*Nedan följer en sammanfattning från sommaren om det senaste inom arbetsgruppen för cybersäkerhet. Sammanfattningen är skriven av ICC:s **Timea Suto**, Global Policy Lead. De papper som hänvisas till för kommentarer är bifogade i utskicket.*

FOR INFO: Updates on UN OEWG on Cybersecurity

The 3rd Substantive Session of the OEWG took place on 25 – 29 July in New York. After four days of extensive conversations, member states reached the adoption of both the First Annual Progress Report of the OEWG and the Procedural Report of the OEWG. The report will now be presented to the General Assembly via the First Committee for adoption.

The main elements of the adopted report, as well as major sticking points during the discussions were:

Threats
While the report recognizes that the severity of cyberattacks is on the rise – especially as it relates to critical infrastructure (CI) – the report does not include specific reference to ransomware despite strong support by several member states for this to be considered by the OEWG.

Rules, norms and principle
The report includes strong language on security of supply chains, based on the 2021 GGE report. It also calls for more transparency measures on the implementation of norms through mechanisms such as surveying.

Divergences persist between delegations on whether the OEWG should be a venue to discuss the implementation of existing norms or creation of new norms. Ultimately, the report notes that the two are not mutually exclusive.

International law
Debate focused on the applicability of international humanitarian law in cyberspace. A number of states proposed a reference to international humanitarian law, including a specific mention of the International Committee of the Red Cross (ICRC).

States continue to express mixed views on the need for new legally binding obligations for state behaviour in cyberspace. A majority do not see the need for nor the feasibility of developing a new legal instrument, while a few see this as a priority for the OEWG.

Capacity building
Cyber capacity building continues to be a topic of great interest, including for the Chair and his team. Several calls were made for more focused discussions on capacity building at the upcoming sessions of the OEWG.

Confidence building measures (CBMs)
Several states voiced support for a clear reference to CERT-to-CERT communication between states as part of CBMs and establishing a PoC directory. States also called for more focused discussions on CBMs at the upcoming meetings of the OEWG. A major output of the report is the recommended next step to produce a global Points of Contact directory.

Regular Institutional Dialogue
The main point of debate was around the reference to the proposed cyber Programme of Action (PoA) and how the report should recommend using future OEWG sessions to discuss the PoA. In the end, the report includes a reference to the PoA, which although much broader than was originally proposed, includes a commitment for future focused discussions.

Participation by stakeholders
Several states expressed their disappointment with Russia's decision to veto certain non-governmental stakeholders' participation in the OEWG. Several of the same states also noted the importance of including stakeholders' input across all topics discussed by the OEWG.

For a more detailed overview of the meeting and the annual progress report, I recommend consulting this analysis prepared by Reaching Critical Will, the disarmament programme of the Women's International League for Peace and Freedom (WILPF).

Please do not hesitate to reach out to me should you have any questions or comments.

FOR INPUT: Annex to ICC Cybersecurity Issue Brief #2 on Cybercrime

As you are aware, ICC is observing the work of the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (AHC). As the AHC is going through the first reading of the Convention's elements, ICC's inputs are informed by our IB#2.

To contribute to the AHC process with **further substantive considerations**, especially as details of the Convention will start to firm up in the second reading starting with the AHC's 4th meeting (January 2023), we are developing an **annex to IB#2**. The aim of this annex is to pin-point the key elements of top priority and importance for business on cybercrime in general and the Convention's provisions in particular, and provide detailed guidance for ICC's positions on these topics.

Thank you to everyone who provided initial comments on the first draft of the Annex. We strongly encourage members to provide further comments on the draft ahead its finalization to reflect the broad set of views represented in our working group.

Timeline and milestones
- **10 September**: Finalize the paper based on your first and second round of comments
- **December 2022**: Submission of the paper to the AHC ahead of its 4th Substantive Session
- **9-20 January 2023**: Side event during the 4th Substantive Session of the AHC

FOR ACTION
- Please send your substantive comments on the shared draft annex **by 1 September 2022**.
- We are also looking to create an advisory group of legal experts that will advise the ICC Secretariat in near real-time on the text of the Convention. Thank you to those of you that already volunteered to participate in this initiative. If you are interested in taking part in this group, please let meni.anastasiadou@iccwbo.org know at your earliest convenience.

FOR COMMENT: Background paper on Cyber Development Goals – next steps & advocacy plan

As you know, the ICC Cybersecurity IB#2 introduced the concept of the Cyber Development Goals (CDGs) and proposed a set of draft objectives.

Over the past months, members worked on a **background paper** to further develop the details of the concept. This paper will serve as the main internal background and guidance document for ICC and members on the concept of the CDGs. This paper will serve as the base for a short (ideally one-pager) **external-facing advocacy document** around which a global communications and advocacy campaign will be built with the aim of gathering multistakeholder support for the CDGs and their implementation. The one-pager document will then be opened for further input, commenting and editing by multistakeholder partners.

Based on the first round of comments by members, the background paper now includes:

the main 8+1 policy elements for consideration as CDGs – for further review

an initial mapping of existing initiatives and resources with broad business support that help implement these objectives – for further expansion

Timeline and milestones

- **25-29 July**: the CDG concept was socialized with member states and stakeholders during 3rd Substantive Session of the Open-ended Working Group and received endorsement in a plenary meeting by the delegation of the United Kingdom that noted its interest to work with ICC on the development of the goals. Further interest was expressed in bilateral discussions by the delegations of Australia, Canada, Costa Rica, Fiji, Indonesia, New Zeeland, Mexico, South Africa and Sri Lanka as well as the Chair's team, UNIDIR, OSCE, the GFCE and the Global Cyber Security Capacity Centre (GCSCC) at the Oxford Martin School

- **August- September**: development of the one-pager external-facing advocacy document
- **September**: High level event on cybersecurity and development during the 77th session of the UN General Assembly
- **28 November-2 December 2022**: ICC BASIS Workshop "Towards Cyber Development Goals: implementing global norms" at the Internet Governance Forum 2022 (IGF 2022)
- **Q4**: work with multistakeholder partners to develop the joint proposal on the CDGs to the OEWG ahead its 4th session planned for March 2023, based on the one-pager

FOR ACTION

Please share your comments, edits and further contributions on the background paper attached (especially on the sections marked with red) at your earliest convenience, but **no later than 1 September.**