Council of the European Union
General Secretariat

Brussels, 15 November 2019

WK 12987/2019 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: Commission contribution on the Blueprint - European coordinated response to large-scale cybersecurity incidents and crises

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

Blueprint

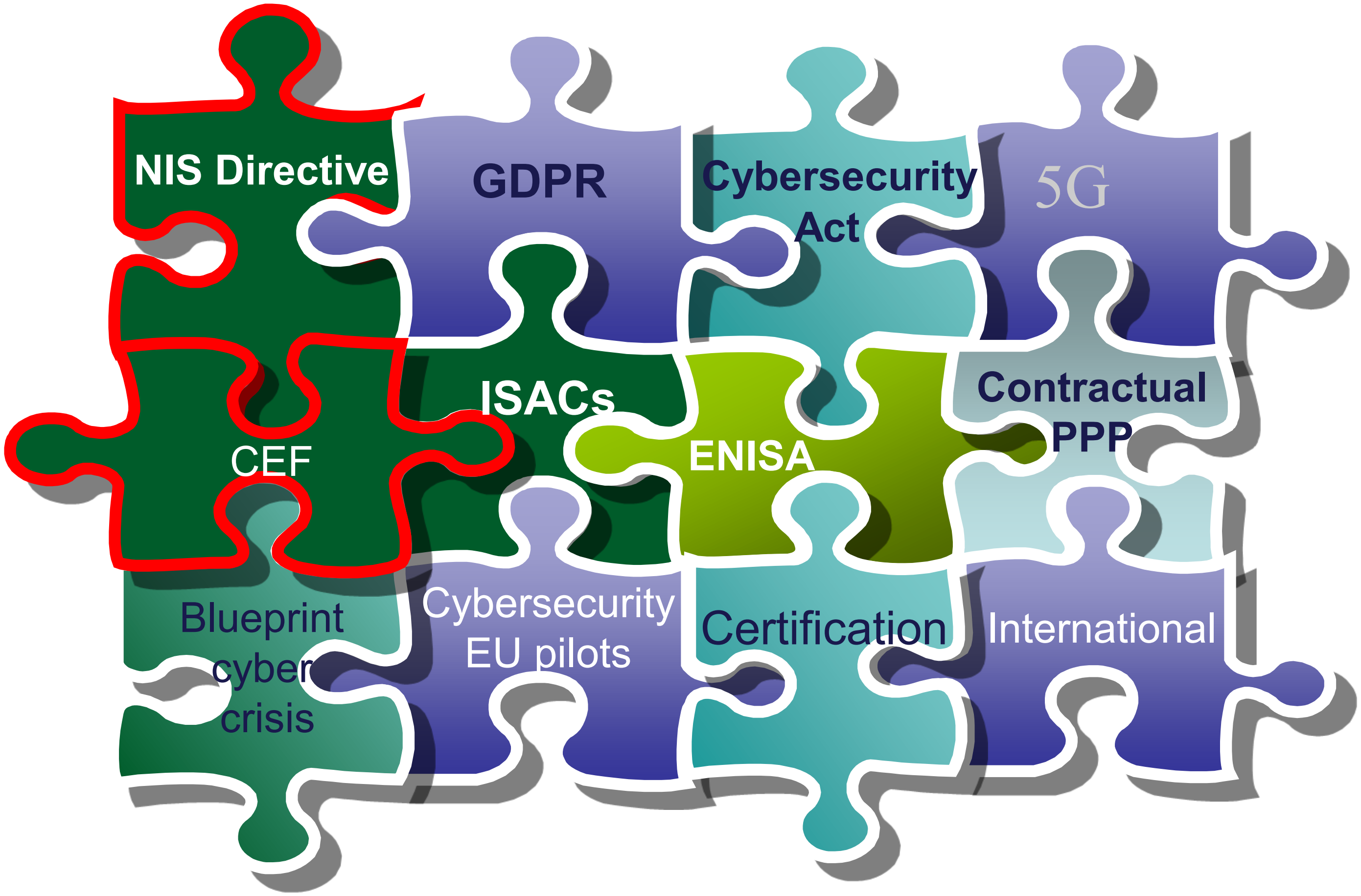
European coordinated response to large-scale cybersecurity incidents and crises

CYBER DIPLOMACY TOOLBOX TABLE TOP EXCERCISE

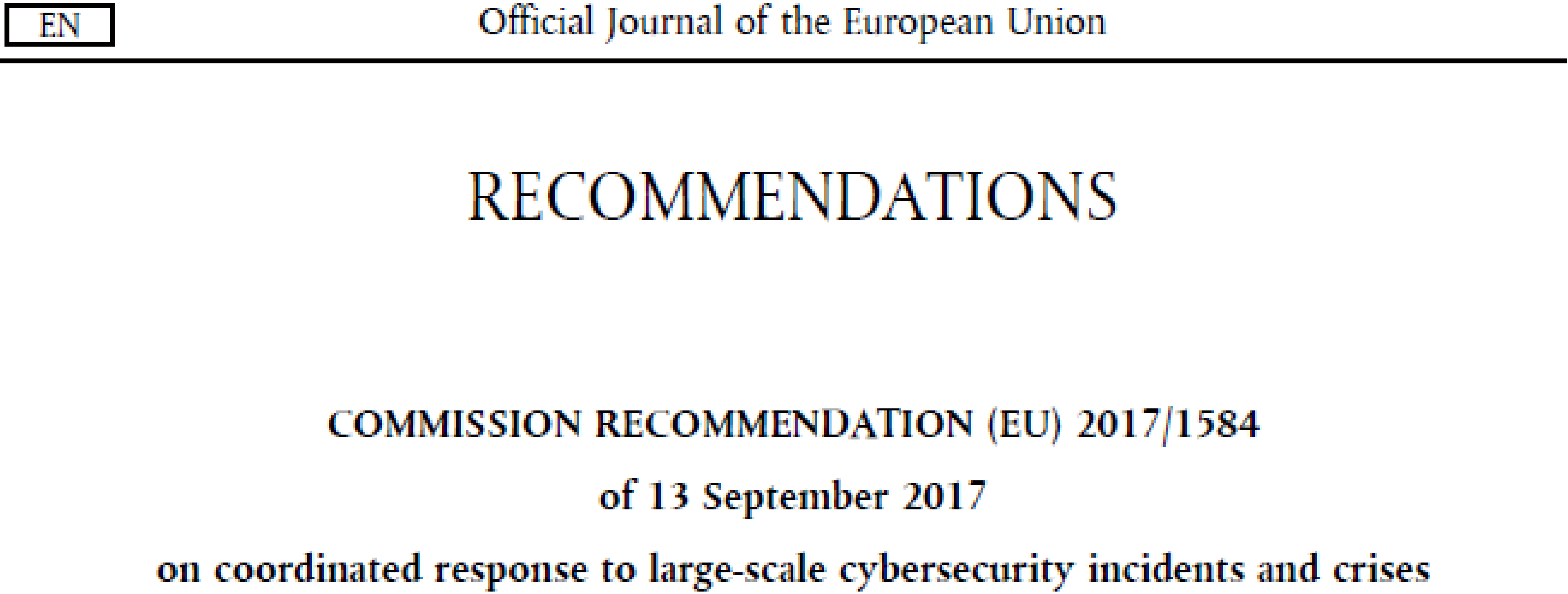
Brussels, 7 November 2019

James Caffrey
Cybersecurity Policy Officer
Unit H1: Cybersecurity Technology & Capacity Building
Directorate H: Digital Society, Trust and Cybersecurity
Directorate General for Communication Networks, Content & Technology
DG CONNECT
European Commission

EU action in cybersecurity



Blueprint



EN — Official Journal of the European Union

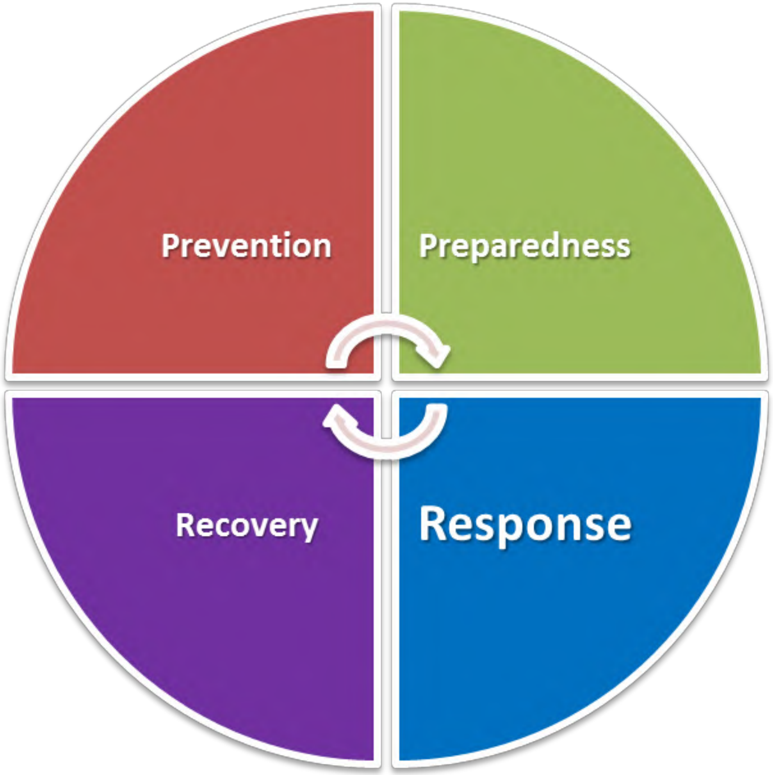
RECOMMENDATIONS

COMMISSION RECOMMENDATION (EU) 2017/1584

of 13 September 2017

on coordinated response to large-scale cybersecurity incidents and crises

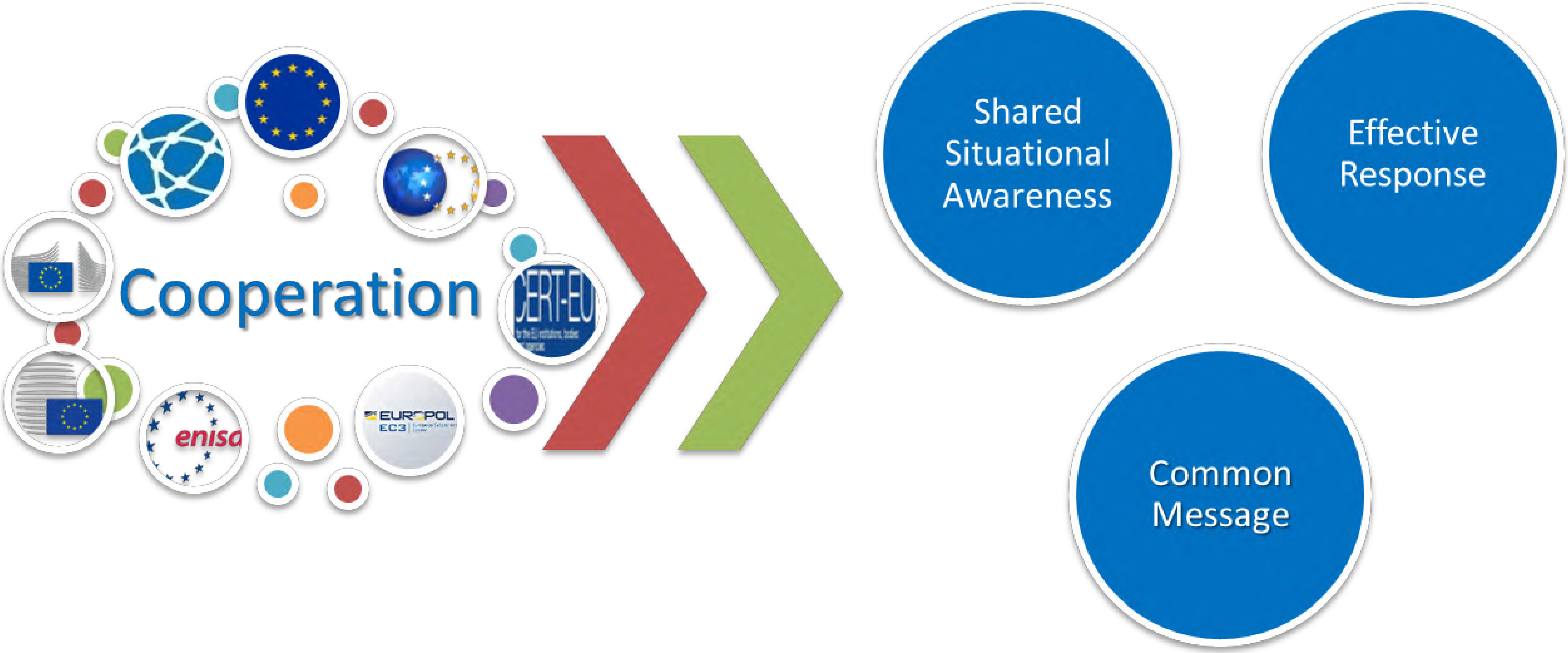
Blueprint - Response



Definition: large-scale cybersecurity incidents and crises

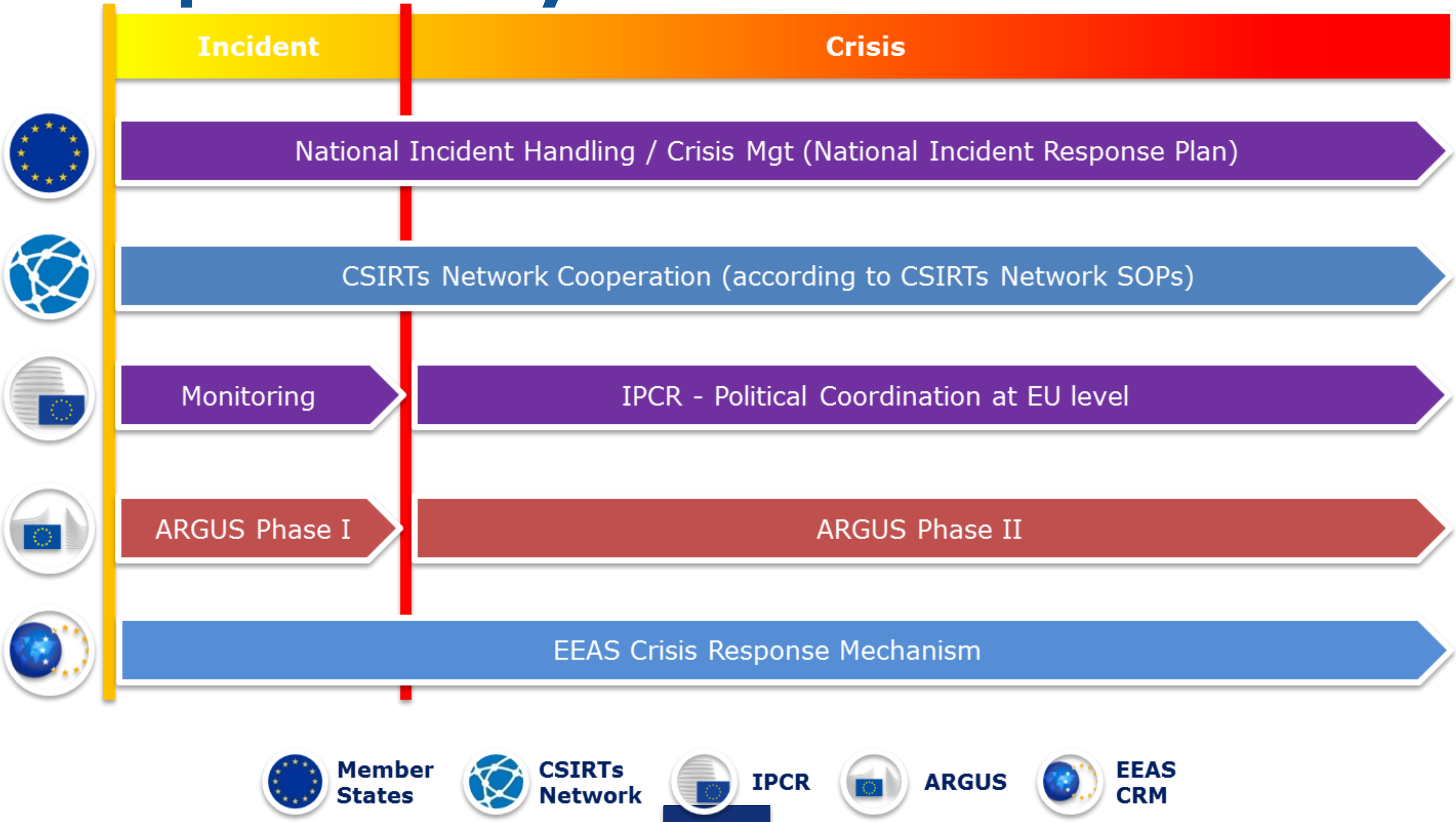
- incidents which cause disruption too extensive for a concerned Member State to handle on its own or which affect two or more Member States or EU institutions with such a wide-ranging and significant impact of technical or political significance that they require timely policy coordination and response at Union political level

Blueprint – core objectives



European
Commission

Blueprint – key mechanisms



Incident

Crisis

National Incident Handling / Crisis Mgt (National Incident Response Plan)

CSIRTs Network Cooperation (according to CSIRTs Network SOPs)

Monitoring

IPCR - Political Coordination at EU level

ARGUS Phase I

ARGUS Phase II

EEAS Crisis Response Mechanism

Member States

CSIRTs Network

IPCR

ARGUS

EEAS CRM

Blueprint – Cooperation at all levels

Technical

- Incident handling during a cybersecurity crisis.
- Monitoring and surveillance of incident including continuous analysis of threats and risk.

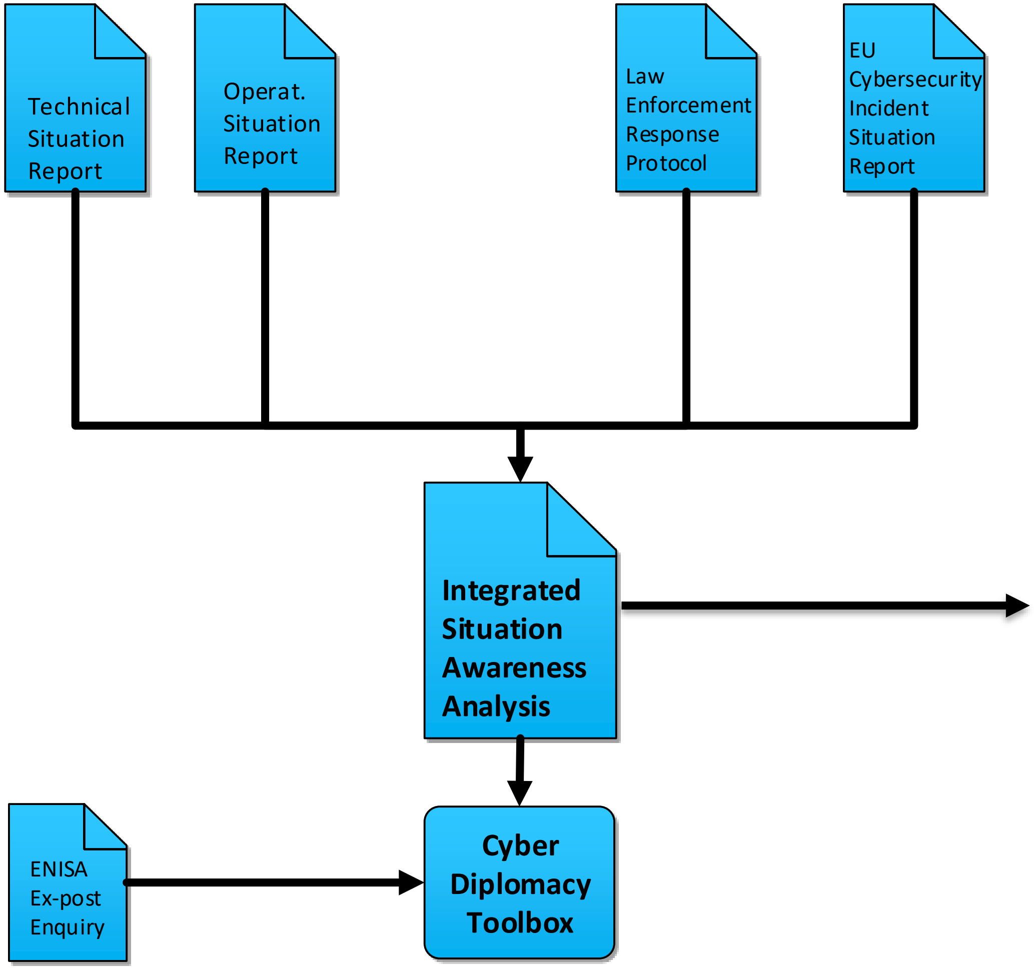
Operational

- Preparing decision-making at the political level.
- Coordinate the management of the cybersecurity crisis (as appropriate).
- Assess the consequences and impact at EU level and propose possible mitigating actions.

Political / Strategic

- Strategic and political management of both cyber and non-cyber aspects of the crisis including measures under the **Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities**

Blueprint – as a Political Decision support mechanism



Technical Situation Report

Operat. Situation Report

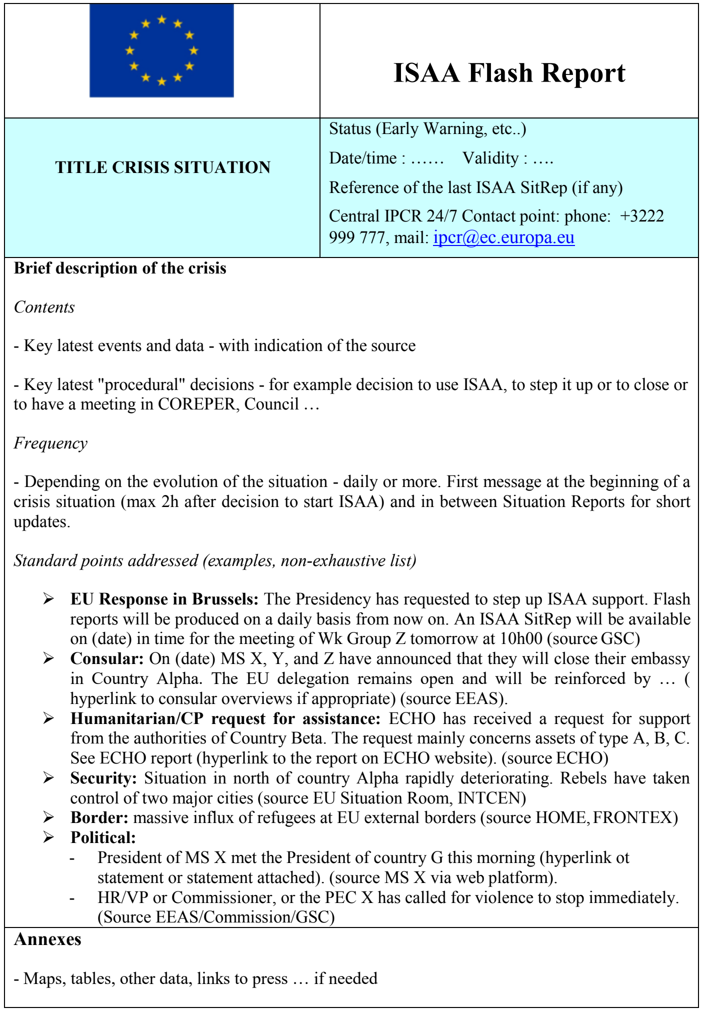
Law Enforcement Response Protocol

EU Cybersecurity Incident Situation Report

Integrated Situation Awareness Analysis

ENISA Ex-post Enquiry

Cyber Diplomacy Toolbox



	ISAA Flash Report
TITLE CRISIS SITUATION	Status (Early Warning, etc..) Date/time : …… Validity : …. Reference of the last ISAA SitRep (if any) Central IPCR 24/7 Contact point: phone: +3222 999 777, mail: ipcr@ec.europa.eu

Brief description of the crisis

Contents

- Key latest events and data - with indication of the source

- Key latest "procedural" decisions - for example decision to use ISAA, to step it up or to close or to have a meeting in COREPER, Council …

Frequency

- Depending on the evolution of the situation - daily or more. First message at the beginning of a crisis situation (max 2h after decision to start ISAA) and in between Situation Reports for short updates.

Standard points addressed (examples, non-exhaustive list)

➢ **EU Response in Brussels:** The Presidency has requested to step up ISAA support. Flash reports will be produced on a daily basis from now on. An ISAA SitRep will be available on (date) in time for the meeting of Wk Group Z tomorrow at 10h00 (source GSC)

➢ **Consular:** On (date) MS X, Y, and Z have announced that they will close their embassy in Country Alpha. The EU delegation remains open and will be reinforced by … (hyperlink to consular overviews if appropriate) (source EEAS).

➢ **Humanitarian/CP request for assistance:** ECHO has received a request for support from the authorities of Country Beta. The request mainly concerns assets of type A, B, C. See ECHO report (hyperlink to the report on ECHO website). (source ECHO)

➢ **Security:** Situation in north of country Alpha rapidly deteriorating. Rebels have taken control of two major cities (source EU Situation Room, INTCEN)

➢ **Border:** massive influx of refugees at EU external borders (source HOME, FRONTEX)

➢ **Political:**

- President of MS X met the President of country G this morning (hyperlink ot statement or statement attached). (source MS X via web platform).
- HR/VP or Commissioner, or the PEC X has called for violence to stop immediately. (Source EEAS/Commission/GSC)

Annexes

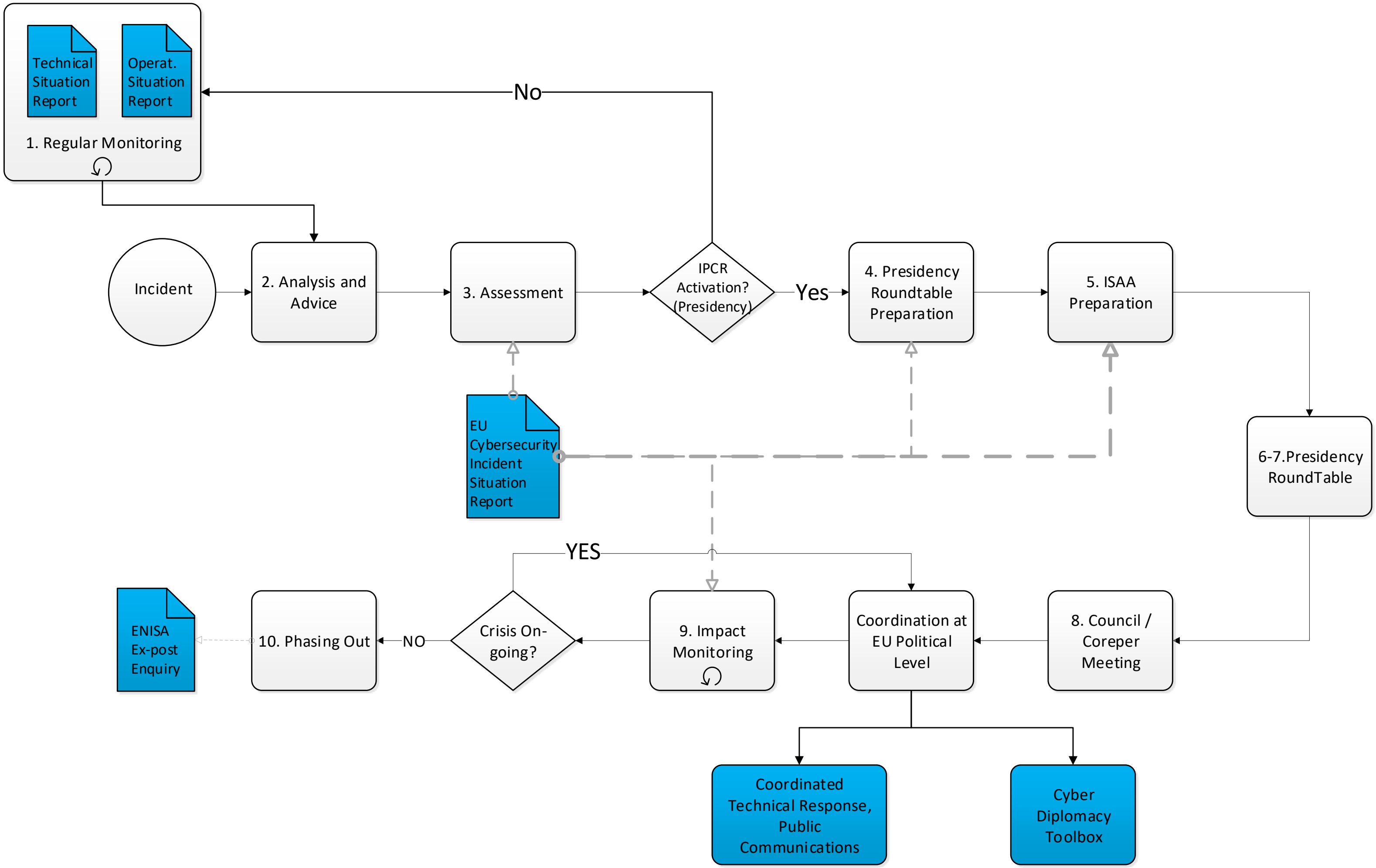
- Maps, tables, other data, links to press … if needed

Blueprint Taxonomy – as a Political Decision support mechanism

Integrated Situation Awareness Analysis

- **Nature of the Incident**
  - Root cause category: (1 of 5)
    - System failures, natural phenomena, human errors, malicious actions, 3rd party failures
  - Severity of threat: (1 of 3)
    - High, medium, low
- **Impact**
  - Sectors impacted: (1 or more of 11)
    - Energy, transport, banking, finance, health, drinking water, digital infrastructure (7 NISD sectors with OES)
    - Communications (EU ecomms framework directive)
    - Trust and identification (EIDAS)
    - Digital services (NISD DSP)
    - Government services
  - Scale of impact: (1 of 4)
    - Red – very large, Yellow – large, Green - minor, White – no
  - Outlook: (1 of 3)
    - Improving, stable, worsening

Blueprint –integration in IPCR arrangements


Technical Situation Report
Operat. Situation Report
1. Regular Monitoring
No
Incident
2. Analysis and Advice
3. Assessment
IPCR Activation? (Presidency)
Yes
4. Presidency Roundtable Preparation
5. ISAA Preparation
EU Cybersecurity Incident Situation Report
6-7.Presidency RoundTable
YES
ENISA Ex-post Enquiry
10. Phasing Out
NO
Crisis On-going?
9. Impact Monitoring
Coordination at EU Political Level
8. Council / Coreper Meeting
Coordinated Technical Response, Public Communications
Cyber Diplomacy Toolbox

Recent developments & next steps

EXERCISE 2018

HEX-ML18/ PACE18

2019 Blue OLEx

NIS COOPERATION GROUP

CYBER EUROPE

enisa

CYBER EUROPE

European Commission

Thank you for your attention!

Trust in a Digital Society
HOSPITAL
Public services
Electronic transactions
Connected mobility
Cybersecurity
Health
Online privacy
Electronic identity
Connected cities
European Commission | powered by European Commission, CONNECT
Digital Society, Trust and Cybersecurity Directorate