Brussels, 15 November 2019

WK 12988/2019 INIT

LIMITE

CYBER

WORKING PAPER

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

WORKING DOCUMENT

From: General Secretariat of the Council
To: Delegations
Subject: CYBER DIPLO TTX 19

Delegations will find in Annex a power point presentation on the above-mentioned subject given by the EEAS in the Horizontal Working Party on cyber issues on 7 November 2019.
AGENDA

10h00-10h05  Welcome and opening
10h05-10h20  State of play "cyber diplomacy toolbox", EEAS
10h20-10h35  Situational Awareness, INTCEN
10h35-10h50  The Blueprint, DG CONNECT
10h50-11h10  National good practices by Member States
11h10-11h30  Coffee break
11h30-13h00  Introduction to the CYBER DIPLO TTX19: Rules of the game
13h00-14h30  Phase 1: Member States' perception
14h30-15h30  Lunch break
15h30-16h45  Phase 2: Situational Awareness discussion
16h45-17h00  Phase 3: Decision making
17h00-17h10  Closing remarks
DELETED
DELETED
Introduction to the CYBER DIPLO TTX19

• *Introduction by the Finnish Presidency of the Council of the EU*

• Geopolitical settings

• Phase I: Member States' initial national perceptions

• Phase II: Situational awareness discussion

• Phase III: Decision making
DELETED
DELETED
PHASE I: Member States' initial national perceptions

Open discussion among MSs on their initial perceptions ONLY following the cyber incidents to be presented by the moderator.
DELETED
PHASE II: Situational awareness discussion

Debate on establishing shared situational awareness, first with Agencies (ENISA, CERT-EU, EUROPOL, CSIRT) contributing to shared situational awareness and then with MSs on the cyber incidents.

Opened and led by INTCEEN and supported by the moderator.
DELETED
DELETED
PHASE III: Decision making

The HWPCI, chaired by the Presidency, plays the "game" of a HWPCI as if it was called for, to discuss the cyber situation presented in the initial scenario.

MSs are invited to use:
• the general information on the scenario presented in Phase I and II,
• the INTCEN report
• and any other individual information that might have received ahead

MSs are expected to respond to malicious cyber activities and prepare a decision of invoking the measures as part of a proportionate EU response.

Observers will be invited to contribute to the discussion.
PHASE III: HWP-Cyber Table Top Exercise