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.10

17 March 2021

Photo: Lucian Alexe | Unsplash

IN THIS ISSUE

Reaching Critical Will

www.reachingcriticalwill.org

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

www.wilpf.org

A WIN FOR DIPLOMACY—QUESTIONS REMAIN FOR CYBER PEACE

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

Applause rang out across multiple conference rooms of the United Nations (UN) headquarters in New York on Friday,12 March, possibly one of few times in many months that this had happened. The source of celebration was the consensus adoption of a final report by the UN's first-ever Open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security (a.k.a. international cyber security).

What made the applause rare was not just the many months of the COVID-19 pandemic, which first shuttered the UN and now has dramatically reduced the number of in-person meetings occurring there—but also a highly challenging global political landscape that has strained disarmament diplomacy and multilateralism to the brink. It was in this same building that, in 2018, UN member states were unable to agree on establishing a single UN process on international cyber security and amid politicisation and acrimony, voted to establish two concurrent and somewhat overlapping processes, to the frustration and disbelief of many.[1] And just last year, member states disagreed over how to best take forward work on cyber issues in before the current round of talks had finished their work.

The adoption by the OEWG of a final report by consensus is being commended by many participants as a significant milestone and accomplishment. Virtually all states acknowledge that the final product is not perfect and reflects much compromise and balance. Yet, it's evident that they are proud of having found ways to achieve that balance despite many uncertain moments, divergent views, and the challenges of pandemic-era negotiating in which meetings took place in virtual and hybrid formats, with delegates joining meetings in the middle of the night from wherever they are based. As Liechtenstein noted in its explanation of position, "If we are in a position to [agree consensus] today that is primarily to the credit of the Chairperson's unwavering commitment to bringing our fruitful discussions to a substantive conclusion, against the difficult odds of a pandemic, a heavily polarized political landscape and serious limitations in the intergovernmental mandate."

Achieving a substantive outcome was particularly important for many states, given that this was the first-ever UN body to debate matters of international cyber security that was open to any and all interested member states. Earlier UN Groups of Government Experts (GGEs) were limited in number and their deliberations closed. The OEWG was also somewhat inclusive of civil society. Numerous delegations stressed in their closing remarks that it was important for their countries to have been able to participate in these discussions for the first time.

How consensus was forged

Earlier in the session, achievement of a substantive final report felt unlikely. Prior versions of the final report consisted of four sections: Introduction; Conclusions and recommendations (which was meant to be the only part open for negotiation); Discussions (meant to reflect where there was not agreement and the spectrum of views); and Final observations.

By Wednesday, it was clear that states were unhappy with various sections of the draft report and that elements of it were hitting their various red lines. Russia, with support from other states, suggested moving the Discussions part of the report into a Chair's Summary, which would be annexed to the final report but would not subject to approval and adoption by member states. That left a shortened and simplified version of the report up for negotiation in the little time remaining.

The version of the report that was ultimately adopted on Friday was distributed late Wednesday night. By our analysis, some of the key modifications meant to address the more

significant concerns of states are outlined in a separate article on page 6.

Measuring success

Whether the changes made to the final report are "good" or not depends on what one's positions are.

In their closing remarks on Friday, many states strongly emphasised the significance of the OEWG report affirming the *acquis*, which is the term that has come to refer to the collective outcomes of the UN's GGEs on responsible state behaviour in cyber space; in particular, the three Groups that issued consensus reports in 2010, 2013, and 2015. Those reports were later adopted by the UN General Assembly, which means that the entire UN membership has endorsed them, but without all member states having directly participated in developing the content of the reports. "While in the past the affirmation was indirect, in the form of General Assembly resolutions adopted by consensus endorsing GGE reports, this time, the affirmation by all the UN Members is direct," Japan stated.

A core component of the *acquis* is the affirmation that international law applies to cyberspace. This reaffirmation was widely welcomed, albeit with regret from many that it was more of a blanket statement and that the report does not have greater specificity about which laws, and how, such as appeared in earlier versions of the draft report and in the discussions of the OEWG. Another important component are the 11 norms for state behaviour in cyberspace, articulated in the 2015 report.

What became evident through this OEWG is that despite the UNGA having adopted the GGE's reports, not all states stand strongly behind the *acquis*. Some, like Iran and Cuba, pointed out repeatedly that as they had not participated in the GGEs, they do not feel ownership of nor can they endorse the GGE's findings. Some of these countries are also the strongest proponents of the development of new norms, legal frameworks, and/or instruments.

The loss of a reference to IHL is a significant concession to China, Cuba, Venezuela, and others who are staunchly against IHL applicability. These and other countries have stated that the applicability of IHL to cyber space and action therein would militarise the domain. These countries appear to be in the minority but were firm on this being a red line—removing the IHL reference looks to be among the cost of achieving a consensus report. Many of these same states were also vocal about adding in references to ICT development for military capabilities and calling more strongly for restraint, which were included.

Many of the countries opposing IHL applicability tend to also be encouraging of a future legally binding instrument or framework, along with other countries like Ecuador and Costa Rica who do support IHL applicability. The explicit mention in paragraph 80 of "possible legally binding obligations" may be a "win" for legal instrument supporters. Yet opponents of a legal instrument, including the United States, European Union countries, Israel, and Australia, among others, can also "claim victory". For these countries, the reaffirmation of the *acquis* and existing norms was a high priority. Since the first OEWG session in 2019, "not starting from scratch" has become something of a mantra for them.

At the same time, many of these states would have liked for the OEWG to have made more progress in clearly defining how and which legal principles are or should be applied to state behaviour in cyber space. Earlier versions of the report had outlined this in greater specificity than the final version did. Several countries, including the Nordic countries, the Netherlands, Germany, Austria, Slovenia, Argentina, and Chile, among others, regretted the lack of reference to human rights and/or international human rights law.

Iran had been one of the largest "unknowns" with respect to whether it would accept the adoption of the report or not. Ultimately it did not block consensus (again, because consensus in the UN is taken as unanimity), but it did choose to disassociate itself from "parts of the report that do not match with its principles and positions". Israel also disassociated itself from any reference to the need for a legally binding instrument.

Quite a few delegations welcomed the sub-sections on confidence- and capacity-building measures (CBMs). There were more critiques of these sections from non-governmental stakeholders, many of whom are already engaged in some of this work practically, as are regional organisations, and are rightfully keen to avoid duplication. An important component of the sub-section on capacity-building are the principles that have been outlined to guide this work, in ways that would include legal and policy capacity, alongside technical support and a "two-way street" approach. Throughout the OEWG process many states expressed hope that agreement of guiding principles for cyber capacity-building would facilitate a narrowing of the global digital divide.

All states acknowledged that their respective "wish lists", in the words of the Netherlands, were not accommodated, and some, like Canada and Australia, used the word "uncomfortable" to describe how they felt about certain elements of the report. Yet, from listening to closing statements on Friday, the overwhelming feeling was positive—more positive than one would have expected, given the politicised origins of the OEWG's establishment. "Diplomacy works, and multilateralism matters," stated the OEWG's Chairperson, Ambassador Lauber of Switzerland.

Many participants expressed that what was most significant for them was the openness, inclusivity, and transparency of the process, which was viewed as an historic "first" for this topic within the UN—but did not always extend to civil society, as we'll cover later. Several noted that the OEWG has helped to build confidence and understanding among all member states on this urgent and very transnational issue.

"After all, this OEWG is unprecedented. This is the first time that all UN Member States are deliberating and negotiating together in the same room, physically and virtually," observed the representative of Malaysia. "My delegation has benefited tremendously from the opportunity to better understand various issues on ICTs and the underlying nuances, by listening directly to the clear articulations of positions and arguments by distinguished delegates."

From adoption to implementation

Of course, a report in itself does not equal meaningful change. "Ultimately, success depends not on the report but on our collective determination to implement the commitments made today," noted the representative of the Czech Republic in closing remarks.

We agree. Adopting a report by consensus is a win for multilateralism and diplomacy, but it brings with it commitments that need to be actioned outside the halls of the UN.

There are tangible recommendations contained in the report that may fall short of the accountability many of us had hoped the OEWG would produce, but would aid in building transparency through information sharing—if they are implemented. For instance, all of the recommendations for states to voluntarily submit information toward the annual UNSG's report is a way to build public understanding about how states are implementing norms or undertaking capacity-building, as well as about how states apply and interpret international law to their use of ICTs. Sharing information about national CBMs with the UN Institute for Disarmament Research (UNIDIR) for its Cyber Policy Portal would likewise help with transparency and build trust.

Beneath these tangibles, however, it should not be overlooked that the report draws directly from the *acquis* in some of its recommendations to states in ways that clearly set out the do's and don'ts of cyber behaviour. For example, paragraph 31 reminds that, "States should not conduct or knowingly support ICT activity contrary to their obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public," which is one of 2015 GGE norms.

Or, while the language on non-use of proxies may have been relegated to the Chair's Summary of the report, the 2013 GGE report states clearly that "States must not use proxies to commit internationally wrongful acts. States should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs." If the

acquis is being affirmed by the OEWG, then this recommendation should hold, too.

Yet, we know that states are using proxy actors, with increasing sophistication and regularity, and that critical infrastructure of various types is being targeted by state-led cyber operations. Which means that bigger and bolder action to stop hostile and aggressive state use of ICTs is needed. This is part of the reason why some states call for a legally binding instrument and why others, and civil society groups, have outlined various accountability mechanisms and frameworks throughout the OEWG process—none of which were ultimately adopted.

In this regard, the statement in paragraph 24 that notes, "In accordance with General Assembly resolution 70/237, and acknowledging General Assembly resolution 73/27 States were called upon to avoid and refrain from use of ICTs not in line with the norms for responsible State behaviour," is welcomed. However, it is a step backward from an earlier version of the final report, in which states were "called upon to avoid and refrain from taking any measures not in accordance with the Charter of the United Nations and international law."

Likewise, it's positive that the report acknowledges that "a number of States are developing ICT capabilities for military purposes"—which was salvaged from the Discussions section and now forms a Conclusion—but merely recalling this fact will do little to stop states from developing such capabilities. Little by little, cyber space will become more militarised and technology more weaponised. The metaphor of a "cyber arms race" can be problematic and is somewhat inaccurate, but it does aptly capture the inherent desire that some governments have for strategic superiority and power, which inevitably leads to violence and weapons proliferation.

A forked road ahead

The language of the final report may have neatly reconciled the different visions about the best ways forward for regular UN dialogue on cyber security, but how that plays out in the real world remains to be seen.

The ongoing sixth GGE will conclude its work within the next few months. It's not possible for this publication to comment on how its closed deliberations are progressing or what outcomes it may produce, but we can attest to the very strong emphasis that was been placed on the sixth GGE and first OEWG reaching complementary outcomes, back when the two bodies were established in 2018.

Given that more than 50 member states now support the proposal for a cyber PoA, it would not be surprising if a negotiating mandate is sought at the 76th session of the UN General Assembly's First Committee in 2021.

Meanwhile, the second OEWG will likely commence work in the next few months; current rumours are that it will have an organising meeting in June in order to set its schedule and participation modalities for the five years ahead. Ideally, it should build on and further develop what was agreed to in this first OEWG—and measure progress of outcomes—but remarks delivered from some delegations on Friday made it clear that they have a few specific goals in mind, such as the elaboration of legal obligations, which may not sit right with the full UN membership.

Moreover, while member states may have compromised on core issues like IHL applicability in this round, they may not do so again in future. "In light of the agreed Conclusions on the development of ICT capabilities for military purposes and their potential humanitarian impact, the ICRC believes that discussions on how international humanitarian law limits the use of ICT capabilities during armed conflict need to continue," observed the International Committee of the Red Cross (ICRC). "We believe that the Chair's Summary presents important milestones in this regard and can be built on, in particular in any future processes for regular institutional dialogue under the auspices of the United Nations."

The language of this first OEWG's report gives space for more discussion and elaboration about the cyber PoA proposal during the second OEWG, but eventually it will need to break off into its own process. Not all states may engage in both. South Africa expressed concern about capacity of some

states to be engaged in multiple processes; while Liechtenstein observed the inherent constraints of the OEWG format and decision-making modalities:

> The discrepancy between the content of the intergovernmental discussions and the substantive results of the Open-ended Working Group does not reflect a lack of effort. It is rooted in the format of this process and its decision-making modalities which favor containment over progress and minority restraint over majority aspiration. Unfortunately, the intergovernmental mandate for the next iteration of the Open-ended Working Group is even more affected by these flaws, pointing to the conclusion that the process in this form may have outlived its purpose.

Across these various fora, the future of civil society engagement must improve. The exclusion of non-ECOSOC accredited organisations from this OEWG prevented stakeholders with established relevant expertise from joining in formal meetings. While this cultivated innovative collaborations between civil society and supportive members states in organising consultations and input opportunities, this cannot become standard practice. Civil society groups and other stakeholders have had to defend time and again our role in implementing the outcomes that these bodies agree to, or our representation of affected communities, and should therefore have a seat at the table when cyber "rules of the road" are being further developed. The OEWG final report recognised the contributions of other stakeholders in the process, but many governments said in their closing remarks that this could have been stronger and should be improved in the future.

The human cost and humanitarian impact of cyber operations can at times feel like an abstract problem, when juxtaposed with the daily harms caused by bombs, mortars, and guns. While not yet as severe or rampant a problem as posed by those weapons, this is precisely why the international community needs to mobilise for cyber peace and stand up to the weaponisation of ICTs. There is a rare opportunity to be preventive and stop the spread of ICT misuse and the militarisation of cyber space.

As a feminist organisation, WILPF views the militarisation of cyber space as an expansion of the patriarchal structures of power that perpetuate violence and repression. This not only overlooks systemic and root causes of violence but sets out to exacerbate and create violence in a new medium where it does not necessarily otherwise occur.

It's evident that some member states want action-oriented outcomes and strong solutions to the ubiquitous cyber threats we collectively face. It's equally evident that others are taking advantage of the painstakingly slow pace of diplomacy. At a time when hostile cyber operations are on the rise and becoming ever more integrated into the regular military activities of a growing number of states, the need for cooperation and bold action toward cyber peace has never felt greater.

NOTES

1. During the 73rd session of the UN General Assembly (UNGA) First Committee in 2018, states established the OEWG via resolution 73/27 and a sixth Group of Governmental Experts (GGE) on Responsible state behaviour in cyber space, via resolution 73/266.

OVERVIEW OF CHANGES MADE TO THE "FIRST DRAFT" OF THE OEWG FINAL REPORT

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

Below is a non-exhaustive overview of changes made to the "first draft" of the OEWG substantive report, versus the final version as adopted.

- The Discussions section was moved into a Chair's Summary and is annexed to the Final Report. This means that the only reference to the applicability of international humanitarian law (IHL) to cyber space and state use of information and communications technology (ICTs) was removed from the negotiated part of the document.
- The sub-sections on Rules, Norms, and Principles and International Law were reversed, so that norms precede law.
- References to UN fora that address other aspects of cyber security such as cyber crime, Internet governance, or human rights, are no longer named specifically.
- An indirect reference to the current GGE was included in paragraph 7 by naming resolution 73/266, which established it, but there is no other recognition.
- References to the concerns expressed about the development of ICT capabilities for purposes that undermine peace and security, and for military purposes, were inserted. These were important to many countries in the Non-Aligned Movement.
- The reference to the potentially devastating humanitarian consequences of malicious ICT activities on critical infrastructure (CI) was retained, along with a reference to security, economic, and social costs.
- The final draft allows for states to decide for themselves what constitutes CI, but provides several examples, including some new services suggested by states earlier in the week. This includes medical facilities, and there continues to be a reference to how the COVID-19 pandemic has "accentuated the importance of protecting healthcare infrastructure."
- The reference to a human-centric approach to cyber security was retained, but some references to the protection of human rights and fundamental freedoms were lost in the course of removing an earlier paragraph that had listed specific principles of the UN Charter seen as relevant and applicable.
- A few states had asked to see the applicability of the UN Charter "in its entirety" affirmed but this was not included.
- Requests to see the right to self-defence were not included and remained in the Discussions section.
- The concept of "tech neutrality" was described, but not named as such.
- New language was introduced, taken from the 2015 GGE report, stating explicitly that, "States were called upon to avoid and refrain from use of ICTs not in line with the norms for responsible State behaviour."
- Calls to include references to supply chain security, and vulnerability stockpiling, were brought from the Discussions section into the Conclusions and Recommendations section, and therefore are part of the adopted report.
- Concerns expressed about reflecting differently relevant UNGA resolutions that were adopted by consensus, versus those adopted by vote, were taken on board.
- In response to opposition to the recommendation that states nominate a national point of contact for confidence-building purposes, the final version recommends states to "consider nominating a point of contact".
- Encouragements to voluntarily submit views to the UN Secretary-General for his annual report on ICTs remain in four sub-sections of

the report (Norms, Law, Confidence-building Measures; Capacity-building).

- References remain to women's meaningful participation in the field of ICTs and to gender-sensitive capacity-building.
- The outcome report from the informal multi-stakeholder meeting held in December 2019 remains annexed to the OEWG's final report. The nature of stakeholder participation in the OEWG meetings is described in paragraph 10 and has been refined overtime to more accurately reflect the ways in which stakeholders have been able to engage in this process, although leaves out explicit reference to the limitations faced.
- The possibility of developing legally binding obligations, as an example of the diversity of ideas presented during the OEWG, is referenced in paragraph 80 in the Final Observations section, whereas in prior versions it was described in the context of the Discussions section.
- To reconcile very different views on if and how to reference the next OEWG and the proposal for a programme of action (PoA) on cyber security, modifications were made to the section on Regular Institutional Dialogue. The PoA proposal is described as one of among several initiatives, and it is encouraged to be "further elaborated, including at the OEWG".
- The original Annex, which is a Non-paper containing specific textual and practical proposals put forward by states during OEWG sessions, was retained and is attached to the Final Report.

WHY SHOULD GENDER MATTER (MORE) FOR THE OEWG?

Verónica Ferrari | Association for Progressive Communications

The Association for Progressive Communications (APC) has followed the Open-ended working group (OEWG) process since its inception in 2019. From the first substantive session, and together with some country delegations and WILPF, we expressed how critical it is to adopt a gender approach to discussions concerning cyber security.

Analysing the gender dimensions of cybersecurity implies asking questions about unequal power relations between genders in digital spaces, including what this means in terms of access to technologies, limitations in how we use and benefit from them, and how our online experiences are different based on our gender identity or sexual orientation, as research from APC and WILPF has pointed out.

As we know, "offline" discrimination, stereotypes, and inequality not only can be replicated in the digital realm but can also be exacerbated and take on new forms. This explains, for example, why women are disproportionately affected by violence on the Internet. A recent report from the UN Institute for Disarmament Research (UNIDIR) explains how gender norms inform cyber security, for example, with the association of technical expertise with men and masculinity, and how these activities and concepts are often valued over those associated with women and femininity.

For these reasons, and as past editions of this Monitor pointed out, gender considerations should not be "secondary" issues at the OEWG.

The OEWG adopted a final report that in its introduction highlights the participation of women delegates in the process and the importance of promoting meaningful participation and leadership of women in cyber policy-making spaces. In the same section, the report acknowledges the importance of bridging the "gender digital divide". However, despite this, discussions on these issues and what states could do about them are nearly absent across the different sections of the report.

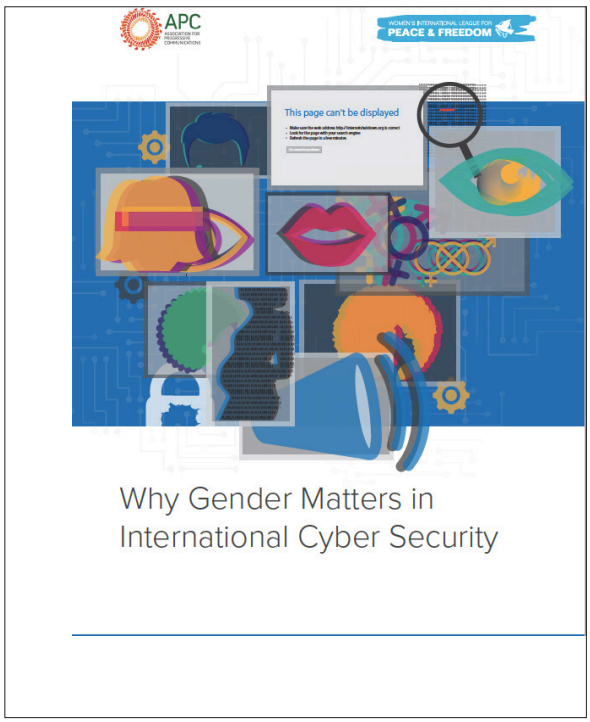
The final OEWG report mentions "gender" only three times and "women" another three. The report recognises that our experiences in cyberspace are not the same and that people in positions of marginalisation or vulnerability experience particular risks. But it could have gone further.

As we expressed in our statement during the informal multi-stakeholder segment of the third session of the OEWG, the report could have emphasised the importance of gender considerations as key to cyber threats discussions and could have offered specific recommendations to states to address this by working with relevant stakeholders. As pointed out by the UNIDIR report, disaggregated data on these differentiated impacts is still scarce and an obstacle to the development of gender-sensitive cyber security policies. Representative and gender-disaggregated data should be gathered consistently and rigorously to allow for a better understanding of the factors shaping women's access and ability to benefit from digital technologies.

Going forward, these are some of the discussions the new OEWG should consider.

The report also recommends that cyber capacity building should be gender sensitive, inclusive, and non-discriminatory. While this is an important first step, gender should be mainstreamed in the design, implementation, and evaluation of capacity-building programmes. And, as APC and WILPF recommended, these programmes should be developed inclusively and with full participation of women's and LGBTIQ groups.

A gender approach to cyber security goes beyond women's participation and gender sensitivity. It implies acknowledges that humans are the ones impacted by cyber threats and that people in positions of vulnerability are because of their sexual orientation or gender identity, among other things, at particular risk. To maintain a truly stable, secure, and human-centric cyberspace, Open-ended Working Groups should go further in addressing and recognising the gender dimensions of cyber security, that unequal power relations affect the experiences we all have online and should meaningfully involve civil society groups to understand how the enjoyment of the rights of women, and people of diverse sexualities and gender expression are affected in cyberspace.



In 2020, the Association for Progressive Communications (APC) and the Women's International League for Peace and Freedom (WILPF) co-authored a report on the gender dimensions of international cyber security.

The report identifies multiple gender-differentiated impacts of cyber operations and builds the case that these differentiated impacts need to be better accounted for and understood. The report explores the digital gender gap that exists within cyber diplomacy and policy professions. It was prepared as a submission to the UN Open-ended Working Group (OEWG) on Developments in the field of information and telecommunications in the context of international security.

Read the report.

NEWS IN BRIEF

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

The News in brief is not a comprehensive record of all statements and positions but attempts to capture key points from discussions.

General and process

- The vast majority of states welcomed the inclusive and democratic nature of the OEWG process.
- Malaysia highlighted that this is the first time all UN member states are working together on this issue. New Zealand said it was heartened by the interest shown in the OEWG from a broad range of member states which it said bodes well for the future. Indonesia made similar observations. Austria stressed that more than 140 delegations actively participated in this OEWG and made their voices heard, which it described as an accomplishment in itself, a view echoed by
- Canada. Belgium and Ecuador appreciated the opportunity provided by the OEWG, having been unable to join in the earlier UN Groups of Governmental Experts (GGEs). Global Partners Digital described the process as heartening and promising, demonstrating that member states can work together despite divergent views.
- Virtually all delegations expressed deep appreciation for the Chair's efforts and dedication to this process, as well as that of the Chair's team, the Secretariat and the UN Office for Disarmament Affairs (UNODA).
- Many states, including Russia and Poland, noted that the conclusion of this process is particularly noteworthy as much of it happened during a pandemic and in virtual or hybrid formats. The Netherlands, Estonia, and Singapore said the adoption of the final report is a major milestone for multilateralism. Others, such as Indonesia, Cuba, Russia, and Slovenia, called this process "historic". Ecuador stated that this process has helped to revive multilateralism, while Italy stated that it shows that multilateralism is "alive and kicking".
- All states that took the floor agreed to accept the final report, even if most noted that it is a product of compromise. Australia said the report is "finely balanced" while Indonesia and Egypt called it a "delicate balance".
- Liechtenstein argued that consensus should always be an aspiration but to evaluate it with universal veto power was a conceptual aberration that future discussions should stay clear of. Liechtenstein was also critical of the format of "this process and its decision-making modalities which favor containment over progress and minority restraint over majority aspiration."
- While congratulating all states for the good spirit that prevailed, Nicaragua, Cuba, and Iran would have preferred a paragraph-by-paragraph negotiation of the final report. Iran stated that the lack of text-based negotiations should not be precedent setting.
- The United States (US) expressed hope that the report's consensus adoption will usher in a return to consensus-based interaction and collaboration building on international law, voluntary norms, and confidence-building measures.
- Iran disassociated itself from the parts of the report that do not match its principles and positions, as it outlined in written and verbal form throughout the OEWG process. It said it would not be obliged by any paragraph that does not align with its positions but would not block the report's adoption by consensus.
- Australia recognised that the report is not the end of states' work but that it can lay another foundation upon which it can be built in future. New Zealand observed that the adoption of the report was not the end "but the beginning".
- Global Partners Digital observed that many of the recommendations rely on voluntary exchange and said it was important that states do more than what they committed to. Indonesia said that the report can serve as a map, and that the priority should now be to

follow up on the agreements, conclusions and recommendations in the report.

- Austria said that the report provides a significant "stepping stone" for the next steps. India also called it a stepping stone in a long journey to ensure a safe and secure cyber space. Turkey felt that the Chair's summary is a good basis for future discussions.
- The Nordic countries said that international diplomacy needs to keep up with the fast pace of technology. The Stimson Center made similar observations.
- Egypt expressed hope that this report can contribute to a prevention of an arms race in cyber space.

Structure of the report

- Argentina, Australia, Colombia, and the Nordic countries said the order of the document should have been the same as in earlier drafts, in which the sub-section on "International law" came before "Rules, norms, and principles".
- The European Union (EU) and Ireland stressed that the order in which international law and norms are presented shouldn't be understood as reflecting the hierarchical order of the two.
- Australia was pleased the Discussions section was retained. India reminded that it had requested to shorten the Discussion section so that it could be adopted by consensus.

Relationship to the UN GGE's and the *acquis*

- The EU, Austria, Estonia, Chile, and the Netherlands were pleased that the OEWG report reaffirms the content of UN General Assembly (UNGA) resolution 70/237. Japan, the Republic of Korea (RoK), Switzerland, Singapore, Czech Republic, Poland, the Nordic countries, the International Chamber of Commerce (ICC), and the United Kingdom (UK), among others, also welcomed that the OEWG report recognised the outcomes of past GGE reports. Canada, Belgium, France, Germany, Italy, Switzerland, the UK, and Ireland, amongst others, said they were pleased to see the *acquis* reaffirmed. Cuba said it is concerned by excessive references to past resolutions like 70/237.
- Chile and Brazil expressed disappointment that the current (sixth) GGE is not well-recognised in the OEWG report; Brazil said references would have been useful in paragraphs 33 and 36.
- Brazil hoped that "the adoption of this report by consensus, together with the report of the ongoing GGE, will lead to the return of a unified, universal, collaborative, constructive and consensus-based dialogue process within the United Nations." Mexico made similar remarks.

Threats

- Australia and the Netherlands welcomed the report's recognition that health infrastructure is critical infrastructure (CI). Belgium noted its concern about attacks on CI, especially medical facilities. The International Committee of the Red Cross (ICRC) welcomed the emphasis on the protection of medical facilities as a part of CI.
- The Netherlands welcomed the reference to the general availability or integrity of the Internet in paragraph 18, which it understands as the public core of the Internet. The Global Commission on the Stability of Cyberspace (GCSC) regretted that the term "public core of the Internet" didn't make it into the final text but welcomed the inclusion of the spirit of this notion throughout the text.
- The GCSC regretted the juxtaposition of CI and critical information infrastructure (CII) in paragraph 18. It argued that it was preferable to separate the "public core" concept from the idea of the critical information infrastructure which does not capture the essence of the Internet "core" being a global public good that is managed in a multistakeholder process.
- Pakistan said it views the reference in paragraph 18 to threats posed by information and communications technology (ICT) capabilities being developed for military purposes as a positive aspect of the report.
- The Netherlands welcomed the reference to threats to electoral processes.

- Cuba would have liked the report to have an explicit reference to unilateral coercive measures in this section.

- South Africa welcomed that the report highlights starkly the risks posed by ICTs. South Africa also was glad to see that the definition of CI is in national competence.

- Egypt regretted that the report doesn't include anything about the threats posed by the weaponisation of cyberspace.

- The Centre for Communication Governance at National Law University Delhi welcomed the acknowledgement that states may experience threats differently.

- The CyberPeace Institute said it will continue to document and analyse cyber attacks and their societal impacts to help operationalise technical and legal instruments.

Rules, norms, and principles

- The US welcomed that all UN member states made a clear affirmation, through the adoption of this report, that they should be guided by the existing non-binding voluntary norms on responsible state behavior in cyber space.

- The UK, Singapore, Australia, Access Now, and Switzerland, amongst others, welcomed this section including paragraph 25 that explains the relationship between international law and norms. The Centre for Communication Governance at National Law University Delhi supported paragraphs 32 and 34 in particular.

- Estonia, Kaspersky, and Access Now supported the recommendation for states to survey their national efforts to implement norms.

- Canada regretted that it its guidance on norms implementation was not incorporated into the text of the final report but in the spirit of compromise, is content with it being included in the summary.

- Cuba said that the report over-emphasises the development of new norms in some areas. Venezuela urged for new norms and principles to be developed, and these must involve binding commitments.

- Iran reminded that the OEWG's mandate requested further developing of rules, norms, and principles, and that the OEWG did not do this is a contradiction to the Group's mandate.

- Israel explained that it will understand the word "norms" in paragraph 24 to refer to the norms agreed by the 2015 UN GGE.

- Singapore, Kaspersky, and India welcomed paragraph 28 on supply chain security.

- The UK said that in reference to supply chains, it will be important to "work through the practical steps" steps and that the best way to establish trust and confidence in the use of ICT products is "to engage users and developers in cyber hygiene, cyber security and resilience in end-to-end product development."

- Kasperky would welcome more concrete recommendations in the future to develop more concrete tools for critical infrastructure protection and ensuring the ICT supply chain security.

- India welcomed recommendations in paragraph 33.

- China said that its priority is the development of new norms and said that it submitted a proposal with specific suggestions to that effect.

International law

- The US welcomed that through adopting this report all UN member states clearly affirm that international law applies to cyber space. Australia, Japan, Poland, Turkey, the UK, New Zealand, Switzerland, the Nordic countries, the ICC, and the EU welcomed that the report re-affirms that international law and the UN Charter apply to cyber space and state use of ICTs. Liechtenstein and Chile regretted that the report does not acknowledge the UN Charter's application "in its entirety".

- Argentina, Costa Rica, Germany, and Ireland would have liked to see stronger references to human rights and fundamental freedoms. Germany underscored that the UN Charter makes cooperation in these areas clear.

- Australia, Belgium, Germany, the Nordic countries, Austria, Brazil, Chile, Slovenia, Czech Republic, Switzerland, Liechtenstein, Estonia, the EU, Canada, Japan, and the University of Oxford would have preferred to see language on the applicability of international humanitarian law (IHL) to cyberspace retained in the negotiated part of the report.

- The ICRC is concerned that more states are developing ICT capabilities for military purposes and the potential humanitarian impact of ICT use. It said that the discussion on how IHL limits use of ICTs during armed conflict needs to continue and is essential for reducing harm and risk to civilians and civilian objects.

- Liechtenstein argued that the future of warfare will be characterised by cyber warfare that will have humanitarian consequences.

- Japan said it heard many convincing arguments, including by the ICRC and academia, for why IHL should be included and is applicable to cyber space. Liechtenstein also positively referenced the ICRC's contributions.

- Cuba regretted the deletion of the reference to specific principles and purposes of the UN Charter. RoK would have liked to see the principle of due diligence included. Japan and Canada would have also liked to see a reference to the right to self-defense in the report. Japan said it hasn't heard convincing arguments why not all principles or all areas of international law are applicable. Germany underlined that state responsibility and due diligence are key concepts under international law.

- The EU stressed that a universal cyber security framework can only be grounded in international law, including the UN Charter in its entirety, IHL, and international human rights law (IHRL), all of which apply in cyberspace. The Netherlands, Slovenia, Estonia, Austria, the Czech Republic, Liechtenstein, Germany, Canada, Chile, and Japan, amongst others, would have also liked to see human rights and or the applicability of IHRL and/or human rights affirmed more clearly. Czech Republic would have liked to see the human-centric approach more integrated in the report. Global Partners Digital and Access Now welcomed the human-centric approach.

- Liechtenstein and the CyberPeace Institute regretted that issues of accountability and attribution weren't included in the report.

- Cuba would have liked to see a reference to unilateral coercive measures in paragraph 34.

Confidence-building measures

- Austria, Japan, New Zealand, Estonia, Slovenia, the Netherlands, and Costa Rica, among others, welcomed this section. The US welcomed confidence-building measures (CBMs) that are essential to communication to improve stability; Belgium said they cannot be underestimated.

- Cuba took note of the changes made in this section.

Capacity-building

- The US, Estonia, Cuba, South Africa, Costa Rica, and Austria, among many others recognised the importance of capacity-building (CB).

- Australia, Austria, Estonia, Slovenia, the UK, Japan, Ireland, Canada, Estonia, New Zealand, and the EU, amongst others, welcomed this section of the report. Estonia said that more needs to be done to implement the existing framework on CB.

- The EU and Cuba stressed the importance of this section, especially with respect to low- and middle-income countries.

- The EU said it was important to include human rights and fundamental freedoms in the list of principles and in the design of CB projects.

- The UK said that the UN can use its convening power to raise the profile of CB and to encourage and coordinate good practice but that others too have a role to play.

- Turkey welcomed that concrete proposals such as the survey recommended in paragraph 65 is included.

- The Global Forum on Cyber Expertise Foundation (GFCE) welcomed paragraph 66.

- Cuba said that despite some changes being made in this section, the proposals of the Non-Aligned Movement were not fully recognised or reflected.

- The GFCE said the section on capacity-building lacked an emphasis on multi-stakeholder engagement. The Institute for Security and Safety also argued that CB sits with non-state actors to a large extent, and that states need to work closely alongside these actors, and offered its support to states. Kaspersky made similar remarks, calling for the strengthening of multi-stakeholders in CB.

Regular institutional dialogue

- Australia welcomed the careful and nuanced way of language in this section. Brazil made similar observations.

- The EU, Poland, the Netherlands, the UK, Estonia, Austria, Liechtenstein, Switzerland, Slovenia, Canada, Italy, Ireland, the ICC, Kaspersky, and Japan were glad to see the proposal for a programme of action (PoA) recognised. The EU said the PoA will offer the opportunity to develop jointly action-oriented, inclusive, transparent and results-based process building on previous outcomes. The Nordic countries argued that the PoA is "the next logical step" and that it places the UN at the centre of multilateral processes. As a co-sponsor of the PoA proposal, Canada felt the references to it fall short but are "minimally sufficient".

- South Africa argued that parallel processes will put a strain on resources, and it hopes to find a way around this constraint. It further said that the report provides a clear mandate for continuity in the new OEWG. It said that any process beyond the next OEWG might not enjoy its support given capacity constraints by its delegation.

- Peru welcomed further developing the PoA proposal in the context of the second OEWG.

- Russia said this OEWG report will guide the international community to boost the negotiation process on ICTs under the UN and will preserve the OEWG format in the future. Cuba and Nicaragua are looking ahead to future negotiations and advancing discussion in the context of the second OEWG; Iran said it will prioritise preparation of the second OEWG.

- The US said it had reservations about the need for the next OEWG to continue until 2025. Liechtenstein informed that it will re-evaluate its participation in the new OEWG. Liechtenstein cautioned that the intergovernmental mandate for the next iteration of the OEWG is even more affected by the flaws of favouring "containment over progress and minority restraint over majority aspiration", and therefore argued that the process in this form may have outlived its purpose.

Legal instrument

- The US reiterated that it cannot support a legally binding instrument (LBI), which is noted in paragraph 80. The EU, Australia, the Nordic countries, RoK, Estonia, Switzerland, Slovenia, the ICC, and Japan also didn't support the reference to a LBI in paragraph 80. Japan said this should have been left in the Discussions section of the final report. Belgium felt to consider an LBI is premature.

- The US argued that some states refuse to affirm essential elements of international law, and are unwilling to comply with voluntary norms, and therefore the US would not gain much confidence from negotiating a LBI. Japan made a similar argument.

- The US argued that ICTs aren't susceptible to traditional arms control agreements, and that it would be a distraction to spend years on negotiating a LBI.

- Egypt regretted that the report didn't include concrete proposals on a LBI. Peru would look forward to the future establishment of a LBI.

- Ecuador outlined that it does not see moving to an LBI, while implementing existing norms, or developing new ones as not mutually exclusive. Ecuador sees these as being

possible to do simultaneously and as mutually reinforcing.

- Israel would have liked for paragraph 76 to be more explicit that future processes will be governed by consensus-based decision making.

- Israel noted that the language in the first part of paragraph 80 reflects the deep disagreement amongst states, and that it does not see any need to develop an additional LBI at this time. Israel disassociated itself from any reference to a need for an LBI.

Stakeholder engagement

- Australia, Mexico, the UK, Poland, Canada, Germany, and Ecuador, among others, expressed their appreciation for the contributions by non-governmental stakeholders to this process.

- Australia welcomed that the report acknowledges the multi-stakeholder community. Mexico was pleased to see that certain experiences and shared concerns by other stakeholders, including international bodies and academia, have been borne in mind. Austria also said that it was pleased that views by various stakeholders, including academia, the private sector and civil society have been included

- The ICC appreciated references to the private sector throughout the text. Kaspersky welcomed the mentioning of public-private cooperation to protect critical infrastructure.

- The Netherlands, the EU, Ireland, and Canada said it would have preferred to see the important role of stakeholders in ICT security better emphasised in the report. The GCSC would have liked to see a clear commitment to a multi-stakeholder approach, particularly in paragraph 18. Switzerland welcomed the importance of a multi-stakeholder approach but would have liked to see more clarification of what the multistakeholder approach means.

- Indonesia said that a platform was needed to enhance partnerships with regional organisations and other stakeholders. Liechtenstein said that states should engage on the basis of the best available knowledge which means engagement of stakeholders, including civil society, academia, and the private sector.

- The GCSC argued that the future process' success will depend on its ability to leverage effective multi-stakeholder engagements to inform its deliberations and to advance the awareness and implementation of its proposals. The GCSC said stronger commitment to the preservation of the present multi-stakeholder management of Internet resources would be welcomed, but congratulated the Chair and Secretariat for involving non-governmental actors in this process.

- The Stimson Center outlined various ways where civil society could help jumpstart UN efforts, including by researching what should be in a PoA, and to assess how to avoid duplication of existing mandates of other UN bodies. The US Council for International Business underscored that governments need multi-stakeholder perspectives to better understand what policies are commercially viable, technically feasible, that offer human rights protection.

- The Institute for Security and Safety observed that multi-stakeholder participation was difficult in this process due to COVID-19.

- Global Partners Digital expressed hope that the a possible PoA would facilitate civil society engagement. Kaspersky and the US Council for International Business also encouraged multi-stakeholder participation in the future regular institutional dialogue and inter-governmental processes.

Gender

- Australia, Canada, Chile, and the UK welcomed the report's references to women's participation. Canada said it is important to see gender perspectives rightfully recognised. It, and Canada, would have liked to have seen stronger language, but consider this report a good first step.

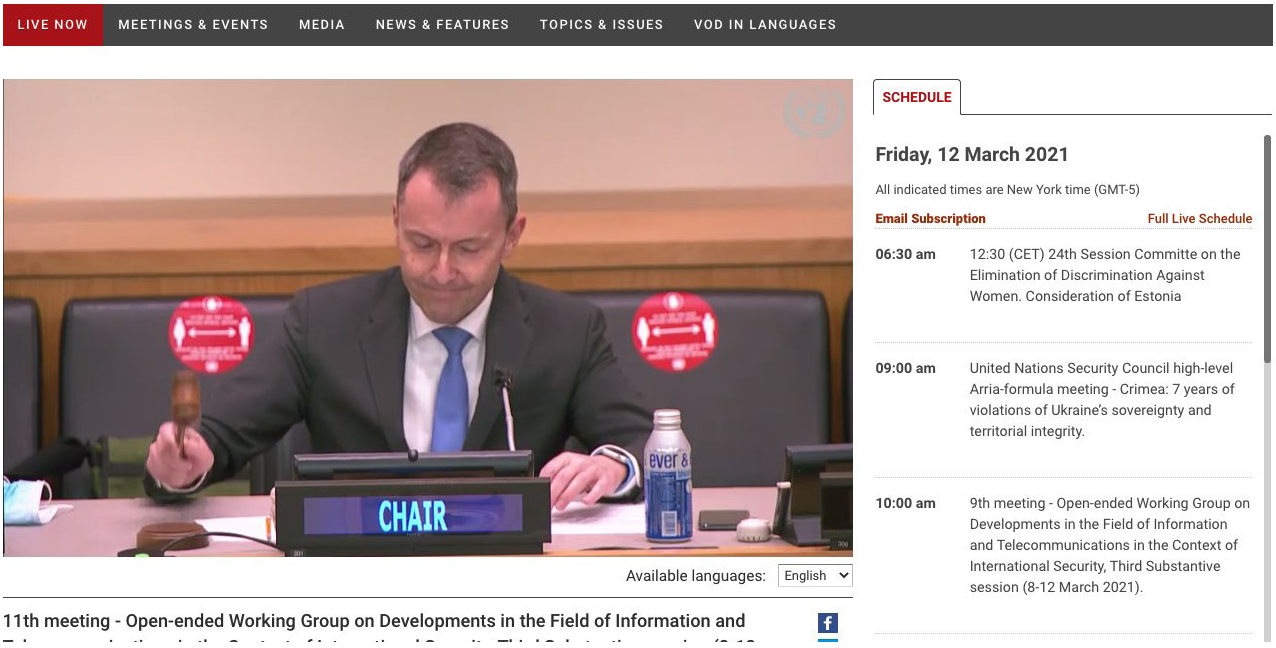
- Argentina, Australia, Canada, Colombia, and the UK welcomed and spoke positively of the impact of the Women in Cyber fellowship

programme, and of the contributions of its participants.

- Argentina and Pakistan stressed narrowing of digital divides, including the gender digital divide, which Ireland also highlighted. South Africa and the Centre for Communication Governance at National Law University Delhi welcomed the recognition of the digital gender divide, and calls to narrow it.
- The UK stressed that states must redouble efforts to ensure that diverse perspectives are heard.

Sustainable development and digital divide

- The Netherlands would have preferred to see the link between cyber space and sustainable development further elaborated.
- Various participants, including the Netherlands, the Centre for Communication Governance at National Law University Delhi, the Global Forum on Cyber Expertise Foundation, Mexico, and South Africa welcomed the recognition of and/or expressed concern over about the digital divide either within the report or generally.



OEWG Chair Ambassador Lauber gavels the adoption of the final report. Photo: Allison Pytlak

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 open meetings of the UN's OEWG on ICTs.

CYBER PEACE & SECURITY MONITOR
Vol. 01, No. 10
17 March 2021

Editor: Allison Pytlak

Contact: disarm@wilpf.org