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.05

9 December 2019

Photo by Khalid Belkhalfi, 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: BREAKING SILOS, BUILDING COMMUNITY

Allison Pytlak and Paul Meyer | Women's International League for Peace and Freedom and ICT4Peace

Some of us in the international community, particularly those working in multilateral spaces, speak of breaking down the institutional siloes that divide our work in order to more effectively address issues of common concern and reduce redundancy. Modern problems are complex and multi-dimensional, and their solutions likewise require a degree of collaboration and communication that the structures we work within do not always easily allow for or encourage.

The intersessional meeting of the UN's Open-ended working group (OEWG) on developments in the field of information and telecommunications in the context of international security, held 2-4 December, may be a rare exception.

Per the UN General Assembly (UNGA) resolution that established the OEWG, this informal meeting was always intended to be the one opportunity for non-governmental stakeholders to contribute their voices and expertise to the process. It was an opportunity made even more important after a widespread denial of accreditation to observe the OEWG's first substantive session in September.

The scale and diversity of participants exceeded the expectations of many however. The over 110 entities registered included non-governmental organisations, academics, research and policy institutes, technologists, software providers, and representatives of other relevant intergovernmental processes. While regional and gender diversity was not perfect, it was also not imperfect. The meeting and OEWG chairpersons, along with the UN Secretariat, further encouraged the contribution of video statements from those unable to participate in person and have done much to ensure that interventions and position papers will be posted online and be accessible to the UN membership, which is not always something offered to civil society.

Throughout, the member states present were largely in "listening mode"—to extent that none raised comments or gave inputs until prompted to near the end of the first day. The meeting did not reach the degree of conversational exchange that may have been desired by its organisers but the content of interventions was extremely rich and as the meeting progressed, some began to refer to and take note of what others had said before them, or even ask questions in the open.

Yet what was perhaps most unique about the meeting is that the vast majority of participants did not come from the disarmament and security field in which the OWEG process is rooted. Rather, most participants represented groups and institutions active in other issue areas pertinent to the OEWG's focus: internet governance; digital rights; technical capacity building; and technology research. Their inclusion might seem like an obvious approach to take on such a complex topic, but it is actually fairly rare in UN meetings to have a majority of interested civil society groups coming from spaces that are not closely associated with the underlying mandate.

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

It did mean that participants entered the discussion from different starting points or used at times, different points of reference and vocabulary but the net result has been the chipping away at some silos and hopefully, the building of new community and a more informed dialogue process. As some acknowledged in their statements, the meeting was in and of itself a confidence and capacity building mechanism.

Continuing in this vein may not be embraced by all states, however, although even on government delegations there appear to be a mix of those who

specialise in cyber security and those who follow the full range of UNGA First Committee subjects. Most prefer to stay close to the "in the context of international security" part of the OEWG's title, and even those willing to be slightly more expansive are going to be constrained by the OEWG's mandate and place in the evolution of a longer discussion about international cyber security at the UN. But a point illustrated well throughout this meeting is that because ICTs are so ubiquitous in our lives, and that a range of non-governmental actors play central roles in ICT development, maintenance, and security, broader inclusion than usual is going to be necessary in this process.

Diversity also generated a wide spectrum of concerns. Certain themes occurred regularly throughout the session and are summarised below. Greater detail can be found in the "News in Brief" section of this edition of the Monitor.

Several participants pointed to the **increase in cyber security threats**, originating from both state and non-state actors, in number and magnitude. Spear phishing and business mail compromise were notably on the rise with attacks more specifically directed. The increased "weaponisation" of cyber space was criticised by some and in particular indications that critical infrastructure was still being targeted despite the agreed norm prohibiting this.

The impact of cyber threats varies with the defence capacities of countries and individuals. Several non-governmental organisations (NGOs) stressed the **disproportionate vulnerability** of many developing societies and marginalised groups within them. This often included recognition of a need for more **gender diverse** delegations in cyber security meetings, as well recognition of the gender-differentiated impact of cyber operations, points highlighted by both member states and non-governmental participants. Continued support by the donor community for capacity-building efforts to help bridge this divide was universally endorsed.

Frequent references were made to the necessity of a rights-based, **human-centric approach** to the governance of international cyber security activity. Concern was voiced on the targeting of human rights defenders by some states utilising ever more sophisticated cyber surveillance systems and there were calls for the export of such systems to be strictly controlled.

There was a refrain throughout the session that states need to be **held to account** for their international cyber operations. Such accountability would require reliable attribution a possibility that is deemed more feasible today than in the past. Several proposals for a network of accountability inputs drawn from the technical security community that could support an accountability procedure at the diplomatic level were suggested.

A possible model for a cyber security "peer review mechanism" is the Human Rights Council's Universal Periodic Review process. Other ideas included variants of the International Atomic Energy Agency or the National Transport Safety Board, but a form of public-private partnership which could ensure credible forensic capabilities and an equitable accountability forum was considered desirable by many, and perhaps even as a suitable "deliverable" for the OEWG itself.

> "We don't have the luxury of just talking about these issues."

A prominent theme in the discussions was the perceived urgency for concerted action by states in addressing the growing threat of malicious international cyber activity. "We don't have the luxury of just talking about these issues" as one industry representative put it. The fact was noted that nine years have passed since the initial consensus report of the UN Group of Governmental Experts (GGE) process on norms of behaviour in cyberspace, and its calls for international cooperation to prevent threats to peace and security, yet this threat has only grown in nature.

The continued divergence of views as to whether it is best to **maintain the status of agreed norms** of responsible state behaviour (such as generated by the UN's GGE process) as voluntary, politically-binding measures or to give them a legally-binding nature was evident during the session, with proponents of either variant covering both

sides of the aisle. There was however a general sentiment that in the near term the emphasis should be on operationalising the existing agreed norms rather than on generating new ones, although the suggestion was made that the ban on attacking nuclear facilities as an element of critical infrastructure should be extended to nuclear weapon complexes as well. The contribution of "Ethical Codes" for cyber incident responders to help prevent destabilising action was also highlighted.

Several participants flagged the **continued gap in awareness** (both among the general public, but also at the political level) of the norms of responsible state behaviour that have been agreed. Greater efforts to promote "cyber hygiene" and "best practices" were seen as important complements to the work of the cyber specialist community in and outside government.

Capacity building proved to be the topic with the greatest number of interventions, and exceeded the time allocated to it. A majority of speakers focused on identifying practical steps to increase capacity between states, the private sector, the public sector, and civil society—but many others also highlighted the importance of building capacity at individual levels, and to those most at risk. A lot of existing initiatives were described, including lessons learned from them, that reinforced earlier points about a digital divide.

Ways forward on a **multi-stakeholder approach** was the theme of the final session. Maintaining an inclusive and multi-stakeholder approach in the OEWG received wide endorsement and little dissent from states in the room. Several practical suggestions were made how to do this, ranging from effective UN meeting formats to the importance of dialogue at national and regional levels, and sponsorship programmes.

However, the future of civil society engagement at OEWG sessions is not clear. Presumably an accreditation process will open up for the next two formal substantive sessions in February and July but it's not guaranteed that this will happen, and neither is the granting of accreditation to all interested groups, or having opportunities to contribute in the room. The report of this meeting—which held an informal status—will be delivered by the chairperson, David Koh of Singapore, to the OEWG chairperson, Ambassador Lauber of Switzerland, in February. It will likely be a factual summary of what was discussed, and where there was agreement or disagreement therein. What would also be of value is if the meeting report could include all the practical suggestions made by participants across all topics, in an annex or attachment, for ease of reference and possible uptake by states.

Regardless of what occurs in formal meeting rooms, it will be difficult to dial back the engagement of non-governmental stakeholders. Some silo-ing is necessary in order to focus work and play to strengths but keeping the OEWG in a vacuum will do the process no favours, and risks achieving effective outcomes that are implementable and make sense in the real world. As stated in the previous edition of this Monitor, the hope is that this is the start, and not the end, of a more robustly inclusive UN dialogue on cyber security writ large.

SIDE EVENT REPORT: GCSC PRESENTS FINAL REPORT

Louk Faesen | Global Commission on the Stability of Cyberspace

On 2 December 2019, the Global Commission on the Stability of Cyberspace (GCSC)[1] hosted the a side event titled "Advancing Cyberstability: from formulation to implementation" at the multi-stakeholder intersessional consultations of the United Nations Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG).

The Global Commission appreciates the opportunity to engage with the OEWG on matters pertaining to international peace and security in cyber space, and how the proposals of the GCSC report *Advancing Cyberstability*[2] can contribute to ongoing global efforts, both within and outside of the United Nations, to enhance responsible behaviour in cyberspace. The GCSC was encouraged to see the level of engagement and support for its proposals from the OEWG participants. It signifies a significant opportunity to bring the perspectives of the Global Commission and other stakeholder groups into the OEWG—a forum aimed at achieving similar objectives within the multilateral context of the UN's First Committee on Disarmament and International Security.

Commissioners Virgilio Almeida (Brazil), Christopher Painter (US), Elina Noor (Malaysia), Wolfgang Kleinwächter (Germany), and Abdul-Hakeem Ajijola (Nigeria) presented the GCSC report, offering a framework for advancing the stability of cyberspace. Emphasising a concerted multi-stakeholder approach, the cyberstability framework comprises four principles, eight norms of responsible behaviour, and six recommendations for the international community and wider cyber security ecosystem.

Participants welcomed the principles, norms, and recommendations of the Global Commission, underlining their relevance to the work of the OEWG on guiding responsible behaviour in cyberspace. The first norm on the protection of the public core of the Internet[3] represents the Commission's attempt to understand what is critical for cyber space to work. The second norm, a call to protect the electoral infrastructure, is an example of what is critical in cyber space—which core infrastructure or services are being powered by cyber space and are crucial for our societies, yet not covered by existing norms. Other GCSC norms were issued against tampering, against commandeering of information and communications technologies (ICT) devices into botnets, for creating a Vulnerability Equities Process, to reduce and mitigate significant vulnerabilities, on cyber hygiene, and against hack-back by non-state actors.

Norm adoption and implementation are necessary steps towards accountability and stability in cyberspace. The need for greater implementation and awareness of proposed norms by the entities that are capable of their implementation was raised, as well as those actors the norms are meant to protect. Capacity building and outreach must include those affected by norms, as these stakeholders may be unaware of the potential impact a norm might have for them. The GCSC has already made progress in terms of implementation of its work on norms. The Paris Call for Trust and Security in Cyberspace[4], a high-level declaration signed by more than 1,000 organisations and states, includes five out of eight GCSC norms, including the protection of the Public Core of the Internet. This GCSC flagship norm has also been embedded into European Union (EU) legislation through the EU Cybersecurity Act.[5]

In response to a question on the role of non-state actors in accountability, Commissioners reiterated that norms will not be effective if those who violate them learn that there is no price for doing so. While attribution in the government context is often a political act, both state and non-state actors play a role in holding malicious actors accountable by responding appropriately to norms violators, ensuring they face predictable and meaningful consequences. Furthermore, the Commission recommends state and non-state actors should collect, share, review, and publish information on norms violations and the impact of such activities.

The Commission believes that a multi-stakeholder approach to norm adoption, implementation, and accountability is crucial. The formation of a community of interest around each norm allows for a more concerted (instead of concentrated) effort to engage the states, private companies, not-for-profit organisations (including standards organisations), and civil society that are affected by the norm. Finally, the GCSC recommends that a standing multi-stakeholder engagement mechanism be established to address stability issues, one where states, the private sector (including the technical community), and civil society are adequately involved and consulted.

The Global Commission was asked to share its best practices and experiences gained over the course of its mandate. Whilst the GCSC is focused on the traditionally state-led dialogue on international peace and security, it did so by using collaborative and consultative methods from the Internet governance community. Over the last three years, the Commission has had the opportunity to develop its ideas and engage with a wide range stakeholder groups through its public hearings, meetings, consultations (including online, public Requests for Comments), peer reviews, commissioned research, and many other engagements. These methods are aimed at facilitating effective multi-stakeholder cooperation and gathering broad input from a wide range of stakeholders. They represented the bedrock of interactions with the wider community of state and non-state experts and will form the basis of the advocacy of the proposals in the report going forward.

For an overview of the report, please see the Fact Sheet[6] and for a copy of the report, visit *Advancing Cyberstability.*[7]

1. *See https://cyberstability.org/.*
2. *Report available at https://cyberstability.org/report/.*
3. *See https://cyberstability.org/report/#appendix-b-the-norms-of-the-gcsc.*
4. *Details on the Paris Call can be found at https://pariscall.international/en/.*
5. *https://cyberstability.org/news/european-union-embeds-protection-of-the-public-core-of-the-internet-in-new-eu-cybersecurity-act-2/*
6. *Available https://cyberstability.org/wp-content/uploads/2019/11/GCSC-Fact-Sheet.pdf.*
7. *Available https://cyberstability.org/wp-content/uploads/2019/11/GCSC-Final-Report-November-2019.pdf.*

Photo by Louk Faesen

SIDE EVENT REPORT: GENDER AND CYBER SECURITY

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

Gender matters in international cyber security.

That was the overriding message of a side event organised on 3 December by the Permanent Mission of Canada and the Organization of American States (OAS). To date, the gendered impact of cyber operations and incidents, as well as gender inequality in the cyber security area, has been a largely unexplored part of the discourse in the in the UN cyber processes. This well-attended event was an effort to start that conversation in a more meaningful way, including by looking to examples from advancing gender perspectives in disarmament and addressing online gender-based violence (GBV).

Opening remarks by the Ambassador of Canada, H.E. Louise Blais, and Belisario Contreras of the OAS reinforced the importance that both attach to this subject including through several practical actions that Canada and the OAS engage in, such as research, sponsorship to meetings, and in their capacity building activities.

Renata Hessmann Dalaqua of the UN Institute for Disarmament Research (UNIDIR) provided the main presentation of the event, which gave an overview of how gender perspectives have grown steadily as a priority in disarmament and arms control fora. She illustrated that UNIDIR's work usually follows two tracks in this regard: advancing gender equality in representation and participation in disarmament meetings; and consideration of how gender norms lead to differentiated impact of weapons and armed violence. Ms. Dalaqua provided statistics on participation from UNIDIR's report, Still Behind the Curve, to demonstrate the stark gender disparity in who participates in UN disarmament meetings. She noted however that this is changing, but that it has very much been a civil society driven process. She suggested that some of the lessons from their experience in disarmament could be applicable to cyber security, but there is less of an evidence base to draw from.

The conversation then opened up to four discussants to react to the UNIDIR presentation.

Allison Pytlak of the Women's International League for Peace and Freedom (WILPF) described her organisation's work to advance gender perspectives in disarmament and agreed with much of the UNIDIR presentation. She also highlighted the risks of a gap between what is agreed in UN meetings on gender and disarmament, versus what is implemented as policy or practice back home. Ms. Pytlak said that what has also been helpful in WILPF's work is to demonstrate linkages between gender-sensitive disarmament commitments and those that states have under other agendas, such as Women, Peace and Security or human rights conventions like the Convention on the Elimination of all Forms of Discrimination Against Women (CEDAW) to encourage policy coherence.

Deborah Brown of the Association for Progressive Communications (APC) shared its work in providing "gender report cards" for internet governance meetings, which show that while women are involved they are usually either a minority in meetings, or speak more to so-called soft issues, and less to technical ones. Ms. Brown also shared some of APC's research in looking at the gendered impacts of data breaches in Brazil and South Africa, in which the personal health information of women put them at risk for either having abortions in a country where it is not legal, or for having filed complaints of rape.

Sarah Shoker of the University of Waterloo highlighted that states have fundamentally different views of "cyber security" that may impact the extent to which gender considerations can be incorporated. For example, there is a huge emphasis on the protection of national critical infrastructure, but that this is not being defined in a way that includes human security—including women—as critical. Ms. Shoker noted that it appears to still be challenging to think about women's access to technologies as a security concern, instead of being "shunted off" as a development concern.

Finally, Raman Jit Singh Chima of Access Now shared information about the extent to which online harassment is gendered, drawing from evidence collected as part of a help line that his organisation operates. He illustrated that over 52 per cent of the cases of online harassment they encounter in South Asia are gendered, and that often it includes threats to physical harm offline. Governments sometimes use obscenity as a pretext for Internet shutdowns in which their actual objective is to regulate sexual and reproductive rights.

Following these reactions, Irene Poetrano of Citizen Lab moderated a discussion that saw a very high number of contributions and responses from the floor. A majority of these came from representatives of Latin American countries, who agreed with what had been said about the challenges of access, representation, and participation. Many shared examples. Others highlighted that it important to do more than just look at numbers of women and men in a conference room, but consider what positions are occupied by different genders within government or other structures. It was noted that more men need to be part of these discussions, and to draw from existing frameworks like the Beijing Declaration and Platform, and the WPS Agenda as much as possible.

Going forward, the Government of Canada will be initiating a research project with APC, WILPF, and the University of Waterloo to identify ways in which the UN's international cyber security processes can generate more gender-sensitive outcomes.

Photo by Daniel McBryde

NEWS IN BRIEF

Danielle Samler and Allison Pytlak | Lawyers Committee on Nuclear Policy and 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 in what was an informal meeting.

Existing and emerging cyber threats: a view from academia and civil society

- Derechos Digitales, Global Partners Digital (GPD), the Women's International League for Peace and Freedom (WILPF), the CyberPeace Institute, Access Now, the Cyber Policy Institute, the CAPA 8 Foundation, the Association for Progressive Communications (APC), and R3D, among others, highlighted in various ways the threats to human and personal security. Some of these groups explicitly called for a more human-centric approach to cyber security in the OEWG. GPD, WILPF, Access Now, Association for Progressive Communications (APC), ICT4Peace, and the Universidad Nacional Autónoma de México made specific reference to the importance of protecting of human rights in the context of the work of the OEWG and international cyber security. WILPF said that there is precedence for this in disarmament bodies and agreements, such as the Arms Trade Treaty.

- The Forum of Incident Response and Security Teams (FIRST) emphasised in its scene-setting remarks that an inability to bring people online in an equal way presents security challenges because there is not always understanding of their unique needs. Derechos Digitales, WILPF, and GPD highlighted that there is regional and national variance in cyber security concerns and threats, which requires more tailored approaches. APC described that different groupings of people experience cyber threats differently and GPD described inequalities in access to technology.

- The UN Institute for Disarmament Affairs (UNIDIR) asked how to synthesise differing regional interpretations of threat? Chatham House replied that this can be done by different organisations and in building the capacity of states.

- Derechos Digitales noted the exploitation of vulnerabilities as a threat for OEWG consideration.

- Chatham House described the negative impact of malicious ICT use on the digital economy, including economic and intellectual property loss, employment disruption, reputational damage, and the undermining of trust.

- Trend Micro highlighted that many threats are "email borne", such as phishing, malware, and ransomware, and are increasingly sophisticated. Many incidents take advantage of loose security standards and general trust among colleagues. The Republic of Korea (ROK) described spear-phishing email operations targeting government officers. The Cyber Security Experts Association of Nigeria (CSEAN) said that phishing has grown 65 per cent in the last year.

- Access Now identified the growth and use of malware as a threat that undermines human rights.

- Access Now pointed out the threat of internet shut-downs. APC noted these are more severe for marginalised groups, as are data breaches.

- The threats from data breaches and leakages was highlighted by the Institute of Computing Innovation. It indicated that the issue will only grow more challenging in future. The R Street Institute stated that a lack of data sharing is an overall threat, and that unjustified data localisation should be condemned.

- Beijing Normal University identified the threats posed to critical infrastructure (CI). ICT4Peace referenced its call to governments to ensure publicly that they will respect emerging norm that critical infrastructure should be prohibited from being a target of any cyber operation. The Commonwealth Telecommunications Organisation (CTO) said that the lack of financial investment in CI as well as disparities between states' capacities and strengths are a challenge, as well as problems in classifying CI and a

lack of technical understanding about the interdependencies between CI.

- Citizen Lab highlighted the threat from commercial surveillance and spyware, noting these often target civil society actors like journalists, scientists, and anti-corruption activists, who lack the resources to defend themselves. It urged accountability norms for commercial spyware.

- Access Now warned against weakening freedom of speech or access to information in the process of responding to global security threats.

- Health Tech & Society, and Luftbrücke Irak pointed to misinformation campaigns as a threat. The Health and Tech Society cited examples from Brazil and in the area of public health.

- INTERPOL noted that malware now more often targets mobile devices instead of computers, especially payment platforms. It also stressed the dangers of botnet, ransomware, and phishing campaigns targeting crypto-currency. The ROK echoed similar concerns about cryptocurrency hacking.

- Jordan encouraged more attention be paid to cyber terrorism by the OEWG. Chatham House noted that non-state actors, such as criminals, put livelihoods at risk but that the discussion is largely state-focused.

- WILPF expressed concern at the normalisation of using ICTs as a medium of or tool for violence and the militarisation of cyberspace. Health Tech & Society noted that cyberspace is being weaponised by using the same sources used to connect people worldwide. The Australian Strategic Policy Institute (ASPI) said it is important that as more states develop military ICT capabilities there is a corresponding need for transparency.

- WILPF raised the vulnerability of existing weapons and their systems to digital attack or misuse, including nuclear weapons, armed drones, and small arms production, marking, and tracing activities, as well as how networks aid in trafficking.

- ICT4Peace asked states in the room to comment on if cyber operations have become more precise and targeted, or more indiscriminate, in their design and impact? The CyberPeace Institute responded that it has observed a decline in the overall volume of malware attacks and improvement in targeting.

- APC said it is critical to ensure a gender perspective in discussions of international cyber security. Luftbrücke Irak encouraged building the online resilience of women. CS2 encouraged the role of women working in this field.

- Beijing Normal University encouraged changing the framework to address threats and using international legal instruments. WILPF encouraged not focusing restrictions on technology or tactics, which are ever-changing, but instead on constraining behaviour. CyberPeace Institute urged new frameworks focusing on closing the accountability gap in cyber space. It noted the shortcomings of norms and regulations. ICT4Peace said there is a need to "act early and intensely" to promote norms. The World Economic Forum (WEF) emphasised that one of the most vital risks the international community faces is the breakdown of trust, norms, and responsibilities. It encouraged prioritising rebuilding trust. The CS2 Initiative said that a constructive attitude is essential for success. The CTO observed that political will to find solutions is missing. The Global Forum on Cyber Expertise (GFCE) noted that not enough outreach has been done to promote agreed norms with those who would implement them.

- Access Now encouraged clarifying the objectives of the OEWG. The CS2 Initiative noted that the next Internet users will primarily come from the global south, many of which will be women and youth. These will have to live with the norms that the OEWG sets.

- Jordan suggested compiling a list of the risks identified in this session, noting that without understanding the risks it is difficult to define rules and norms.

Rules, laws, and norms: how can stakeholders support government?

- In its scene-setting remarks, Temple University said that the UN cyber norms (as outlined in the reports of the Groups of Governmental Experts) don't bind states but do set a social standard of shared expectations. It explained that the problem is in the application of these rules, and that their application requires assessment; interpretation of key concepts, like CI; and also incentive to implement. It emphasised the roles for non-governmental actors in all these aspects.

- The Oxford Institute for Law, Ethics and Armed Conflict encouraged more states to share their views on norms and rules applicable to cyber space, noting that a lack of transparency is a barrier to its research. France and Australia agreed with this and pointed to the sharing of their respective strategies.

- Chatham House and EU Cyber Direct reminded that while states have agreed that international law and the UN Charter apply to their activity in cyber space, states have not reached agreement on how it applies. R Street Institute encouraged keeping legal debates separate from the OEWG mandate.

- ICT4Peace Foundation stated that while all UN cyber norms are worthy, the one prohibiting operations against CI is particularly important. It noted that despite this norm having been adopted more than four years ago, state-conducted cyber operations targeting CI occur. APC expressed support for the cyber norms, especially that relating to protecting the public core of the internet. GPD encouraged moving to operationalisation of the norms, noting that they will only have an effect when they are implemented.

- FIRST described it work in raising awareness about the UN cyber norms with computer emergency response teams (CERTs) especially the norm against conducting operations against another states' CERT. It emphasised better partnership and inclusion in the design phase, noting that many CERTS are unaware of the UN norms. Igarape Institute highlighted the gap that exists between policymakers and the technical community in relation to the UN cyber norms, despite the technical community being at the centre of norm implementation. ASPI announced it is building a curriculum on implementation of 2015 UN GGE report to help fill gaps.

- Research ICT Africa noted that the UN cyber norms were developed in a "top down" approach and are not grounded in African perspectives or considering differing levels of technological development which impacts how well they can be implemented.

- In its scene-setting remarks, the International Committee of the Red Cross (ICRC) stated that any discussion on fostering a rules-based cyberspace should be built on the understanding that international law applies. It urged all states to affirm that international humanitarian law (IHL) applies to cyber operations during armed conflict, but that doing so does not legitimise cyber warfare—it merely places constraints on belligerents.

- R Street Institute said that a new cyber convention could be useful in future as an important source of international law, but that the OEWG should focus on how stakeholders can assist states. Trend Micro referred to its Project 2020 which had envisioned the creation of an international cyber court. While this has not happened, it still sees value in the premise. Australia and MAFINDO expressed interest in this idea.

- The ICRC said it has no strong view on the need for a new convention but that having views expressed on the applicability of existing law can help to identify if new law is needed.

- ICT4Peace Foundation suggested that OEWG states consider a possible ban on cyber operations against nuclear facilitates.

- EU Cyber Direct highlighted the risks of differing national interpretations of existing norms and law and encouraged more states to share interpretations publicly.

- IPANDETEC noted that only Panama and Costa Rica have joined the Budapest Convention and encouraged more commitment from Central American countries and better cyber awareness in the region.

- DXC Technology reminded states that technology is not standing still while their work is being done and that the context and realities in which norms and rules being discussed now will apply later could be very different. Australia noted it takes a "technology neutral" approach in order to try and keep pace with new developments.

- Chatham House observed that most cyber conflict between states is of low intensity, which has certain legal implications for reponse.

- The CyberPeace Institute outlined concern over new vectors of attack, including cryptocurrency and blockchain, and encouraged reporting on existing vulnerabilities as "crucial". This was echoed by the Tech and Law, Africa CERT, and the Cybersecurity Tech Accord, which further recommended the adoption of vulnerability equity policies and processes. Trend Micro outlined its work with vendors in the handling of vulnerabilities and pointed out that one of the greatest challenges in this area is that governments are one of the largest consumers of vulnerabilities from black and grey markets.

- APC outlined the roles for civil society in shaping and implementing norms, including building the capacity of stakeholders; monitoring compliance; and awareness-raising. These points were echoed and expanded on by Tech and Law, and GPD, who also described the work of CERT coordination and building understanding on how the norms impact human rights. The Technological Institute at the University of Singapore emphasised how engaging more stakeholders was beneficial in the development of its cyber security bill. DXC Technology encouraged the private sector to partner more with academia and civil society and that the UN could learn more from these stakeholders, and vice-versa.

- In its scene-setting remarks, the Center for Technology and Society at Fundacao Getulio Vargas Law School focused on the threats posed by terrorist organisations in using social media platforms and called for better content regulation, but to take care with distinguishing between legitimate expression. Uruguay said the right to freedom of expression is a pillar that states must recognise and promote.

- Canada announced that it will be looking more into the gender dimensions of cybersecurity.

Stakeholders' commitments to rules, norms and principles: Tech Accord, Charter of Trust, Global Transparency Initiative, Paris Call and beyond

- The IGF Best Practices Forum on Cybersecurity, Microsoft Corporation, France, ICT4Peace, Global Cyber Alliance, GFCE, WEF, Ecuador, and Australia, among others commended the Paris Call, the Tech Accord, and the Charter of Trust for acting as a first step in operationalising the UN norms and rules in cyberspace, and building trust and confidence among states, the private sector, public sector, and civil society.

- Microsoft and France in respective scene-setting remarks noted that the Paris Call is the world's largest multi-stakeholder initiative as it is endorsed by more than 1,000 entities. Microsoft noted that the Call creates multi-stakeholder communities of action and will only be strengthened through partnership with the UN.

- ICT4Peace reminded that while there is an impressive number of stakeholders committed to the Call, some leading states are absent. It noted that unless those states "get on board" the effectiveness of the Call will remain an open question.

- The question of whether cyberspace norms and rules should be legally binding or voluntary was brought up by many participants. Egypt, Pakistan, Argentina, Microsoft Corporation, Huawei Technologies USA, the Philippines, and Ecuador spoke in favour of binding norms or mechanisms.

- Igarape Institute, among others, urged focus on implementing already agreed norms. It noted that multiple norm building efforts do not necessarily lead to duplication but can lead to greater consensus. It stressed identifying what best pratices are already in place while also looking for new avenues.

- Egypt remained committed to establishing legally binding norms and rules for cyberspace, for which it sees a "growing consensus". It noted that it is "very difficult for states to rely on voluntary recommendations to prohibit certain behaviour" and seldom do voluntary norms work in the context of international security issues.

- Egypt also said that voluntary and binding norms are not mutually exclusive and should be pursued in tandem as they can strengthen one another. Argentina, Access Now, APC, Huawei Technologies USA, and the Philippines made similar acknowledgements.

- Argentina said that the best way to prevent malicious acts using information and communication technologies (ICTs) is to have a consensus on binding and non-binding norms. APC warned stakeholders to avoid packing all issues into one negotiation process, and suggested defining areas where binding norms make sense and where voluntary norms make sense. Huawei Technologies USA said that while legally binding norms are an imperative, states need to first focus on implementing already existing norms, reminding states that they do not have the luxury of spending years discussing legally binding norms.

- The Philippines stated that a legally binding instrument "could provide the teeth and a stronger mechanism to facilitate implementation of the agreed norms." It also noted that states need to address how a legally binding instrument on behaviour in cyberspace would address state sovereignty and existing domestic laws.

- Argentina urged having consensus on binding and non-binding norms, suggesting that twin tracks are the best way to prevent malicious acts. The University of Hong Kong asked why having separate paths is perceived as a bad thing, and highlighted benefits of parallel processes.

- Australia noted that states created legally binding obligations in cyberspace when they agreed that international law and the UN charter apply in cyberspace. It further argued that the 2015 GGE norms are the only ones that have been endorsed by every country and warned that negotiating a legally binding convention or instrument would give states the opportunity to pick and choose which components of international law they believe should apply in cyber space.

- Canada added that negotiating a legally binding instrument would be time consuming and distract states from the more important matter of operationalising the already existing norms outlined in the 2015 GGE report. R Street Institute supported this view. GFCE told states and stakeholders not to underestimate the power of voluntary norms, saying that even with voluntary non-binding norms, it is still possible to take collective action to enforce those norms if they are broken or violated.

- ICT4Peace reminded participants that one of the UN GGE norms flags the necessity for attribution accountability for the malicious use of ICTs. It further said that if this norm is to be implemented, it will require a reliable attribution mechanism—suggesting a peer-review process similar to Universal Periodic Review.

- Many participants expressed concern over the gaps in knowledge and understanding of the norms, rules, and principles surrounding cyberspace between developed and developing countries. Many civil society organisations recognised this gap and suggested that their work can help bridge it by providing education, training, and assistance to states that lack awareness on existing norms and rules in cyberspace. Those that addressed this were CAPA 8 Foundation, Jordan, and Igarape Institute.

- GFCE brought attention to another gap of knowledge that exists between the people present at these OEWG and cyber security meetings, and heads of state and higher-level officials. The Organization of American States (OAS) highlighted the importance of including gender perspectives as well as participation in these kinds of meetings as well as in all issues related to international cybersecurity.

- Central European University said that cyberspace is place of norm contestation. It

said that the OEWG can be a good space to achieve cyber norm legitimacy by giving equal access to norm contestation by all member states.

- ASPI noted that internet technical communities are less represented in the OEWG intersessional.

Confidence-building between states and between states and the private sector

- All speakers called for greater cooperation between states and the private sector as well as between states and civil society. Many underscored that these partnerships create confidence, trust, and communication all of which are essential in maintaining a free, open, and secure cyberspace.

- ICT4Peace suggested that the OEWG dedicate some of its proceedings to learning from regional groups and the specific measures they are implementing in order to increase confidence and capacity.

- Huawei Technologies USA said it is important to test products for vulnerabilities and share those vulnerabilities with each other.

- The Institute of Strategic and International Studies Malaysia identified international CBMs which are focused on strong communications channels, and domestic ones such as improving cyber hygiene.

- The University of Waterloo and R Street Institute resisted two-tier encryption, backdoor channels, and golden keys arguing that they undermine confidence between users and within the ICT environment. They further noted the importance of data integrity and transparency.

- The Azure Forum spoke to the threats of quantum computing and autonomous cyber weapons and that there are increasing levels of autonomy being used in defensive measures. It urged that these unique attributes be accounted for in confidence building measures.

- FIRST highlighted that incident response requires trust. It urged making interactions with incident responders more predictable and reliable.

- Strathmore Law School and Access Now both pointed out that informal and inclusive meetings such as this intersessional are in itself a confidence building measure by bringing in widespread participation, expertise, and cooperation among states, civil society, the private sector, and the public sector. The Cybersecurity Tech Accord echoed this, noting that as international tensions move from the conventional domain to the cyber domain, efforts to build trust will equally have to adapt.

- R Street Institute proposed creating an independent body with the structure of the International Atomic Energy Agency (IAEA) responsible for risk reduction in cyberspace. This "cyber IAEA" would not act as a court but would facilitate and give statute reports to the UN General Assembly on states' activities in cyberspace. ICT4Peace asked for further elaboration on this suggestion and noted that the IAEA is connected to the implementation of a treaty.

- ASPI proposed maintaining a list of all reported cyber incidents to improve transparency in cyberspace. This kind of transparency will help build capacity and trust between states and ensure that policy leaders are aware of what is actually happening in cyberspace.

- The CyberGreen Institute proposed publishing cyber risk indicators similar to those that the World Health Organization publishes. This would be a way to promote and assess internet health. They suggested creating scorecards for each nation based on the data attained in order to see where capacity building efforts need to be improved.

- Ecuador urged states and stakeholders to take a multidisciplinary approach to capacity building that includes international gendered approaches; that consider the differentiated impact of cyber attacks on certain groups; and consider greater inclusiveness for people with disabilities in the area of capacity building.

Engaging all stakeholders to enhance capacity-building efforts

- ASPI proposed creating a core team of experts that would act as an international advisory team providing technical assistance. It stressed the importance of this group being independent of donor preferences. Egypt commended ASPI for this proposal and said it is a suggestion that the OEWG can consider.

- FIRST suggested making interactions with incident responders more predictable and reliable, noting that effective incident response requires trust. It also pointed out that sanctions and export restrictions can seriously hamper information sharing ability between states, particularly with regard to CERTs' ability to share and report information internationally about an attack.

- Trend Micro suggested improving diversity in the field of cyber security to enhance capacity building. This diversity should come in the form not only of gender diversity, but also diversity of professional backgrounds. It argued that having cyber security experts from different professional and personal backgrounds brings different perspectives to cyber security issues, raises awareness, and can help create trust and confidence among states, civil society, the private sector, and the public sector.

- The University of Waterloo and R Street Institute suggested states and civil society ask the question "what kind of ICT infrastructure is required so that these discussions on confidence building and capacity building can exist in the first place?"

- The Center for Technology and Society and R Street Institute identified that not knowing who to contact or reach out to for cyber security training is an obstacle to capacity building. The GFCE noted that if countries "know what they need and don't have the available resources, they need to know where to look."

- Egypt pointed out that "one size does not fit all" and careful assessment of each country's capacity building needs and current cyber security situation is essential. It also recognised the importance of reporting—which can increase implementation but also help identify gaps where states have challenges thereby identifying where capacity building efforts are most needed. The CyberPeace Institute recognised the importance of reporting but noted that states need to determine what they want to measure and report on to make these reports most effective.

- APC noted that cyber security touches on many other areas of governance therefore cooperation is key. It further said that there is often an underrepresentation of gender in cyber and internet governance. The relationship between gender, internet governance, and international security needs to be taken into consideration and addressed when engaging all stakeholders.

- Australia suggested developing a best practices guide on capacity building so that states can learn from one another. It further noted that capacity building is a two-way street, better coordination is required, and it is necessary to consider how to move capacity building from a codified industry to a professional service.

- Hiperderecho pointed out that it is equally crucial to train rural communities in cyber security as they tend to be more vulnerable groups. It argued that by not training these communities, they become the weaker links in local and global environments therefore weakening cyber security as a whole. They proposed aligning cyber security programs with digital inclusion programs.

- Ecuador, Argentina, the OAS, and Luftbrucke Irak made references to the important role that training and education can play in both capacity building and engaging all stakeholders in the process. Ecuador called for a nexus between scientific literacy and diplomacy, suggesting that private sector and academics can play a key role in educating diplomats and the general population on cyber security issues.

- Luftbrucke Irak said that education, training, and awareness creates informed citizens which enhances cyber resilience. They also called for human expertise at the regional and national level, and asked states to enable

local practitioners to provide expertise. It said this will increase efficiency, confidence, and capacity between states.

- Argentina said that all stakeholders need to be involved in capacity building efforts. They noted the importance of effective training and said states need to take a long-term approach to cyber security. It highlighted that a main challenge is institutionalising the dialogue with all national sectors so that they can contribute to all aspects of training and use the same terminology and definitions.

- The OAS outlined its practice of hosting seminars, conferences, workshops, and providing a base of information in cyber security to diplomats and all relevant stakeholders. It also highlighted their gender-based approach and emphasised the need to increase gender diversity and take a gendered perspective to cyber security.

- Universidad Nacional Autonoma de Mexico noted that everyone in the discussion, stakeholders and states alike, provide broader understanding of cyberspace, therefore it is essential that coordination exist among various stakeholders. It stated that part of a government's work is to listen to all stakeholders and take their views under consideration.

- The CTO reminded participants that every state has unique cyber security strengths and weaknesses therefore it is essential to analyse and identify these individual strengths and weaknesses. It suggested the best way to develop this is through a national cyber security capacity review. It also stressed the importance of political will in achieving and kind of capacity building effort. CAPA 8 Foundation agreed and added that it is important to ensure that the new generation has room for growth in this sector both domestically and internationally.

Conclusion: Ways forward on a multi-stakeholder approach

- Virtually all speakers commended the fact that this intersessional meeting allowed the voices of diverse actors to be heard.

- In its scene-setting remarks, WILPF set out several practical suggestions for ways to improve multi-stakeholder approaches in future meetings as well as encouraged exploring avenues for remote participation and nation multi-stakeholder dialogue.

- WILPF spoke of the "elephant in the room" in reference to the denial of accreditation to non-ECOSOC organisations at the OEWG's September session and noted that is an obstacle to multi-stakeholderism in the process. Australia and Germany said that future meetings should not exclude those groups. Derechos Digitales hoped that this open meeting would be a starting point for continued multi-stakeholder approaches.

- In its scene-setting remarks, the EU's Cyber Direct programme emphasised three points for multi-stakeholderism going forward: bring people and their concerns into the conversation; protect the core of multi-stakeholder approach; and that multi-stakeholder engagement is an investment in the future.

- The Center for Strategic and International Studies Indonesia, in its scene-setting remarks, offered four suggestions going forward including through diversifying inputs and establishing synergies with other processes. It supported an earlier suggestion to have a registry to share outcomes from meetings on cyber security and best practices.

- Iran commented that the possible framing questions and scene-setting should have been arranged in collaboration with all member states. It reminded that states bear the responsibility for security in cyberspace. It urged an objective report from this meeting that shows where this convergence and divergence of views.

- Ireland, the EU, the United Kingdom (UK), Uruguay, and Malaysia all expressed the desire for broader participation from stakeholders. Ireland said that inclusion of all stakeholders will help bridge the digital divide. Malaysia said that cyber threats are rapidly evolving and becoming sophisticated so it is "crucial for us all to elaborate on this process in the UN and work together to produce

significant outcomes." It also reiterated CTO's earlier point about having the necessary political will.

- Ecuador spoke against the militarisation of cyberspace. It highlighted the need for transparency and proportionality. It also recognised that the Women, Peace and Security Agenda could be incorporated into cyber security strategies and policies.
- The Telenor Group stressed protecting human rights in cyber space.
- Brazil encouraged states to find ways to allow non-governmental stakeholders to participate in the decision-making process. It noted that the OEWG mandate includes reference to "regular institutional dialogue" with "broad participation".
- GPD gave examples of how some states, like Australia and the UK, are consulting with non-governmental stakeholders in developing national strategies.
- Access Now urged states to take a human-centric approach to cyber security, saying that there is "incredible infrastructure in place, and it is on us to leverage this infrastructure effectively."

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. 05
9 December 2019

Editor: Allison Pytlak
disarm@wilpf.org