ICC United Kingdom welcomes the opportunity to submit our views to the Third Substantive Session of the Open-Ended Working Group on the security of, and in the use of, information and communications technologies (OEWG). We will address both the questions posed by the Chair in his June 22nd letter and the recommended next steps outlined in the draft progress report, and open with some related perspectives that may be of use to delegations and stakeholders.

Issues around stakeholder participation

Like many others we were very disappointed to see that a large proportion of stakeholders seeking accreditation to the OEWG’s work were blocked by a very small minority of member-states. Given the mix of entities blocked and their origins, it is difficult to see these objections on any basis other than politically-motivated. It is our view that stakeholder participation decisions should always be based upon objective criteria, solely related to their interest in, and ability to, contribute to the processes to which they seek accreditation.

It is particularly regrettable to see such a large proportion of the private sector entities seeking accreditation being denied, given that the vast majority of the Internet’s infrastructure is managed and/or owned by the private sector, and given how significantly the private sector is harmed by malicious use of ICTs directly in the mandate of the OEWG.

The OEWG’s work programme and capacity building, technical assistance, and confidence building measures (CBMs)

As we have said at previous sessions, the most important contribution this OEWG can make to fulfilling its mandate is to agree practical measures that significantly increase the level of global implementation of the acquis agreed by consensus by the UN General Assembly in adopting the work of previous GGEs and the OEWG. We urge the OEWG’s member-states to agree to measures that support this shared goal of member-states and the broader stakeholder community. Cyber-insecurity is rising, the costs of acts contrary to the acquis are also rising. This OEWG will ultimately be judged on how, and to what extent, its work contributed to reversing these two trends.
A fundamental element to this is for this OEWG to agree at a high level what elements of national law and policy are prerequisites to implementing the aquis at the national level, and also as foundations to cooperate with states and stakeholders worldwide in the same vein. Globally the International Chamber of Commerce has endorsed this concept in calling for “Cyber Development Goals” that would define these high level elements, which would, in turn, allow all states and stakeholders who provide technical assistance and capacity building to collaborate to ensure resources exist for all states to meet these minimums. This third meeting of the OEWG, with a focus on development, is an important opportunity for member states to converge around practical steps that move in this direction.

Guiding questions for stakeholders provided by the Chair

We were glad to receive the guiding questions, and the many submissions of stakeholders demonstrate what is widely known: non-state actors provide invaluable contributions to the implementation of the acquis and to building the capacity of states and stakeholders to promote a more trusted, secure, Internet.

We would like to highlight two particularly important issues related to the various questions on how stakeholders can assist states in implementation of the acquis on responsible state behaviour:

1. When states implement the acquis, it is fundamentally important to involve national stakeholders in a discussion of how to develop the legal and policy landscape related to state behaviour online. There are many reasons why this is essential, of which just one is that as mentioned above, most of the infrastructure of the Internet as well as the services and products used by the public are the products, or are owned and operated by, the private sector and the expertise of the private sector related to that infrastructure is integral to making good choices on how to use it and how to protect it.

2. If states do not fully implement the acquis, or if they implement it and do not publish the details of state policy with respect to implementation, then other stakeholders do not have a foundation upon which to support the activities of public authorities. It is therefore important, when states look at the contribution stakeholders can make to implementation, to first look at what the state itself has done, is doing, or intends to do; stakeholders need a policy and/or legal framework upon which to base their own contributions.

Proposals for action in the draft report

We believe there are many positive proposals for the work of the OEWG proposed by states during the debate and recognised in the draft report. Before we address the report section-by-section, we have an overarching issue with the role of stakeholders on a horizontal basis.

The report should recognise that stakeholders have a role to play on a horizontal basis, not selectively, as is presently the case. Given that it is widely recognised that cybersecurity is a whole-of-society undertaking, the report should recognise this reality. It is our view that stakeholders should have a role by default across all areas of action, even if that role is different depending upon the context of their involvement and the area of activity concerned.

Existing and Potential Threats

In this section, bullet ‘a’ and recommended step 2 limits the sharing of risk assessments and technical information - including threat intelligence and relevant compendia - to states alone. This is unfortunate. It is the stakeholder community that mainly drives information-sharing, threat analysis, and cutting-edge research, rather than states. Cooperation solely via bilateral exchanges could be challenging for smaller states in particular, but also for many other developing countries more generally; it is important that all proposals for collective action should ensure that all states can benefit and participate meaningfully. The report could offer proposals on how the OEWG could systematically strengthen exchanges on threats with the broader multistakeholder community for the benefit of all states.

The call for specific measures to safeguard the so-called ‘public core’ of the internet is very welcome. We encourage states to hold focused discussions in future on specific components of critical infrastructure essential to the internet’s functioning - and accompanying commitments to recognise these nationally and to cooperate in protecting them across borders.

With respect to data security, we submit that this subject is not well-suited for the OEWG to work on, given that the subject goes far beyond the mandate of the OEWG and relates to many other policy domains outside of international peace and security. Any work done at the OEWG therefore brings a significant risk of unanticipated negative consequences for the economy and society.

Rules, Norms and Principles of Responsible State Behaviour

We welcome the emphasis on leveraging the online self-assessment hosted by UNIDIR implementing the national survey on responsible use of ICTs by states, originally proposed by Australia, Mexico, and others. This aligns with the recommendations in the 2021 OEWG
GGE reports, citing that “states, on a voluntary basis, use the model ‘National Survey of Implementation of United Nations General Assembly Resolution 70/237’ to help them assess their own priorities, needs and resources.” This is particularly valuable when combined with our previous recommendation, for states to agree on what we have called the Cyber Development Goals - the more states use the UNDIR survey, the more all stakeholders would be aware of where important gaps in capacity exist, which could then be addressed more proactively. A reasonable deadline for a first assessment could be the 4th substantive session.

In our view, further development of norms and their implementation are not mutually exclusive and should take place in parallel - but there is a need to emphasise wider implementation of the norms we have now. That said, the report should also outline ambitious and urgently needed steps on how to update the UN normative framework to better address current and future ICT threats, to secure global ICT supply chains, protect humanitarian data, and restrict the use of so-called ‘cyber mercenaries’ - the rapidly expanding industry of companies developing and selling tools, techniques and services that allow their clients - often governments - to break into networks, computers, phones and internet-connected devices and undertake acts contrary to international peace and security.

The stockpiling and selling of vulnerabilities for profit undermines trust and security in the online environment and gravely impacts human rights. It also violates the spirit of norm ‘(j)’ in the 2015 GGE report, which calls on states to encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies. This situation will only escalate and increase insecurity across the entire digital ecosystem if measures are not taken to address them through cooperation globally. We recommend that states act swiftly to provide additional guidance on this norm (j). At the same time, the discussion of this issue should also ensure there is space for more states to understand why disclosure of vulnerabilities is so important for all stakeholders, including governments.

We also welcome the proposal to encourage submissions of working papers to drive the OEWG’s work on, inter alia, norms guidance, implementation, checklists, and building common understandings of ICT terminology. This call is currently only addressed to ‘states’ and ‘groups of states’ - it should also encourage participation of stakeholders, to leverage their resources, expertise, and experience to drive work on norms implementation.

**International Law**

---

2 We support the comments of the Women’s International League for Peace and Freedom with respect to this issue, which may be found at [https://documents.unoda.org/wp-content/uploads/2021/12/WILPF_OEWG_December2021.pdf](https://documents.unoda.org/wp-content/uploads/2021/12/WILPF_OEWG_December2021.pdf)
What is key for the private sector is a focus on how international law’s application in the online environment can improve trust and increase legal certainty at a practical level. We therefore submit that this is the right lens through which to view the OEWG’s work in this area.

We welcome the proposal to change from general exchanges of views on international law to more granular, thematic exchanges of how different bodies of international law apply in the ICT environment. We submit that these exchanges should have a practical focus, rather than a focus on the law itself, as the object of the exercise - after all, the value in international law is not as an end in itself, but in how it is applied to produce legal certainty and international peace and security.

We also welcome the idea of inviting experts to deliver thematic briefings on different subjects of international law as well as leveraging existing academic initiatives, such as the Oxford Process, to provide relevant expert briefings.

Including a non-exhaustive list of topics proposed by states for further discussion under international law - spanning due diligence to human rights issues - was useful and could offer future opportunities for more detailed discussions. Although the list is non-exhaustive, we support explicitly mentioning international humanitarian law (IHL), rather than just listing its core principles without referencing the relevant body of law directly. Additional thematic areas that could be explored include questions on how prohibition of the use of force applies in cyberspace, legal rules prohibiting the use of proxies for conducting malicious cyber activities, the rules governing extraterritorial activities in cyberspace, and the extent to which states may take practical measures to limit acts that undermine international law emanating from their territory which are originated by non-state actors which are not proxies.

We endorse an OEWG process to hold states accountable for publishing their views on how international law applies to them, understanding this would be on an informal basis. It was positive to see concrete, action-oriented proposals on international law by states in the report, but overall, the recommended steps lack specific references to identifying gaps and exploring the need for additional legal obligations based on those gaps. The first step to seeing how the acquis’ obligations on international law are working is to understand how it has been applied and where by states.

Finally, we caution against using the term “mutual legal assistance” in international peace and security discussions as this generally relates to sharing information and evidence for criminal investigations. The section on threats (bullet ‘vi’) and the proposal in the section on international law (bullet ‘c’) for “improving mechanisms of mutual legal assistance for
investigating malicious use of ICTs” contains such references. While we fully support this idea in principle, we believe it falls outside of the remit of the UN First Committee and its subsidiary bodies.

Confidence building measures (CBMs)

Adopting cyber-specific CBMs at the global level would be welcome, as tools for reducing tension, minimising the risk of misperception and building trust. Given the work on CBMs in regional organisations we advise the OEWG not to duplicate efforts, but to distil existing regional efforts, good practices, and globalise them to focus on aiding implementation or amplification of previously agreed CBMs.

The proposal for the OEWG to establish a global points of contact (PoC) directory on ICTs is welcome, as is growing support of it by states. It should however include all relevant stakeholders, including private sector entities and operators of critical infrastructure - we note and welcome the offer of FIRST to contribute points of contact from the CERT/CSIRT community to this effort in their statement to the 3rd Session. The draft report’s specific limitation of this to states is a disappointment and we hope that a broader construction is adopted in the final report. We would also highlight that the UN need not create its own list, but instead build on successful efforts at the regional level; this would also help ensure the list is kept up-to-date. Finally we welcome the call in the draft report for the Secretariat to report on what initiatives already exist and to report to the OEWG so that it may progress work in this area.

We also support the proposal to convene an intersessional meeting with all relevant stakeholders to develop and implement additional CBMs beyond the proposed PoC network.

For the same reasons as above, we support the proposed focus on supply chain issues, preventing malicious uses of ICTs tools and techniques and of harmful hidden functions, and sharing of current threat information. We believe that a focused discussion on these key issues would allow states to compare and contrast different approaches and help to distil opportunities for collective action.

We also recommend examining additional CBMs that foster private-public partnerships to counter ICT threats and to establish global procedures for the coordinated disclosure of vulnerabilities among relevant stakeholders. There has yet to be enough focus on the issue of

---

vulnerability disclosure in the work of the OEWG - this is a subject that deserves a more intensive focus: disclosure of vulnerabilities benefits everyone, including states, and learning more about why this is the case would be of great value to the international community at large.

Finally, stronger references to the use of the UNIDIR Cyber Policy Portal as an avenue for sharing information (such as, White Papers, national strategies and policies including ICT capabilities, information on national ICT institutions and structures, and national lists of recognised types of critical infrastructure) would be welcome. We encourage states to further fund the UNIDIR Cyber Policy Portal so that it can expand its services in these and related informational products. In many ways, the Portal and the information it offers is a CBM in its own right. The OEWG can and should act to promote implementation, and states’ publicly reporting on their norm implementation and CBM-related efforts, with those efforts catalogued and accessible for all stakeholders through UNIDIR’s portal.

Capacity Building

As we mentioned above, capacity building and technical assistance is an area where further work by the OEWG may have the most impact, in two ways:

1. Agreeing on a set of Cyber Development Goals, (CGDs), so that the international community has a benchmark that can be used to assess what states need in order to reach the level of institutional and legal development that makes possible full implementation of the acquis by all states;
2. Leveraging that set of goals, it can agree how to leverage the survey previously mentioned, and decide upon any other mechanisms necessary, so that states may evaluate what assistance they need in order to reach the goals.

In our view these fundamentally positive steps could do more to ensure the acquis delivers on its promise to improve international peace and security in the cyber realm than any other single measures the OEWG could take.

We can see elements in the report that lead in this direction, from the emphasis on stepping up cybersecurity capacity building, and the suggestion that the OEWG could help improve understanding of capacity-building needs in developing countries.

We also welcome the recommendation to establish a trusted UN focal point with responsibility of coordinating offers and requests for capacity-building assistance. When this is established, we urge states to closely coordinate these efforts with organisations that have long-established experience and greater visibility into activities and programs in this domain, such
as the GFCE, which has a well-developed programme to aggregate capacity building projects in its Sybil portal. Such an approach would ensure a truly global collaboration for the benefit of all states, whilst avoiding competition and duplication of efforts.

In this vein, we also encourage the UN Secretariat and UNIDIR to work with the GFCE and other relevant stakeholders to analyse the results of this survey and present the outcomes at future OEWG sessions. As well as building understanding into the needs of developing countries, the OEWG and the UN Secretariat could also assist those states currently lacking the resources to meaningfully engage in UN discussions on cyber processes.

The Chair could convene a set of meetings – open to all relevant stakeholders – focusing on building the capacities states require. Opening this to other stakeholders would also help ensure a greater understanding in the multistakeholder community of the topics and challenges that the OEWG is addressing.

Therefore, we are encouraged to see a reference to states considering the establishment of a permanent mechanism for exchanging views and ideas related to capacity building in ICTs in the draft progress report.

**Regular Institutional Dialogue**

Unfortunately, as we have repeatedly stated, the overall security of the online environment continues to deteriorate. This is despite the progress in building an international framework for peace and stability in cyberspace that has resulted from these dialogues. The number of countries investing in offensive cyber capabilities continues to increase, and attacks have grown more frequent and more sophisticated, in seeming disregard of international expectations. The situation is made worse by the current, unlawful invasion of Ukraine.

Given this, there must be greater efforts at international level to increase the security and stability of cyberspace. There needs to be a regular and ongoing dialogue between all interested parties on these critical issues. We believe that it is time to establish a permanent UN forum broadly focused on cybersecurity issues – one that allows meaningful multistakeholder participation.

We welcome the fact that many states support creating a permanent body under the auspices of the UN that would include support for norm implementation and capacity building. The proposal for a Programme of Action (PoA) was positively referenced in the draft report, which we strongly support. However, we hope that the PoA is adopted as soon as possible and that it focuses on more than simply capacity building. We believe that the PoA should be a permanent, standalone body, rather than tied to the OEWG with a time-limited mandate. Moreover, it needs to be able to navigate in an area that values speed and innovation, meaning
that it should retain sufficient flexibility for states to agree on future new areas of work, and embed stakeholders directly in its strands of work.

There is little doubt that such a PoA would be a positive contribution to UN cybersecurity processes. Its establishment would send a strong signal of commitment by states to preventing, combating, and eradicating threats emanating from cyberspace. Moreover, it is envisioned to serve as a permanent, more structured yet flexible solution that allows for consensus driven, action-oriented and transparent regular dialogue between states, more multistakeholder engagement, and embeds the importance of capacity building. Such a structure would ensure both sustainable funding and incorporate existing processes into a single, permanent, mechanism.