International Chamber of Commerce Submission to OEWG 4th Intersessional Meeting

Points of Contact Directory

The International Chamber of Commerce supports the idea of creating a UN Point of Contact Directory. This would be a vital tool, helping to build confidence both internationally and domestically. While the directory would undoubtedly help to enhance international cooperation and avoid conflict between states, it will also encourage broader confidence in the online environment across all stakeholder groups.

The PoC directory will particularly help facilitate coordination when the impact of cyber incidents extends across borders. This is incredibly important for business, given that their clients, assets, and operations are increasingly distributed across the globe. While the private sector is working hard to develop, deploy and use secure technologies, they also count on the support of governments to ensure that the necessary policies, norms, and laws are in place to ensure their citizens and companies are protected. The presence of a global directory of Points of Contact will help not only to direct and expedite response during times of crisis, but also to reassure citizens and business that countries are working together in the face of borderless cyber threats.

There is a need for the PoC directory to eventually include all relevant stakeholders. When an incident occurs, businesses are often not only the first target, but also first responders. Their expedited action can be instrumental in minimizing the impact or escalation of a threat. That’s why we encourage member states to consider including the private sector in the PoC directory. We also want to draw attention to the value of computer emergency response teams as points of contact. National and regional CERTS can act as a convener for stakeholders and enable education and best practices on cybersecurity issues. Today, too many countries do not have a CERT, and should be supported to develop them. This can itself act as a confidence building measure.
Cyber Development Goals

Cybersecurity is an inextricable part of digital development, and accelerating digital transformation is essential to achieving the Sustainable Development Goals. However, with transformation comes increased cybersecurity risks, especially in low- and middle-income countries that may lack adequate cyber resilience against constantly evolving digital threats.

There is a tension between the need to close digital divides and advance digital transformation and the lack of a strong cybersecurity posture. This presents a risk to achieving the SDGs and a threat to achieving a safe, secure, and rights respecting online environment.

The implementation of the acquis needs to be accelerated in order to protect societies from the increased cybersecurity risks associated with digital transformation.

To help achieve this aim, the international community needs to recognise that there are essential elements in national law and policy frameworks, and institutional capacities, without which a state cannot effectively implement the acquis agreed by the international community.

Agreeing what those elements are through a set of specific measurable goals would greatly facilitate countries in implementing and complying with universally endorsed UN norms for responsible state behaviour in cyberspace. The Cyber Development Goals – or CDGs – is a multistakeholder effort to define such a set of goals.

The CDGs could help to:

- Agree the elements of national law and policy that are integral to implementing the existing international acquis at the national level
- Contribute to mainstreaming cybersecurity into the development agenda, and facilitate the integration of cybersecurity capacity building efforts with existing development programs
- And mobilize the UN Development System and stakeholders worldwide around achieving concrete goals and facilitate coordination.

The International Chamber of Commerce remains committed to supporting the working group and ensuring that business plays a part in the acquis delivering on its promise to improve international peace and security in the cyber realm. The CDGs could contribute to this mission.

The role of business in capacity building

Business plays a central role in capacity building – providing technical guidance and implementing programs through involvement in existing multistakeholder forums, such as the Global Forum for Cyber Expertise. These forums act as a resource for states, coordinating regional and global cyber capacity projects and initiatives; sharing knowledge and expertise by recommending tools and publications; and matching individual needs for defensive cyber capacities to offers of support from the community. ICT infrastructure is largely built and maintained by the private sector, and a vast wealth of cybersecurity skills and knowledge is found within the private sector. Business wants to support states around the world to build their cyber capacities, and welcomes mechanisms which strengthen public-private collaboration.