Outcome report: Safe and Secure Resilient Network Solutions

Session Date and Time: Session 1, Tuesday, 6 July 2021 (06:00 – 07:00 Geneva time). 60 minutes.

Moderator:

- Hon. David Butcher, Executive Director, Civil Service Institute, New Zealand

Speakers:

- Dr. Mamello Thinyane, Principal Research Fellow, United Nations University, Macao, China;
- Mr. Aaron Boyd, Managing Partner, Welchman Keen;
- Ms. Joyce Chen, Senior Advisor – Strategic Engagement, APNIC.

1. **Session summary:** This session presented selected initiatives on using emerging technology for connectivity. The presenters focused on the importance of building resilient and secure digital economies by ensuring governments and private sector stakeholders understand the new risks and develop and execute strategies to mitigate them. The experts elaborated on the challenges and way forward for securing critical infrastructure, strengthening emergency response capabilities, and building cyber resilience.

2. **Main outcomes highlighting the following:**
   a. **Discussed Topics:**
      Cyber Resilience and National Cybersecurity Strategies, Data Privacy and Data Sovereignty, Internet of Communities and Resilience
   b. **Key achievements and challenges shared by the panelists and/or the audience**
      - Lots of risks in the opportunities of emerging technology, including privacy, concentration of power, and digital inequality.
      - Cyber resilience discussions need to look not just at the technology, but also the human element and civil society.
      - UNU research shows that few countries give elaborate framing and operationalization of cyber resilience, and there are limited avenues for citizen co-production of cybersecurity. Citizens are framed as recipients mainly.
      - We need a whole-of-society approach for cyber-resilience, given the multi-dimensionality of the concept and the need for civil society to act as active cybersecurity agents
      - There need to be clear modalities and avenues of engagements for civil society stakeholders. Voluntary cybersecurity actions by citizens are outside the legal framework, so that participation needs to be defined.
      - Data privacy is a challenge in the current world. Data is aggregated and stored in multiple areas, with complications surrounding the question of national data sovereignty.

- Emerging technologies (Blockchain, Artificial Intelligence, Internet of Things, Satellites) will connect more things, but IGOs and NGOs should endeavor to work together to build a trust-but-verify system of data governance that ensures the greatest degree of personal and national data sovereignty while accounting for lawful intercept, legal requirements and a variety of cultural norm.
- International dialogues need to happen on privacy standards. Multinational companies need to ensure trust to rally around open-source standards while addressing privacy and national sovereignty considerations.
- Common forms of cyberattacks include ransomware, malware, phishing, and distributed denial of service attacks. There is also a rise in ransomware and supply chain attacks. The Internet of Things will create a wider possible attack surface.
- Technology is not a panacea. People's habits need to be changed, so an internet of communities needs to be considered. There needs to be a multistakeholder approach to engagement, as capacity building is not just about training, but also about collaborating with each other to form strong support networks.

c. Main conclusions reached during the discussion

- Technology alone is not the solution, but a combined community effort is needed with citizens and users.

-Cross-sectoral collaboration is needed, especially since network is only as strong as your weakest link.

- There is a need to increase awareness of threats and emerging technologies more widely in society.

3. Panelists contributions to the outcome reports

- Getting resilience is about investing in your communities. This is not just specific communities that we think may be critical to the infrastructure, but all kinds of different stakeholders and communities. **Collaboration** is key.
- We can only be as resilient as the weakest sectors of society, so as a society and community, we need to make sure that we **leave no one behind in cybersecurity and cyber resilience.**
- **Trust** is used a great deal in cybersecurity, but in terms of international collaboration and communication systems, trust is incredibly important, because once that trust is broken, it's very difficult to earn it back. In terms of community and international collaboration, building on systems that help bolster and enshrine that trust is going to be important for the future.