COMMISSIONER OF COMMUNICATIONS | Digital Security Authority

NATIONAL CSIRT-CY

ITU

2023 Interregional CyberDrill

for Europe and Asia-Pacific

28 November – 1 December 2023, Limassol, Cyprus

DAY 1: ITU INTERREGIONAL FORUM

on Critical Information Infrastructure Protection and the Role of National CSIRTs in Ensuring Cyber Resilience

Overall moderation/master of ceremony:

- Ms. Valentina Stadnic, ITU Office for Europe
- Ms. Natalia Spinu, Event coordinator

Tuesday 28th November 2023 (GMT+2, Cyprus Local Time)

08:00 – 09:00 Registration

09:00– 09:40 **Opening Segment**

Opening Statements

- Mr. **George MICHAELIDES,** Commissioner of Communications, Regulator for Network and Information Security (NIS) for Critical Information Infrastructures (CIIs), Cyprus
- H.E. Mr. **Philippos HADJIZACHARIAS,** Deputy Minister of Research, Innovation and Digital Policy in Cyprus
- Dr. **Cosmas Luckyson ZAVAZAVA**, Director of the Telecommunication Development Bureau (BDT) at the International Telecommunication Union (ITU)

Regional Context

- Ms. **Atsuko OKUDA,** Regional Director of the ITU Regional Office for Asia and the Pacific
- Mr. **Jaroslaw PONDER**, Head of the ITU Office for Europe

09:40 – 10:00 Coffee Break and Group Photo

10:00 – 11:45 **Session 1: State of Cybersecurity in Asia Pacific and Europe regions:** The session will delve into the rapid acceleration and increased digitalization spanning various sectors. This trajectory of growth and inclusion has exposed the new cyber threats due to expanding attack surface. Highlighting the shared experiences of Europe and the Asia-Pacific region in addressing cyber-attacks, this discussion will focus on ongoing efforts to enhance regulations, particularly in the realm of data protection. Through illustrative examples, it will outline the effectiveness of cybersecurity frameworks within their respective geographies.

Setting the Context: Mr. **Jaroslaw PONDER**, Head of the ITU Office for Europe

Speakers:

- H.E. Mr. **Tadeusz CHOMICKI**, Ambassador for Cyber and Tech Affairs, Ministry of Foreign Affairs of Poland
- Mr. **Luke HO**, Deputy Director of the National Cyber Threat Analysis Centre, Cyber Security Agency of Singapore
- Mr. **Jitendra PRAKASH**, Director, Security, Department of Telecommunications, India
- Mrs. **Liliana MUSETAN**, Head of Unit, Council of the European Union
- Mr. **Apostolos MALATRAS**, Team Leader, Knowledge and Information, European Union Agency for Cybersecurity
- Mr. **Zdravko JUKIĆ**, Deputy Executive Director, HAKOM, Co-Chair of BEREC Cybersecurity Working Group
- Mr. **Arthur Glenn MAAIL,** Senior Officer of Digital Economy, ASEAN Secretariat

---

11:45 – 13:15 **Session 2: Best practices for Critical Information Infrastructure Protection:** The session shall discuss the multiplying effects of cyber threats across critical infrastructure, and how increased digitalization and dataflow are evolving cyber risks to society and economy. The session shall present case-studies from Europe and Asia-Pacific, and analyze interregional

lessons learnt, and engage in discussions to address region specific concerns and challenges in critical information infrastructure protection.

Setting the Context and Moderation: Ms. **Yiota NICOLAIDOU,** Holistic Security Strategist, Safety Critical Infrastructures Adviser, Cyber Security Assurance Lead – NTT Data

Speakers:

- Mr. **Rexhion QAFA**, Director, Cybersecurity Analysis Directorate, Director of the National CSIRT, Albania
- Mr. **Ahmed Bakht MASOOD**, Director (Cyber Security), Pakistan Telecom Authority
- Mr. **Chalermchai WONGGATE,** Director of Critical Information Infrastructure Management Office, National Cyber Security Agency, Thailand
- Ms. **Marinela LAZAREVIC,** Head of Department for Electronic Communications and Radio Spectrum, Ministry of Economic Development and Tourism, Government of Montenegro
- Mr. **Daniel EHRENREICH**, Trainer at Secure Communications and Control Experts (SCCE), Israel
- Mr. **Florian PENNINGS,** Director EU Government Affairs – Cybersecurity, Microsoft, Brussels, Belgium

---

13:15 – 14:15 Lunch Break

14:15 – 15:45 **Session 3: National Cyber Crisis Response Plan, facing new threats - Intersectoral coordination with national impact**: As cyber threats escalate in both scale and complexity, it is imperative for nations to develop dynamic response mechanisms to protect their digital ecosystems. This panel will explore the detailed components of a National Cyber Crisis Response Plan, highlighting the crucial role of intersectoral coordination. Representatives from diverse sectors will discuss how industries, government agencies, and other stakeholders can collaborate effectively to tackle cyber crises that have national implications.

Setting the Context and Moderation: Mr. **Calvin CHAN,** Programme Administrator for the ITU's Regional Office for Asia, Bangkok, Thailand

Speakers:

- Mr. **Alexandru COREȚCHI**, Director, Information Technology and Cyber Security Service, Republic of Moldova
- Mr. **Mihajlo ANDREJIC**, Head of Department for System Implementation and Information Security at the Office for Information Technologies and e-Government, Government of the Republic of Serbia
- Ms. **Fonoti Fiapaipai SAKUMA**, Principal, Samoa Computer Emergency Response Team, Ministry of Communications & Information Technology, Samoa
- Ms. **Pratima PRADHAN**, Deputy Chief ICT Officer, Bhutan Computer Incident Response Team, Cybersecurity Division, Government Technology Agency, Bhutan
- Ms. **Biljana JOVANOVSKA BALESKI**, Agency for Electronic Communications, National Centre for Computer Incident Response-MKD-CIRT, North Macedonia

---

15:45 – 16:00 **Coffee Break**

16:00 – 17:30 **Session 4: The Role of Partnerships in Advancing Cyber Diplomacy:** In today's interconnected digital landscape, cyber threats are not confined by borders, nor are their repercussions limited to a single nation. It is in this context that cyber diplomacy – the strategic communication and negotiation between states in the digital realm – gains unparalleled importance. This panel delves into the pivotal role of partnerships in fortifying and advancing the cause of cyber diplomacy.

Setting the Context and Moderation: Ms. **Natalia Spinu**, Director, European Institute for Political Studies, Republic of Moldova

Speakers:

- H.E. Mr. **Tanel SEPP,** Ambassador at Large and Director-General for the Cyber Diplomacy Department, Ministry of Foreign Affairs of the Republic of Estonia

- Mr. **Ampuan Shazwi AMPUAN SADIKIN,** Senior Operations Officer, Cyber Security Brunei
- Mr. **Wojciech BEREZOWSKI**, Cybersecurity Counsellor in the Ministry of Digital Affairs of Poland, CEPT Com-ITU ViceChair, ITU Council Working Group on Internet Chair
- Dr. **Andreja MIHAILOVIC**, Teaching Associate at the Faculty of Law, University of Montenegro, President of Women4Cyber Montenegro
- Ms. **Philomena GNANAPRAGASAM**, Director, Asia-Pacific Institute for Broadcasting Development (AIBD), Kuala Lumpur, Malaysia

17:30 – 17:45	**Closing remarks**

DAY 2: TRAININGS

Wednesday 29th November 2023

Management Track
Title: **Cyber Diplomacy**
Instuctors: Dr. **Carmen Elena CIRNU**, PhD, Scientific Director & Cyber Diplomacy Center Coordinator
Dr. **Alexandru GEORGESCU**, PhD, Senior Researcher Cyber Diplomacy Center
National Institute for Research and Development in Informatics ICI Bucharest
Technical Track
Title**: Threat intel Pipelines**
Instructor: Mr. **Jarosław JEDYNAK**, Cybersecurity Expert, FIRST

09:00-09:30	**Registration**	
09:30 – 10:00	**Opportunities of Engaging with ITU Standards in Cybersecurity** The discussion will focus on the key principles and components of ITU-T standards on cybersecurity. It will identify potential areas for collaboration and standardization between Europe and Asia-Pacific, while promoting partnerships among industry stakeholders. Professor **Heung Youl YOUM**, Chairman, ITU-T Study Group 17, Security I Professor, Department of Information Security Engineering, Soonchunhyang University, Republic of Korea.	
10:00– 10:30	**Training: Technical Track** Threat intel Pipelines FIRST	**Training: Management Track** Cyber Diplomacy ICI Bucharest
10:30–10:45	Coffee Break	
10:45–12:30	**Training: Technical Track** Threat intel Pipelines FIRST	**Training: Management Track** Cyber Diplomacy ICI Bucharest
12:30–13:30	Lunch Break	
13:30–15:00	**Training: Technical Track** Threat intel Pipelines FIRST	**Training: Management Track** Cyber Diplomacy ICI Bucharest
15:00–15:15	Coffee Break	

15:15–16:30	**Training: Technical Track** Threat intel Pipelines FIRST	**Training: Management Track** Cyber Diplomacy ICI Bucharest

DAY 3 and 4: CYBER EXERCISES

Thursday 30th November 2023

08:30-09:00	**Registration**
09:00–09:30	Team creation, registering team accounts to Cyber Range
09:30–11:30	**Scenario 1: Cyber Threat Intelligence** Mr. **Jarosław JEDYNAK**, Cybersecurity Expert , FIRST
11:30–11:45	Coffee Break
11:45–12:45	**Technical workshop:** Dark Web Investigation Ms. **Selene GIUPPONI**, Secretary General of Women4Cyber Italy Chapter
12:45–13:45	Lunch Break
13:45–15:45	**Scenario 2: "Winter Vivern" - Blue Team Exercise** Mr. **Alexandros CHRISTOFI,** Digital Security Authority, Cyprus Mr. **Andreas MAKRIS,** Digital Security Authority, Cyprus Mr. **Stelios TRIKOS,** Digital Security Authority, Cyprus
15:45–16:00	Coffee Break
16:00–17:00	**Technical workshop:** Predictive & Proactive Threat Management

Friday 1st December 2023

09:00–11:00	**Scenario 3: DFIR for APT Security Incident** Mr. **Marwan Ben RACHED**, Cybersecurity Coordinator, ITU
11:00–11:15	Coffee Break
11:15–12:15	**Technical workshop:** Open-Source Intelligence (OSINT) Mrs. **Selene GIUPPONI**, Secretary General of Women4Cyber Italy Chapter
12:15–13:15	Lunch Break
13:15–15:15	**Scenario 4: Silverthorn Power Plant Attack** Mr. **George NICOLAOU**, Co-Founder, Head of Research and Innovation at CYBER RANGES, Limassol, Cyprus

15:15–15:30	**Closing remarks**
15:30–16:00	Networking Coffee