Subject: *Request to Amend the Annual Progress Report (APR) - Emphasizing Co-Development of Emerging Threat Countering Toolkits and Automating Points of Contacts for Confidence Building Measures*

Dear Respected Chair,

In reference to the letter shared on the 27th of July on the Open-ended working group on security of and in the use of information and communications technologies 2021-2025. I am writing to request an amendment to the Annual Progress Report (APR) of the UN Open-ended Working Group (OEWG) on ICT Security, with a specific emphasis on the necessity of co-developing futuristic shared emerging threat countering toolkits and automating Points of Contacts as Confidence Building Measures (CBMs).

As we work towards fostering a secure and resilient cyberspace, it is essential to address both current and future cyber threats effectively. We would like to propose the inclusion of the following key measures as an active research society who is building the R&D capacity, policies and regulations pertaining to the different innovation platforms and solutions in the space:

1. Co-Development of Emerging Threat Countering Toolkits: The report should recognize the importance of collaboration in co-developing futuristic shared emerging threat countering toolkits. These toolkits will serve as a comprehensive repository of knowledge, best practices, and cutting-edge techniques to counter evolving cyber threats. By pooling the expertise of various stakeholders, we can create a robust defence mechanism that stays ahead of emerging threats. We suggest adding that to the existing and potential threats in paragraph 10 and to section C on Rules, Norms and Principles on Responsible State Behaviour

2. Automated Platforms for Points of Contacts: As part of the Confidence Building Measures (CBMs), the report should highlight the significance of automating platforms for Points of Contacts between nations. Joint Manual and Automated systems in collaboration with existing networks of IRS and CERTS will facilitate real-time communication and information exchange, enabling swift responses to cyber incidents and improving cooperation during times of crisis. This can be added to section E paragraph d.

3. The rapid evolution of technology demands a proactive and holistic approach to cybersecurity. I would like to elaborate on a few key areas that merit comprehensive consideration:

A. Emerging Technologies: The report should emphasize the impact of emerging technologies on cyber threats. For instance, Artificial Intelligence (AI) and quantum computing pose unique challenges that must be addressed to ensure the responsible and secure use of these transformative technologies. This can be addressed in section C , paragraph d and as well in section B paragraph 15

- AI Example: AI-powered cyberattacks can autonomously adapt to defensive measures, making them more challenging to detect and combat. Therefore, we must promote responsible AI development and address potential security implications.

- Quantum Computing Example: Quantum computers could break currently secure encryption algorithms, compromising sensitive data. The report should underscore the urgency of quantum-safe encryption research to safeguard data privacy.

- Supply Chain and Digital Smart Cities Example: The interconnectedness of supply chains and digital smart cities demands robust security measures. By addressing potential risks in these areas, we can bolster overall cyber resilience.

B. Digital Smart Cities and Supply Chain Security: The interconnectedness of digital smart cities, built on IoT and 5G networks, demands robust security measures to safeguard critical infrastructure. Encouraging sovereign R&D development of secure technology will contribute to stronger supply chain security and reduce dependency on foreign sources. This can be addressed in section C , paragraph d and as well in section B paragraph 15

C. Co-Development of International Laws and Cyber Global Governance: The APR should recognize the significance of fostering common understandings of how international law applies to ICTs. In this context, co-developing international laws and cyber global governance can be considered as a crucial confidence-building measure. By engaging in cooperative efforts to address cyber threats and challenges, nations can build mutual trust and promote a more secure and stable cyberspace. This can be addressed in section D. This can be addressed in section C , paragraph d and as well in section B paragraph 15

4 . Sovereign Supply Chain: To strengthen global cyber sovereignty, we should encourage the development of independent and sovereign supply chains. Nations must prioritize the research and development of secure technology, reducing dependency on foreign sources for critical ICT infrastructure components.

5. Responsible State Behaviour: The report should highlight the role of technology in fostering responsible state behaviour. Encouraging sovereign R&D development of secure technology is vital for building a foundation of responsible cyber governance based on Rules, Norms, and Principles of Responsible State Behaviour.

Regarding the last suggestion, I wholeheartedly support the idea of sharing national views to foster common understandings of how international law applies in the use of ICTs. The voluntary sharing of national statements and state practices on international law helps create a cohesive global approach to addressing cyber threats. Furthermore, considering relevant studies and opinions of international legal experts will complement the process and contribute to the development of a holistic framework.

By incorporating co-developed emerging threat countering toolkits and automated Points of Contacts, we can foster greater confidence among nations and promote an environment of trust and collaboration. These measures will strengthen our collective resilience against cyber threats and ensure a more coordinated and effective response to emerging challenges.

In conclusion, I kindly request your attention to include these vital elements in the APR. By embracing innovation and cooperation in our approach to cybersecurity, we can build a more secure and prosperous digital future for all.

Thank you for your consideration, and I look forward to your positive response.

Sincerely,

Professor. Hoda Alkhzaimi

EMARATSEC

(Emerging Research and Security Center, NYU/ NYUAD)

New York, AbuDhabi