equally as important.

- The Philippines reminded states that it is essential to consider the greater political climate in which the OEWG pursues CBMs. They noted that the current polarised political atmosphere poses challenges and has an impact on what the OEWG does and affects how states navigate challenges vis-à-vis international peace and security.

- Iran and Belarus emphasised the impact of bilateral agreements on confidence building. Belarus argued that bilateral agreements could result in "good neighbourliness" which could then be expanded regionally and eventually globally.

- Russia stressed that CBMs in cyber space should be subject to concrete requirements. It urged that CBMs should not jeopardise the security of member states; give any one state an advantage; not be used as an instrument for interference in domestic affairs of states; and not be used to carry out unobjective assessments.

- The Netherlands, UK, Australia, and Denmark all emphasised the importance of transparency with regards to the development of offensive cyber capabilities. Denmark said that the "train has left the station" with respect to the number of states building offensive cyber capabilities, but states need to be transparent about their capabilities in order to build trust. Australia and the UK added that disclosing their offensive cyber capabilities can lead to increased transparency, accountability, and building patterns of responsible state behaviour.

- New Zealand suggested that in addition to sharing best practices and information, states should also share crisis management procedures, which was echoed by Singapore and Kenya. Singapore noted that practical drills and exercises can build trust and confidence between states. It also said that confidence building measures need to evolve to address evolving threats. Kenya advocated for regular international and regional cyber drills to build capacity for handling crises.

- A number of delegations emphasised the important role that other stakeholders can play in building confidence globally. Switzerland said that universities, civil society, and the private sector can play a big role in strengthening capacity, raising awareness, increasing transparency, and increasing confidence among states.

- Australia, Mexico, China, Cuba, Iran, ROK, Algeria, Kenya, Syria, Austria, Indonesia, Singapore, Croatia, Malawi, Bangladesh, Ecuador, Malaysia, Access Now, APC, Canada, UK, South Africa, Nigeria, Uganda, UN Department of Economic and Social Affairs, New Zealand, and the EU emphasised the importance of cultivating relationships between governments, the private sector, and civil society.

Capacity building

Proposals and possible OEWG outcomes

- New Zealand reminded the Group that delivering practical outcomes on capacity building (CB) is one of the more concrete things the OEWG can accomplish.

- Canada and Australia would support a call in the final report for better resource mobilisation to build capacity in order to promote the implementation of 2015 GGE reports and decisions of the OEWG. The EU said that the OEWG should address how CB can support implementation of the UN GGE reports. Belgium said the final report could indicate guidance on how CB programs can stimulate norms, rules, and principles for state behaviour.

- The PIF would support the OEWG report recommending improving global coordination in CB; noting that a simple mechanism to match needs with resources would be useful.

- Brazil said a coordination mechanism could be a good outcome from the OEWG.

- Mexico said that the focus in the final report must allude to the complementarity between CB and all other of the OEWG topics, which India also highlighted.

- Mexico referred to the proposal it has submitted for an implementation mechanism on CB.

- Egypt urged that the mandate of whatever institutional dialogue is proposed include a strong focus on coordinating CB efforts.

- Cameroon proposed that the OEWG could establish a fund to facilitate the participation of developing states in major meetings, or trainings, and to develop capabilities.

- Ghana said the OEWG can provide binding or voluntary guidance on best practices and practical guidelines for CB initiatives and should adopt a shared capacity building agenda with agreed priorities.

Guiding principles

- New Zealand asked if there are there principles of CB that the OEWG could recommended, drawing on where there is commonality from among principles currently in use or endorsed by member states. Nigeria and the PIF agreed with this approach.

- New Zealand emphasised that its principles include a partnership approach; a focus on results and practical outcomes; sustainability; and it would encourage and add a gender focus.

- Netherlands identified and support the following as principles of capacity building: ownership, sustainability, inclusivity, trust, transparency, and accountability.

- Cameroon highlighted principles of sustainability, ownership, gender sensitivity, and multi-stakeholder inclusion.

- Ghana said CB is core to a human-centric approach.

- Kenya suggested the OEWG could recommend the principles of inclusivity, sustainability, measurability, and effectiveness.

Coordination, matching, and regional work

- New Zealand outlined that heightened levels of cyber CB necessitates better coordination to avoid duplication and redundancy. Estonia and Australia agreed and said it is important to identify the gaps and where more CB is needed.

- Switzerland, with support from Australia, said it would like to hear from organisations who are in the "matching business" to learn about what works and what does not. Chile encouraged a mapping.

- Canada encouraged building on existing regional CB initiatives. Brazil agreed and encouraged the OEWG to include in its recommendations a call for broader cross-regional CB. Lao highlighted the necessity of building on existing CB frameworks in ASEAN, or elsewhere, as Estonia highlighted.

- The Netherlands, Argentina, New Zealand, Canada, and Estonia referenced the work of the Global Forum on Cyber Expertise (GFCE), as a good basis that could be expanded on, or learned from.

- Egypt referenced the interesting proposals made in at the multi-stakeholder meeting on harmonisation and strengthening CB at global and local levels.

- Argentina highlighted how the knowledge of regional land sub-regional organisations can be fundamental, referencing the Organisation of American States in particular.

Types of capacity building

- Indonesia outlined that CB for developing countries should be comprehensive, including policy and technical capacity; be coordinated and not overlapping; and be non-discriminatory and with no conditions.

- India also referenced the importance of building capacity in policy dimensions, and that it should be unconditional.

- Nigeria, Philippines, Singapore, and India stressed the importance of politically neutral CB. Syria questioned how this can be possible.

- Australia explained that its CB programmes always includes a technical and policy component in order to emphasise responsible use.

- Slovenia highlighted developing cyber diplomacy capacity.

- Ethiopia suggested that a mechanism to support developing countries in building relevant institutions would be considered a CBM.

- Norway noted that a gap which has not been clear to everyone is of the varying ability of countries to apply international law.

Considerations for effective CB

- South Africa, EU, Thailand, Canada, Kenya, the Philippines called for a gender sensitive approach to CB. Nigeria said it supports women in cyber security. Argentina highlighted building the capacity of women in peace and security processes as a "right and intelligent decision".
- South Africa shared lessons learned from its experience with CB for African women in the area of mediation as relevant for the OEWG and cyber capacity building.
- South African "context specific" and "sustainable" programmes. The UK noted that the most effective CB is based on local stakeholder input and priorities.); beneficiaries should feel empowered (France); demand driven (Egypt)
- Malaysia said that a "top down" strategy is vital in providing adequate protection, and that states should continuously send messages to leaders to make cyber security a top item on national agendas.
- Singapore stressed the importance of good metrics to assess what capacity building measures work, and which do not. It is currently developing metrics with the UN Office of Disarmament Affairs. The UK supported this. Canada spoke to the importance of an evidence-based approach.
- Most delegations supported an inclusive and multi-stakeholder approach to CB, and variously named different stakeholder groups ranging from the private sector to academia.
- Mexico encouraged states to think beyond traditional donor and recipient modalities to also explore south-south and triangular cooperation. The PIF, Czech Republic, and Brazil referenced a "two-way street" approach.
- Malaysia, Thailand, and Brazil spoke to the relationship between CB and building trust. Indonesia noted promoting norms and principles of state behaviour.
- Canada felt that CB is critical for implementation of the norms and for CBMs, stressing that they are interlinked, which was echoed by Estonia in calling CB "an enabler".
- Nicaragua, the PIF, the Netherlands, and Norway highlighted the relevance of cyber capacity building for achieving Sustainable Development Goal (SDG) 9; the Netherlands further referenced SDG 5 and SDG 10 and encouraged integration of the SDGs into capacity-building initiatives and that the OEWG should ensure and codify this link, and to reference it in the final report. This was supported by Norway.
- South Africa, Uganda, CARICOM, Chile, Mauritius, and Ghana stressed the risks and challenges of cyber crime, encouraging that the final report reflect this.

Existing intiatives

- Uganda shared its experience in developing a first-ever national cyber security strategy, which also aims to develop its ICT sector. The UK urged that stories and examples like these be shared in the final report.
- Antigua and Barbuda explained that CB increases not only the ability of the Caribbean Community (CARICOM) to combat cyber attacks regionally, but will increase trust and confidence throughout the region. It noted though that every state in the region is unique, with its own needs.
- Thailand described a Japan-ASEAN capacity building project. ROK spoke of its training programmes in East Asia with the International Committee of the Red Cross (ICRC).
- Slovenia highlighted capacity building activities in the Western Balkans that includes information sharing and incident response.

Role of UN

- South Africa encouraged enhancing existing UN structures rather than developing new ones. Indonesia noted the central role of UN in promoting implementation of norms to CB programs.
- Mexico noted there is an entire UN architecture that already exists in other areas

of digital cooperation and encouraged the OEWG to focus on cyber security.

- Kenya said that the UN is uniquely positioned to coordinate CB at a global level and could start by making a registry with contact points; synthesising lessons learned; developing a road map for CB; availing states of resources; and tracking progress.

Regular institutional dialogue

- Most delegations welcomed the opportunity for inclusive, inter-governmental dialogue that has been presented by the establishment of the OEWG. New Zealand highlighted it as a CBM in and of itself. Argentina spoke of the OEWG's "special responsibility" for dialogue, and in creating trust.

- Most delegations agreed on the general importance of continuing such dialogue, although views varied on purpose, format, and how or when to take that decision.

- India indicated it would like the OEWG process to continue, noting the need to systematise UN discussions on this subject. Algeria suggested that the final report of the OEWG could consider establishing a permanent OEWG or subsidiary body. Iran said that the OEWG needs to continue its work until and unless another mechanism is agreed and encouraged the presentation of a roadmap for work beyond 2020. Cuba would like to continue work in the UN system until the establishment of a legally binding instrument.

- Kenya also supported a continuation of the OEWG and stressed engagement with all stakeholders, highlighting gender diverse representation in particular.

- Russia noted the obvious benefits of the OEWG format and general optimism around it, regardless of which states voted for its establishment. It hopes that the final report can include a recommendation to the UNGA to extend the OEWG's mandate into the future for a longer period than two years, which is standard. Russia indicated it would like the current OEWG chairperson, Swiss Ambassador Lauber, to become its "Chair for Life".

- Austria and ROK noted that it would be important to first see what comes out of the OEWG, as it is on-going, and how this process is managed.

- China suggested exploring the establishment of an effective international mechanism within framework of the UN to focus on peace and security aspects of cyber security.

- Singapore sees value in exploring characteristics of a future dialogue mechanism.

- The US stated that it would listen to suggestions for a future dialogue mechanism, but also reflected on the importance of being cautious, stating that there is no "silver bullet" to achieve consensus on matters of international cyber security and reminded that past progress such as achieved through the GGEs took years of deliberation.

- Estonia said it was not sure of the value of regular dialogue, and urged a focus on implementation of norms, CBMs, and CB. It had questions about the purpose, scope, participation and financing of a new dialogue body. Israel said it is premature to recommend the establishment of a new permanent, institutional dialogue body, and urged first defining what gaps exist and need to be addressed.

- Canada, New Zealand, UK, Switzerland, Mexico, and Finland were supportive of on-going dialogue but urged that "form should follow function", in that states must first determine the objectives of a new dialogue platform or body. Japan and EU highlighted the necessity of carefully examining the purpose, mandate, financing, and participation modalities.

- Egypt, Canada, UK, EU, Poland, Ghana, US, Switzerland, Austria, and Argentina among others, stressed the importance that any future platform should not duplicate the work of other forums or UN bodies. Most indicated that the focus on cyber security in the context of international peace and security is unique

- Mexico encouraged establishing synergies with other bodies, while avoiding duplication, and to not work in a disconnected way.

- Indonesia, Canada, New Zealand, Ghana, and the PIF highlighted financial considerations implicit in establishing a new dialogue platform. The UK cautioned that it would be inappropriate to divert funds to a new administrative mechanism. Austria, Ghana, and the PIF highlighted the resource burden that more meetings place on smaller states.

- Australia floated the idea of considering a location other than New York for a future dialogue platform.

- Algeria, EU, US, Singapore, Austria, Argentina, and Pakistan noted that maintaining consensus-based decision-making would be important for any future platform.

- A majority of delegations stressed the importance of engaging with other stakeholders in any future platform. Germany noted that a big success of the OEWG was the multi-stakeholder intersessional meeting, and recognised it as something to include in any new mandate. Ghana said a future dialogue platform should have more formats for multi-stakeholder dialogue.

- The US reflected on the importance of participants having a basic understanding of issues and how they "play" within the international environment.

- Poland, Japan, Kenya, US, Belgium, Mexico, and Germany, among others, referenced the on-going work of the GGE as being part of any consideration of a future dialogue platform established by the OEWG. Australia also highlighted the issue of timing, as the GGE will conclude its work one year after the OEWG.

- Switzerland referenced the Geneva Dialogue on Responsible Behaviour in Cyber Space, which looks at non-state actors such as civil society, academia, tech community, and the private sector.

- Some states put forward more concrete ideas for what a future body or platform could address, or where to prioritise future effots. Egypt suggested the creation of functioning mechanisms for reporting, confidence and CB.

- Indonesia suggested a focus on how to reduce risk; develop and implement norms; as well as to disseminate best practices of regional cooperation.

- The EU said that future dialogue could build on efforts to help with norm implementation and CB. China suggested a focus on "situational assessments" that would work toward national codes of conduct and a legal instrument, which was similar to ideas expressed by Iran.

- Egypt highlighted the UN Programme of Action on small arms and light weapons as a possible model to consider. Indonesia suggested the possibility of joint UNGA Committee meetings, such as the annual joint meeting between First and Fourth Committees on outer space.

- Australia requested that a specific proposal be made concerning a mandate for future discussions, in order to focus discussion.

Gender

- Australia, New Zealand, the Netherlands, Canada, Chile, Ecuador, Argentina, Italy, Bangladesh, Thailand, Slovenia, EU, UK, Cameroon, South Africa, Kenya, Nigeria, Switzerland, APC, and WILPF all referenced the importance of incorporating a gender perspective into OEWG discussions on international cyber security at different points throughout the session.

A NEW 'WOMEN IN CYBER' FELLOWSHIP HAS A BIG IMPACT ON THE OEWG

Allison Pytlak | Women's International League for Peace and Freedom

Toward the end of the penultimate day of the second substantive session, the OWEG Chair, Amb. Lauber of Switzerland noted that when reviewing the delegation lists he realised that something "fantastic" had occurred at this meeting, for which applause broke out in the conference room: gender parity.

While an equal number of women and men participating in an international conference in the year 2020 shouldn't seem that farfetched or unusual, it unfortunately is, especially in the disarmament and arms control space. A report from the UN Institute for Disarmament Affairs notes that of all the UN General Assembly committees, the First Committee on Disarmament and International Security has the lowest proportion of female diplomats, among other trends.[1] For over a decade, WILPF's disarmament programme Reaching Critical Will has been tracking the sex of individuals delivering statements to UN disarmament forums on its website as a part of its conference monitoring; an analysis of which also demonstrates consistent gender inequality.[2]

What largely accounted for the rebalancing in this session is the Women in International Security and Cyberspace Fellowship, a joint initiative of the governments of Australia, the United Kingdom, Canada, the Netherlands and New Zealand. It promotes greater participation by women in discussions at the UN on international peace and security issues related to responsible state behaviour in cyberspace. The Fellowship supported the participation of more than 20 women from Africa, Asia, the Pacific, Latin America, and the Caribbean to this and the upcoming final session in July. Most are already working within their governments on cyber security, either from a technical or policy perspective.

Yet, and as WILPF has long pointed out, improving the gender diversity of a meeting room just by filling seats with women over men is not the right approach. Diversity needs to be built into decision and policy-making processes across a range of roles and go beyond gender to account for the views of other marginalised or minority groups with a stake in the issue at hand. It cannot be tokenistic.

Therefore what is noteworthy about the Fellowship is that alongside the opportunity to participate in the session, it also included three days of advance training beforehand, and will offer three more days in July. The training included backgrounders on the UN cyber processes; how gender perspectives are being taken up elsewhere in the disarmament community, and what the opportunities could be for the OEWG; what the "hot button" issues are in the OEWG context; and on negotiation skills. It also featured a "speed mentoring" event that enabled frank conversations and sharing between the fellows and selected mentors. The Fellowship is ensuring that participants develop relevant knowledge and skills so as to contribute to policy and position development and work with other delegations.

This comes at a time when there has been greater uptake of "gender" in disarmament; whether it be the focus of the Arms Trade Treaty states parties conference on gender and gender-based violence in 2019[3]; the first-ever side event about the gendered impacts of biological weapons in the context of a meeting of the Biological and Toxin Weapons Convention[4]; and a significant upsurge in gender references within UNGA First Committee resolutions in 2018 and 2019[5], among other wins.

Yet in the field of international cyber security, little is known about the gender dimensions of interstate cyber operations—even while there is strong documentation about online GBV and the human rights dimensions of this issue. Numerous delegations referenced gender considerations during this OEWG session however—usually in the context of participation, but some also with reference to frameworks like the Women, Peace and Security Agenda, the Sustainable Development Goals, or in capacity building activities. These references are captured in more detail in the News in Brief section of this edition. By our count, 119 out of 280 statements delivered during the second substantive session were delivered by female delegates.[6]

WILPF, along with other researchers will publishnew research this spring that will explore why gender matters in international cyber security, with the support of the Government of Canada. The report will provide an evidence base and recommendations for how the OEWG could concretely account for a gender perspective in its final report, and any future work at either national, regional, or international levels.

1. Renata Hessmann Dalaqua, Kjølv Egeland, Torbjørn Graff Hugo, *Still Behind the Curve*, 24 June 2019.

2. See www.reachingcriticalwill.org

3. Final Report, ATT/CSP5/2019/SEC/536/Conf.FinRep.Rev1, 30 August 2019.

4. Reaching Critical Will, "Better late than never: gender perspectives have made their way into BWC discussions", *Report on the 2019 Meetings of Experts of the Biological Weapons Convention*, August 2019, http://reachingcriticalwill.org/news/latest-news/14015-report-on-the-2019-meetings-of-experts-of-the-biological-weapons-convention#gender.

5. Katrin Geyer, "Gender", *First Committee Monitor, No. 6*, 9 November 2019, http://reachingcriticalwill.org/news/latest-news/14015-report-on-the-2019-meetings-of-experts-of-the-biological-weapons-convention#gender.

6. See http://reachingcriticalwill.org/disarmament-fora/ict/oewg/statements#second.

Photo by Johanna Weaver, via Twitter

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

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

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. 07
18 February 2020

Editor: Allison Pytlak
disarm@wilpf.org

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