DRAFT AGENDA
2nd Inter-Regional Conference on Cyber/ICT Security: Regional Response to Global Challenges

May 1st:

08:30 – 09:00
Registration of the participants

9:00 – 10:00
Taking Stock of the Cyber/ICT Security Environment in Asia and the OSCE Region

Description: The event shall start with opening remarks by the National Host and the OSCE plus a review of the current cyber/ICT security environment.

10:00 – 11:30
Global advancements through (inter-)regional efforts: reflections on how capacity building, norms development and confidence-building measures are developed and how regional organizations translate them into practice

Description: The United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security lays out a four pillar approach that underlines the importance of addressing cyber/ICT security policy challenges from multiple angles. Efforts undertaken by regional organizations in this regard have proven the importance of a systematic co-ordination and collaboration across regions as well as across pillars. This panel seeks to discuss how global and regional efforts undertaken in this realm can reinforce each other and maximize their impact.

11:30 – 11:45
Coffee Break

11:45 – 13:15
Stronger or weaker together? Strategic dimensions of state behavior in cyberspace and its effect on international co-operation

Description: Many governments are operating in cyberspace as they are in other military domains. Some states openly discuss their offensive cyber capabilities, others stress the importance of reducing vulnerabilities and focusing on defensive measures. This panel seeks to stimulate a discussion about states' strategic view on cyber/information space in a time of increasing inter-state tensions and reduced international co-operation.

2nd Inter-Regional Conference on Cyber/ICT Security: Regional Response to Global Challenges

13:15 – 14:15
Lunch Break

14:15 – 15:45
Securing Critical Infrastructures – What is the government's role and how does effective Public Private Partnership look like?

Description: Critical infrastructures form the backbone of national economies and systems of government by ensuring the timely and seamless circulation of energy, information, goods, services and other necessities. This also makes them a prime target for threats stemming from cyberspace, and an important consideration for policy and decision makers dealing with cyber/ICT security and resilience. During the session, the panelists will discuss national and international efforts and good practices, for enhancing the protection of critical infrastructure, the role that different sectors can play.

15:45 – 16:00
Coffee Break

16:00 – 17:30
Inter-regional best practice exchange on national incident classification systems – toward greater intercompatibility?

Description: States regularly classify cyber/ICT security incidents based on its severity, impact, urgency, and other parameters. While this can be observed as an entirely technical procedure, political considerations are becoming increasingly relevant when classifying cyber/ICT security incidents. This panel seeks to foster an exchange on national best practices across regions as well as stimulate a discussion toward internationally comparable classification schemata.

18:00
Light Reception

2nd Inter-Regional Conference on Cyber/ICT Security: Regional Response to Global Challenges

May 2nd:

9:00 – 11:00
New frontiers: how technical advancements will shape the international cyber/ICT security policy and legal landscape

Description: While existing rules and regulations continue to provide a framework for technology companies for their operations, technological advancements will continue to outpace policy developments. This inherent challenge is also an opportunity to revisit how technology, policy and law interacts and shapes each other. This panel seeks to clarify how this interconnectedness can be properly understood in the context of cyber/ICT security and how policy-makers can technology developers can best collaborate with each other.

11:00 – 11:15
Coffee Break

11:15 – 12:45
Looking ahead – Review of the most pressing cyber/ICT security policy challenges for international organizations

Description: The cyber/ICT security policy landscape is constantly changing and effected by new technological advancements such as Artificial Intelligence. Moreover, several issues such as rules of responsible state behavior or confidence-building measures have been part of negotiations for many years and discussions are now also shifting toward implementation of those agreements. Based on the decision to create a new United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) and also an United Nations Open-Ended Working Group (UN OEWG) on the same matter, this panel seeks to discuss which issues need to be addressed by policy-makers and international organizations in the years to come.

12:45 – 13:15
Closing Remarks