Telecommunication
Development Bureau (BDT)

Ref.: BDT/DDR/EUR/DM/014 Geneva, 25 September 2023

- Administrations of ITU Member States of the Europe & Asia and the Pacific Regions
- Regulators of the Europe & Asia and the Pacific Regions
- ITU-D Sector Members of the Europe & Asia and the Pacific Regions
- Academia of the Europe & Asia and the Pacific Regions
- Regional Organizations of the Europe & Asia and the Pacific Regions

Subject: **ITU Europe & Asia-Pacific Interregional CyberDrill, Limassol, Cyprus, 28 November - 1 December 2023**

Dear Sir/Madam,

I am pleased to invite you to participate in the **ITU Europe & Asia-Pacific Interregional CyberDrill** to be held from 28 **November to 1 December 2023**, in Limassol, Cyprus.

This event is organized by the Telecommunication Development Bureau (BDT) of the International Telecommunication Union (ITU) and hosted by the Digital Security Authority of Cyprus within the framework of the ITU Regional Initiative for Europe on Trust, and confidence in the use of telecommunications/ICT's and the ITU Regional Initiative for Asia and the Pacific on Contributing to a secure and resilient information and communication technology environment, as agreed by 2022 World Telecommunication Development Conference (WTDC-22).

The ITU Europe & Asia-Pacific Interregional CyberDrill shall enhance communication and incident response capabilities of the participating teams as well as to ensure a continued collective and collaborative effort in mitigating cyber threats among Europe and Asia-Pacific Computer Security Incident Response Teams (CSIRTs).

The CyberDrill is available to CSIRTs, ministries, regulators, telecommunication operators, universities, general education institutions, telecommunication equipment manufacturers, research and design institutes, software developers, and other stakeholders from ITU Member States, Sector Members, and Associates.

The first day is dedicated to the Interregional Forum on Critical Information Infrastructure Protection and the Role of National CSIRTs in Ensuring Cyber Resilience. This event will bring together decision-makers and ICT professionals in government, industry, academia, and NGOs. Its purpose is to facilitate the exchange of ideas, fostering the enhancement of cybersecurity and resilience within both regions.

Shifting focus to the subsequent day, the agenda centres on technical capacity-building training on CSIRTs management.

The last two days will be dedicated to CyberDrill exercises, structured around a variety of scenarios that involve emerging types of cyberattacks. Additionally, the sharing sessions will provide a platform for participants from Europe and the Asia-Pacific to collaborate, deliberate, and advance cross-learning opportunities pertaining to cybersecurity issues.

Considering the practical nature of the event, I encourage participation of teams from Europe and Asia-Pacific, comprising a minimum of two members of your national CSIRT, accompanied by a senior cybersecurity manager. This team structure will allow you to gain maximum benefit from the cyber threat simulations and CyberDrills that are crucial components of the event. Please note that this event will be held in a paperless format. All relevant documents, such as the event agenda, registration form, and practical information for participants, can be accessed on the ITU website at http://itu.int/go/CyberDrill-EUR-ASP23. We encourage all participants to download the necessary documents prior to the event.

It is recommended for participants to initiate their visa applications for Cyprus at the nearest Embassy or Consulate as soon as possible to facilitate a seamless process. The visa approval procedure can take several days, and participants may be required to present an invitation letter from the local host to the Cyprus Embassy/Consulate in their respective countries.

While this event does not require a participation fee, please note that all travel, accommodation, and insurance expenses for your representatives must be borne by your administration, organization.

Should you need further information or assistance, please do not hesitate to reach out to Ms. Valentina Stadnic, ITU Regional Office for Europe (valentina.stadnic@itu.int, with eurregion@itu.int in copy) and Mr. Calvin Chan, ITU Regional Office for Asia and the Pacific (calvin.chan@itu.int). They are at your full disposal for any questions you might have concerning this event.

I look forward to your valuable participation and contributions to this interregional event.

Yours faithfully,

Cosmas Luckyson Zavazava
Director

ITU Asia-Pacific & Europe Interregional CyberDrill, Limassol, Cyprus

28 November - 1 December 2023

DRAFT AGENDA

DAY 1: ITU INTERREGIONAL FORUM on Critical Information Infrastructure Protection and the Role of National CSIRTs in Ensuring Cyber Resilience

Tuesday 28 November 2023

[08:00 – 09:00]	Registration
[09:00– 09:30]	**Opening Ceremony**
[09:30 – 10:00]	Coffee Break and Group Photo
[10:00 – 11:20]	**Session 1: State of Cybersecurity in Asia Pacific and Europe regions:** The session will c into the rapid acceleration and increased digitalization spanning various sectors. trajectory of growth and inclusion has exposed the new cyber threats due to expanding a surface. Given the shared experiences of Europe and Asia-Pacific in contending with s sponsored cyber-attacks the ongoing efforts to strengthen regulations such as data prote Through illustrative examples, it will outline the robustness of cybersecurity framew within their respective geographies.
[11:20 – 12:40]	**Session 2: Best practices for Critical Information Infrastructure Protection:** The session discuss the multiplying effect of cyber threats across critical infrastructure and how incre digitalization and dataflow are evolving the cyber risks to society and economy. The ses shall present case-studies from Europe and Asia-Pacific and analyze interregional les learnt and engage in discussions to address region specific concerns and challenges in cr information infrastructure protection.
[12:40 – 14:00]	Lunch Break
[14:00 – 15:00]	**Session 3: National Cyber Crisis Response Plan, facing new threats - Intersec coordination with national impact**: As cyber threats escalate in both scale and complexi is imperative for nations to develop dynamic response mechanisms to protect their d ecosystems. This panel will explore the detailed components of a National Cyber (Response Plan, highlighting the crucial role of intersectoral coordination. Representa from diverse sectors will discuss how industries, government agencies, and other stakeho can collaborate effectively to tackle cyber crises that have national implications.
[15:00 – 15:30]	**Session 4: The Role of Partnerships in Advancing Cyber Diplomacy:** In today's interconne digital landscape, cyber threats are not confined by borders, nor are their repercuss limited to a single nation. It is in this context that cyber diplomacy – the stra communication and negotiation between states in the digital realm – gains unparal importance. This panel delves into the pivotal role of partnerships in fortifying and advar the cause of cyber diplomacy.
[15:30 – 16:00]	Coffee Break

[16:00 – 17:20]	**Session 5: Opportunities of Light Version FIDO (ITU-T Standards X.1277 (Universal Authentication Framework) and X.1278 (Client to Authenticator Protocol/Universal 2-Factor Framework):** The session will provide a concise overview of FIDO and the significance of its light version for improved authentication. The discussion will focus on the key principles and components, identifying potential areas for collaboration and standardization between Europe and Asia-Pacific, while promoting partnerships among industry stakeholders.
[17:20 – 17:30]	**Closing remarks**

DAY 2: TRAININGS

Wednesday 29 November 2023

08:00 – 09:00	Registration	Registration
09:00– 09:30	**Training Track I: FIRST**	**Training Track II: UNCCT**
09:30–10:00	Coffee Break	
10:00–11:00	**Training Track I: FIRST**	**Training Track II: UNCCT**
11:00–11:30	Coffee Break	
11:30–12:30	**Training Track I: FIRST**	**Training Track II: UNCCT**
12:30–13:30	Lunch Break	
13:30–16:00	**Training Track I: FIRST**	**Training Track II: UNCCT**

DAY 3 and 4: CYBER EXERCISES

Thursday 30 November 2023

09:00–09:30	Team creation, registering team accounts to Cyber Range
09:30–11:00	**Scenario 1**
11:00–11:30	Coffee Break
11:30–12:30	**Scenario 1**
12:30–13:30	Lunch Break

13:30–14:30	**Scenario 2**
14:30–15:00	Coffee Break
15:00–16:00	**Scenario 2**

Friday 1 December 2023

09:00–09:30	Registration
09:30–11:00	**Scenario 3**
11:00–11:30	Coffee Break
11:30–12:30	**Scenario 3**
12:30–13:30	Lunch Break
13:30–14:30	**Scenario 4**
14:30–15:00	Coffee Break
15:00–16:00	**Scenario 4**