Council of the European Union
General Secretariat

Brussels, 27 October 2021

WK 12891/2021 INIT

LIMITE

CYBER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	Cyber Diplomacy Toolbox exercise concept - presentation

Delegations will find in Annex the EEAS slides on the Cyber Diplomacy Toolbox exercise.

European Union
EXTERNAL ACTION

Cyber Diplomacy Toolbox Table-top Exercise (CyDipTTX 2021) concept

Horizontal Working Party on Cyber Issues
27 October 2021

Content

- General information
- Focus
- Objectives
- Participants
- Preparation
- Conduct

General information

- Date/time: 17 November 2021, all day in-person event
- Name: Cyber Diplomacy Toolbox Table Top Exercise (CyDip2021)
- Place: Justus Lipsius building (meeting room TBD)

Focus

- Exchange of information on situation assessment
- Options for joint diplomatic response to malicious cyber activities against MS and EUIBAs

Objectives

- Promoting awareness on and practicing of Cyber Diplomacy Toolbox (CDT) procedures

- Stimulating discussions on potential update of CDT implementing guidelines

- Promoting synergies and awareness between relevant cybersecurity actors (EU INTCEN, CERT-EU, Europol, ENISA, CSIRT Network, CyCLONe, IPCR)

- Inform PSC discussion on Article 42(7) from cyber perspective

- Contribute to upcoming exercises

Participants

- Facilitator: person leading the exercise
- Training audience (players): MS delegates to HWPCI
- Contributors: representatives of EU INTCEN, CERT-EU, Europol, ENISA, CSIRT Network, CyCLONe, IPCR (providing information on their actions in accordance with scenario, but not playing)
- Observers: guests, no specific role (EDA, EUMS, DG CNECT, DG DIGIT, DG HOME)

Preparation

- Scenario
  - Large-scale cyber attacks on MS and EUIBAs
  - Under threshold of armed attack
  - Additional inject - potential terrorist attack or man-made disaster situation
- Information package (scenario, guiding questions, brief general information on INTCEN, CERT-EU, EUROPOL, ENISA, CSIRT Network, CyCLONe, IPCR with respect to cyber crisis management)
- Distribution of information package (a week before the exercise)

Conduct

- AM session:
  - opening
  - introduction to scenario and rules
  - contributors information
- PM session:
  - Part 1: discussion on the main scenario
  - Part 2: discussion on additional inject
  - First impression and closing

Thank you for your attention
Questions?