# Views on Capacity Building Efforts and UN Cyber OEWG

Capacity building initiatives under UN Cyber OEWG and it's accredited stakeholders have been instrumental in achieving aims of the consensus agreed upon by states in formal substantive sessions as well as informal sessions.

Third Eye Legal seeks to synergise capacity building efforts with all states and stakeholders under the auspices of UN Cyber UNOEWG. Third Eye Legal has participated in many events on topics of vulnerability disclosure held by Microsoft and Let's Talk Cyber, programme of action consultation held by Cyber Tech Accord and contributed to UNIDIR's effort to collect views on programme of action among many others.

Stakeholder initiatives held by Kaspersky, GFCE and others have contributed in helping states build technical capacity in cyber security, cyber resilience and protection of critical cyber security incidents through incident response programs.

Just as malicious actors share lessons, techniques and tactics to cause harm so should states, law enforcement, private sector and civil society collaborate to defend cyberspace especially the critical information infrastructure and critical infrastructure before the onset of an attack through effective early warning mechanisms of sharing threat intelligence via CERTs and mitigate harm after an attack by way of sharing technical, legal and forensic information through joint collaboration of Critical Incident Response Teams.

UNIDIR's cyber policy portal has been instrumental in mapping capacity building efforts among states and stakeholders. One of the UNIDIR's side events at the UN Cyber OEWG shared a project on taxonomy of malicious ICT incidents that measures implementation of norms, rules and principles of responsible state behaviour in their response to cyber incidents in cooperation with stakeholders; can be helpful in providing an overview of threats against measures taken to mitigate them, thereby strengthening confidence building measures among states. This can also be achieved in close coordination with other bodies under the UN umbrella mandated to assist states in Critical Security Incident Response through CSIR Teams. National Survey of Implementation collection through the portal can also assist states to map which areas they may lack in and require capacity building efforts.

Stakeholders representing business interests of the private sector like International Chamber of Commerce, United States Council for International Business and others have assisted members of their respective representation to achieve ICT security.

Businesses have key role in maintaining peace and security in the ICT ecosystem. Businesses as well as non-governmental stakeholders own civilian infrastructure responsible to provide digital products and services and any potential weakness in one and can have a negative and at times devastating impact on not only the business itself but its users. The supply chain effects can leave cascading impact and result in huge losses in monetary terms as well as other effects such as loss of critical data. Similarly, critical infrastructure services that operate using private sector data can be exposed to vulnerabilities which if not mitigated can have grave consequences.

Security of critical infrastructure during peace times is essential and can be achieved if states follow agreed upon non-binding voluntary norms, however, in case of discord which may lead to a potential and actual conflict, there is a need for a legally binding instrument based on UN Charter and International Law that binds states not to attack critical civilian infrastructure. States need to recognise that the need for such a legal instrument is not a premature proposition given the current geopolitical situation of hybrid conflicts persisting in different regions of the world. Third Eye Legal seeks to work with states and interested stakeholders on International Law and have contributed to various formal and informal sessions with proposals on how such an outcome can be achieved.

International law is the foundation for stability and predictability in relations between States. In particular, international humanitarian law reduces risks and potential harm to both civilians and civilian objects as well as combatants in the context of an armed conflict. In various sessions of the UN Cyber OEWG, states underscored that international humanitarian law neither encourages militarisation nor legitimises resort to conflict in any domain and therefore the need to agree on principles of IHL as well as International Human Rights Law in the use of ICTs only cements the prospect of peace in times of conflict.

Norms implementation and the need to agree on principles of International Law that apply in ICTs are confidence building measures pivotal to attain the objective of the UN Cyber OEWG that is to maintain peace and security in the use of ICTs. Third Eye Legal seeks to synergise with UN bodies and stakeholders of UN Cyber OEWG to build capacity in law and policy.

Capacity building of states along with private sector and non-governmental organizations included is required to assure peace and security in the use of ICTs that

can be achieved through collective effort and collaboration; giving due respect to differences and ensuring diversity, equity and inclusion in such efforts.