International Chamber of Commerce
Input to the First Substantive Meeting of the OEWG 2021-2025

Given the significant reliance of business, large and small, on information and communication technologies (ICTs), the International Chamber of Commerce (ICC) is committed to ensuring that these work for everyone, every day, everywhere. We believe that the world benefits if all can fully realize the potential of the digital economy.

To this end ICC works with governments and businesses worldwide to build a common understanding of what constitutes a robust cybersecurity policy. We also seek to share best practices that can foster a more secure Internet for businesses and users alike, and safeguard the integrity of critical infrastructures.

We also recognize the important role the private sector plays in developing and maintaining secure technologies. The vast majority of the online environment is operated by the private sector, and we believe it is critical our experiences are reflected in the discussions at the United Nations (UN) on the topic. As an observer accredited to the UN General Assembly, ICC participated throughout the deliberations of the 2019-2021 Open-Ended Working Group (OEWG) as the representative of the private sector, and is now looking forward to further contributing to the work of the OEWG 2021-2025 by channelling the views of the global business community.

We therefore appreciate the opportunity to share the following perspectives for the Group’s consideration at its first substantive meeting, guided by the questions shared by Chair.

Participation of stakeholders

ICC commends the efforts of the 2019-2021 OEWG I to involve all stakeholders in its deliberations and strongly recommends that the 2021-2025 OEWG builds on those foundations, to ensure that the multistakeholder approach continues to evolve and deepen in all UN work in this area. We welcome the fact that the Chair of 2019-2021 OEWG I went out of his way to involve non-governmental stakeholders in the deliberations - either through written input, participation in the informal consultations or complementary events organized by member states and partners. These efforts resulted in invaluable insights and considerably enriched the work of the OEWG, reinforcing its efforts and contributing to the success of its final report.

However, outside a single meeting, these were informal efforts and as a result the bulk of the discussions took place in parallel silos, with little opportunity for meaningful dialogue between non-governmental stakeholders and all members of the UN. Non-governmental stakeholders only succeeded in sharing their valuable input thanks to the commitment and resolve of the Chair, the United Nations Office on Disarmament Affairs (UNODA) Secretariat and some of the member states who made it their mission to champion stakeholder input and ensure that all views were considered during the deliberations of the Group.

We respectfully ask that these pathways are not only kept open now, but turned into stable, open and formal communication highways, giving the opportunity for all interested stakeholders – not only those with consultative or observer status – to meaningfully participate in the work of the OEWG 2021-2025.

Therefore we wholeheartedly support the joint letter shared with the Chair on behalf of a group of over 150 states, organizations and individuals, which ICC was also proud to sign. We believe the principles offered therein will enable the Group to engage stakeholders in a ‘systematic, sustained and substantive’ manner.

Given that the OEWG’s mandate is for 5 years, we would also recommend that the list of non-governmental representatives be kept open or that frequent opportunities are given for
its update and renewal, thus ensuring that any new and emerging organizations can join the group’s work. The process itself should also be reviewed regularly to ensure it facilitates the accreditation of more diverse stakeholders throughout the five year cycle.

**Action-oriented approach and deliverables**

We believe that a structured approach to the discussions of the OEWG has the greatest potential to yield results. A pre-determined schedule and program of discussion, dealing with topics in a sequenced fashion can help ensure adequate preparation, consultation and thorough discussions that lead to actionable results.

Holding all meetings in sequence, under the guidance of the Chair and with the participation of all delegations ensures that even the smallest delegations can meaningfully participate and consult their experts in capitals, even real-time, if necessary. It also has the potential for enhanced effectiveness, as any decisions or recommendations for a way forward can be taken with the participation of all, without subsequent vetting or re-negotiation in plenum, as any subgroup decisions would inevitably do. Last, but not least, this would also decrease the burden on the Secretariat, that can focus its full attention to supporting and reporting from one meeting at a time. Therefore, with **meetings held in sequence with the participation of all delegates**, it would not be necessary to create additional working groups or subgroups.

Given the time-critical nature of the issues the OEWG will address, we believe it is of fundamental importance that the OEWG delivers substantive outputs for adoption by the General Assembly throughout its cycle, rather than waiting until the end of its mandate to report back. Transboundary cyber incidents are escalating exponentially and the OEWG is, at present, the only body actively addressing peace and security issues in the online environment. In this context, regular substantive deliverables from the OEWG would not only address these pressing challenges in a timely fashion, they would also send the signal that the international community takes seriously its obligations in this area and is seized of the seriousness of the issues in question. We therefore call upon member-states to ensure that the modalities of the OEWG provide for **at least two substantive deliverables for decision by the General Assembly during this OEWG cycle**.

One such possible output of Group could be an overview of the various legal, policy, and bureaucratic building blocks that are deemed necessary at the national level to facilitate the implementation of existing agreements. This could serve not only as background for member states and all relevant stakeholders in the implementation of the existing acquis, but also as a guidance for capacity building programmes.

**Substantive areas of work**

Crucially, the OEWG 2021-2025 will not be starting its work from scratch. Rather, the OEWG 2021-2025 will be building on robust acquis. The existing acquis of international law, including international humanitarian law and human rights law, the entirety of the Charter of the United Nations, reports of the GGE – especially the voluntary and non-binding norms of responsible State behaviour it developed – as well as the report of the previous OEWG are the foundations that should underpin future work, thereby ensuring their broad recognition and, critically, their effective implementation worldwide.

The OEWG I was particularly helpful in summarizing existing work and discussions on the most pressing challenges under six thematic areas: (i) existing and potential threats, (ii) international law, (iii) Norms, rules and principles for responsible state behaviour, (iv) capacity building, (v) confidence building, and (vi) continued institutional dialogue. The latest GGE also decided to follow this structure for their deliberations.

**We believe that it would be a natural and productive continuation of previous conversations to organise the work of the OEWG 2021-2025 under these six themes.** Continuing in this fashion would also ensure that progress is made towards the implementation of the valuable recommendations of the previous OEWG.
With regards to the substantive questions under the six thematic areas proposed by the Chair, we would like to share for the Group’s attention and consideration ICC’s recently published Call for Government Action on Cybersecurity.

As outlined in the paper, cybersecurity is a shared responsibility between the private and public sectors, and both must work together to curb threats and mitigate risks. Unless we take decisive collective action to address the growing trend of cyberthreats, the private sector and by extension our economies will continue to bear the brunt of these attacks.

The global business community has, and continues to make significant investments in securing technologies and developing defensive cyber tools, skills, and procedures. At the same time, to substantially curb the ever-rising trend of cyber threats, both in the probability of occurrence and in its organisational and social impact and incidents, concrete actions are also needed by governments—on both the national and international fronts.

While business investment in prevention and defensive capabilities is essential, the private sector alone is unable to deter, prevent, or properly shield itself, and the communities it helps sustain, from the destructive effects of cyberattacks.

Therefore, we urge governments to take more assertive and ambitious action to curtail cybersecurity threats that impact individuals, communities, and economies. In this context, our paper calls on governments worldwide to, among others:

- **Uphold commitments to international law and norms of responsible state behaviour in cyberspace as set out in the most recent OEWG and GGE reports.** To counter the flood of disruptive and damaging cyberattacks around the world, it is essential that these norms are properly implemented. A potentially useful tool here is the survey of norms implementation proposed by Australia, Mexico and other states that encourages governments to assess and report on how they are implementing their commitments.

- **Implement and enforce legal instruments that deter malicious cyber activity.** Turning the tide against escalating cyber risks will require states to go beyond high-level commitments and focus on their implementation within individual national contexts. National legal regimes must provide states with the tools necessary to effectively combat cyber threats and protect their businesses and communities from an ever-growing ecosystem of affiliated and unaffiliated threat actors with both political and criminal objectives.

- **Invest in capacity building.** Implementation efforts should include formal activities to develop managerial and technical skills and competences in judicial, security, and legislative actors involved in the investigation and administration of justice and set up the organisational infrastructure that’s required to implement international obligations and best practices. This requires resourcing and governments should recommit themselves to ensuring the resources are available so that all countries are in a position to cooperate with each other and industry to implement to take the actions required.

- **Adopt a multistakeholder approach to inform policies.** While governments have unique responsibilities in implementing agreed norms and protecting business and civil society from foreign and domestic cyberthreats, the shared nature of cyberspace requires collaboration between and across stakeholder groups to protect the safety and integrity of cyberspace. Multistakeholder action is critical across rules development, capacity building, and implementation.

The 2019-2021 OEWG has laid an invaluable foundation by establishing and reinforcing norms, but the dialogue cannot stop here. Undermining the security of ICT supply chains, attacking healthcare organisations, threatening energy, transportation, and jeopardizing food resources cannot become the kinds of activities that are normalised due to inaction.
As we demonstrated in the 2019-2021 OEWG, the International Chamber of Commerce is committed to providing continued support and meaningful business contribution to the work of the OEWG and looks forward to sustained dialogue with Member States and other non-governmental stakeholders. We are convinced that the 2021-2025 OEWG will enable us to build on existing foundations and make further progress for the benefit of communities across the globe that increasingly depend on a stable and secure online environment.