Deepening our understanding of GGE norms on responsible States behaviours

FFT Paper

Croatia, Finland, France and Slovenia believes that both OEWG and GGE should build on the norms defined by previous GGE reports and endorsed by the UN General Assembly to address today's stakes.

All States face challenges when ensuring that their territory and ICT systems are not being misused or used for malicious acts. The increasing number of non-states actors, in particular lawful businesses, that are using offensive cyber capabilities outside of the perimeter of their network has become one of those challenges. In that regards, the role of private sector actors in developing and using ICT defensive and sometimes offensive capacities for their own use can be problematic and potentially escalatory. This concern has already been raised in many fora notably by the Paris Call for trust and security in cyberspace's community.

While defending themselves from threats originating from all over the world, these actors may make use of these capabilities in other States' territory. This new trend raises serious concerns and could be a growing destabilizing factor to State-to-State relations, thus becoming a threat to international security and the stability of cyberspace. Yet, non-State actors also need to be aware of what they can or cannot do in case of a cyber-attack.

From a technical point of view, due to the complexity of the attribution of cyberattacks – as recognized by previous GGE reports – and to the risk of misperceptions, non-state actors could easily target innocent entities in other States. Responses, in particular if non-proportionate or unnecessary, could have damaging effects. The consequences of such responses to cyberattacks, in particular in case of wrongful attribution or inadequate response, could then lead to harmful consequences on State-to-State relations.

In its previous reports, the GGE recognized that States have a primary responsibility for maintaining a secure and peaceful ICT environment and agreed – among others – the following norms of responsible State Behaviours:

- States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;
- […] States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty..

We considers that those elements should be stressed and underlined in the work undertaken at UN level, with a view to preserving the security and stability of cyberspace and avoiding escalatory behaviours, while recognizing that a broad range of actions can legitimately be undertaken by private entities.

In order to deepen our collective understanding and ability to implement agreed GGE norms, the report should mention, as it clearly derives from previously agreed norms and from the principles of International Law, including sovereignty , that **States should be encouraged to take measures to prevent non-State actors, including the private sector, from conducting ICT activities for their own purposes or those of other non-State actors to the detriment of third parties including those located on another State's territory.** This aim could be achieved by working with the private sector to define permissible actions using a risk-based

approach and to develop concrete tools - certification processes, best-practices guides, response mechanisms to incidents and, as appropriate, national regulations.