# Informal Multi-stakeholder Cyber Dialogue

**EXISTING AND EMERGING THREATS**
**08 December**
**SESSION REPORT**

## GENERAL SUMMARY

The United Nations' Open-ended working group (OEWG) on developments in the field of information and telecommunications in the context of international security is mandated, among other things, to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them.

This session, co-chaired by Indonesia and Australia, aimed to provide an opportunity for the multi-stakeholder community, including civil society, academia, industry and the private sector, to brief UN Member States on existing and emerging cyber threats, with a focus on those most likely to impact international peace and security.

The session attracted a broad participation of 180 people who joined from Zoom and the Livecast representing governments, civil society, academia, and the private sector. The Livecast attracted viewers from 17 countries and 25 cities around the world.

## SESSION OUTLINE

The session opened with introductory remarks from Rolliansyah Soemirat, Director for International Security and Disarmament, Ministry of Foreign Affairs of the Republic of Indonesia and Johanna Weaver, Special Advisor to Australia's Ambassador of Cyber Affairs and Critical Technology, and Head of Delegation to the OEWG and Group of Government Experts, Department of Foreign Affairs and Trade Australia.

The session included civil society, academia and industry presentations from: Jeremy Thompson, Executive Vice President & Deputy Cyber Security Officer Huawei Western Europe; Yihao Lim – Principal Intelligence Enablement Consultant (Asia Pacific) FireEye; Anastasiya Kasakova – Public Affairs Manager Kaspersky; Jessica Woodall – Cyber & National Security Senior Analyst Telstra; Benjamin Ang – Senior Fellow, Cyber and Homeland Defence Programme of CENS Centre of Excellence for National Security, RSIS Singapore; Gunjan Chawla – Programme Manager Centre for Communication Governance National Law University Delhi; John Hering – Senior Government Affairs Manager Microsoft and representative of the Cybersecurity Tech Accord; Maarten Van Horenbeeck – Board Member and former Chairman of the Forum of Incident Response and Security Teams (FIRST), Arindrajit Basu – Research Manager Centre for Internet&Society India, Georgia Turnham and Eric Pinkerton – Trustwave; Stéphane Duguin – CEO CyberPeace Institute; and Paul Meyer – Senior Advisor, ICT4Peace.

A set of guiding questions was distributed in advance in order to inform the contributions of participants. Presenters were asked to address the following questions:

1. What cyber/ICT related activities do you assess to be the biggest threat to international peace and security?

2. With respect to the draft "Existing and Emerging Threats" section of the OEWG pre-draft report, are there any notable omissions, additions, or statements with which you support or disagree?

Presentations were followed by small panel discussions moderated by discussants from: Arina Pazushko – Head of Brand Development BI.ZONE, Farlina Said – Analyst Foreign Policy and Security Studies ISIS Malaysia, Dr Fitriani, CSIS Indonesia.

Presentations and panels were followed by an interactive question and answer session from participants and panellists. All views expressed during the session represented the views of the individuals or organisations who expressed them, and not those of the chairs, sponsors or partners.

## MAJOR THEMES / AREAS OF CONVERGENCE

Presentations were wide-ranging in their assessment of the cyber threat landscape. Themes that cut across several presentations and panel discussions of existing and emerging threats included: the centrality of trust; importance of transparency; risk of escalation and risk of balkanisation; the disproportionality of cyber risk; and the delineation of threats within or outside the mandate of international peace and security.

Presenters and panellists provided the following key points to summarise the session:

- Trust is a key asset in tackling emerging threats in cyberspace
- The ability to respond to threats posed by ICT and cyber developments are restricted by the same difficulties as conventional efforts to maintain peace and stability, and reliant on nation states being transparent about their capabilities, in a time when we are seeing a declining trend in transparency around State cyber policies
- The digitalization of smart devices can escalate the physical threat of malicious cyber activity
- Continued incidents of malicious cyber activity despite deterrence and response efforts
- The escalation of threats from dual-use goods, surveillance technologies, and democratisation of military cyber capabilities could undermine human rights
- The difficulties associated with differentiating between state and non-state actors
- International peace and stability can also be impacted by other related issues:
    - There is a growing concern and need to address the issues of misinformation and access so all people can enjoy the benefits of ICT safely
    - Deep-fake technology can exacerbate the impact of information operations
    - The need to differentiate and distinguish between the development and deployment of offensive cyber capabilities on the one hand, and the varying roles of corporations as non-State actors in the ecosystem as vendors of ICT equipment and services on the other hand.

## RECOMMENDATIONS

Presenters, panellists and participants provided the following recommendations in the course of written or spoken comments and questions during the session. These points do not constitute formal recommendations of the session's chairs, sponsors or partners:

- The building and maintenance of trust in cyberspace should not only focus on states but also on non-state actors, private sector, communities and individual users
- Governments and law-makers should be encouraged to set minimum requirements for cyber security, and create labs and test centres to encourage innovation
- The multi-stakeholder community, including states, should work on global standards for cyber security rather than bifurcate into regional standards
- Measures to promote responsible state behaviour in cyberspace should be accompanied by greater accountability
- The UN should move from general discussion of cyber threats to measures that mitigate or eliminate those threats. In this regard, the "Programme of Action" represents a concrete way forward
- All stakeholders should address the escalation of threats to human rights being undermined in cyberspace
- Further and continuing dialogue including all multi-stakeholders is needed to shed light on current and future threats and promote a collective approach to developing solutions.