First session of the AHC on Cybercrime, Agenda Item 3 (General Debate), Mark Shaw of GI-TOC

- Excellencies, distinguished delegates. It is a pleasure to be addressing the Ad Hoc Committee on behalf of the Global Initiative Against Transnational Organized Crime.
- We appreciate the efforts of Her Excellency the Chair and the Secretariat in taking us forward in this process.
- Since the adoption of the UNTOC in 2000 we have seen an unprecedented expansion and diversification in how organized criminals do business. Technological growth has played a key role in providing new avenues for illicit actors to ply their trade, but not all of these illicit activities depend wholly on technology, and many of these acts are already criminalized around the world.
- Policy makers and law enforcement face an incredible challenge in tackling the range of both cyber-dependent crimes such as ransomware attacks which can threaten business, critical infrastructure and public services, and cyber-enabled crimes such as child sexual exploitation or illicit wildlife trafficking which harm the most vulnerable or exploit our natural resources.
- Cybercrime, cybersecurity and government control of the internet are closely interconnected issues. This Committee has already seen how external crises and factors impact on our discussions here, and will continue to do so. It is the responsibility of states to negotiate this instrument in good faith, and to ensure that implementation matches the commitments that have been made.
- We and others in civil society stand ready to support the Committee, despite the challenges, and encourage it to continue consulting and engaging with civil society organizations who are experiencing and gathering data on the effects of cybercrime in communities around the world.
- To begin with I want to share the following 9 key principles that we see as priorities for a new instrument:

1. The instrument should have a stated aim of improving all countries' ability and capacity to prevent and counter cybercrime with a focus on the types of illicit activities that do the most to harm to people, societies and the environment. This must be done whilst safeguarding human rights and freedom of speech.
2. This process is an opportunity to fast-track capacity building and technical assistance support to the places that need it most. Tackling all types of organized crime requires a development-centred response, and cybercrime in particular highlights the digital divide.
3. Definitions should be concrete and based on existing agreements. It should not promote definitions of 'cybercrimes' as crimes against the state. The treaty should not be used as a platform to criminalize journalism, information sharing, or dissent.
4. The instrument should enhance practical international cooperation across different constituents – between law enforcement and judiciary from different countries, between law enforcement and the private sector, and crucially between these groups and civil society. Indeed, the role of civil society should be enshrined in the convention, recognizing their role in protecting their communities against cybercrime, alongside law enforcement.

5. It should improve all countries' ability to gather and share cross-border evidence and data in a mutually trusting way, prioritizing transparency. In facilitating this cooperation, there should be adequate safeguards on human rights, data protection, protection of witnesses, including whistleblowers and journalists.

6. The instrument must address the role and responsibilities of the tech providers and social media platforms in preventing and responding to criminal activity, without facing undue intimidation or harassment from authorities.

7. There should be a dedicated chapter on prevention, as included in UNTOC and further developed in UNCAC.

8. The Convention should mirror UNTOC Article 28 on the 'collection, exchange and analysis of information on the nature of organized crime'.

9. Consequently, the conference of parties and review mechanism should be open, accessible, flexible and able to discuss the latest research, trends and data. The instrument and its follow up mechanisms should be coordinated and strategically aligned with existing UN processes on transnational organized crime, digital governance and human rights.