Good Practices Cyber Exercises: Cyber Europe & Cyber Atlantic

Cyber Crisis Exercises & Cooperation
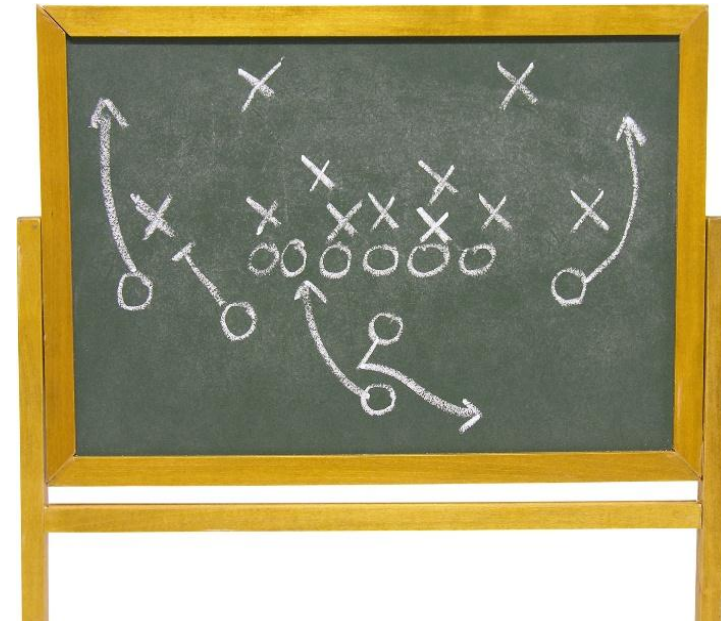
Resilience and CIIP Unit

ENISA

Agenda

- Introduction
  - Cyber Exercises Area at ENISA
- Good Practices on Cyber Exercise Organisation
  - The Cyber Exercise Lifecycle
- Case studies
  - Cyber Europe
  - Cyber Atlantic
- Cyber Exercise Stocktaking

# Cyber Exercises at ENISA

- **2009**
    - Good Practice Guide on National Exercises
- **2010**
    - Support all Member States (MS) to run exercises (seminars)
    - The first Pan-European Exercise 'Cyber Europe 2010'
- **2011**
    - Study National Cyber Contingency Plans (NCPs)
    - Cyber Atlantic 2011
- **2012**
    - Two regional exercises (EuroSOPEx)
    - Cyber Europe 2012
    - Cyber Exercises Stocktaking
    - International Conference on Cyber Exercises, Paris, 27th June 2012

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-exercise-stocktaking/cyber-exercise-conference

Agenda

- Introduction
  - Cyber Exercises Area at ENISA
- Good Practice on Cyber Exercises
  - The Cyber Exercise Lifecycle
- Case studies
  - Cyber Europe
  - Cyber Atlantic
- Cyber Exercises Stocktaking

Lifecycle of an Exercise

The Exercise Lifecycle

Identify → Plan → Conduct → Evaluate
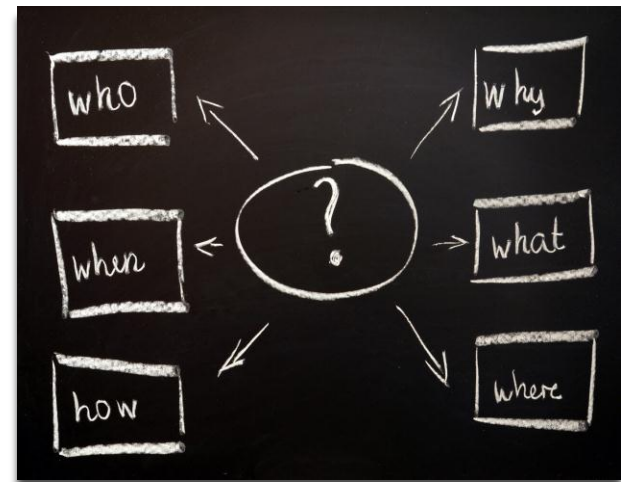
Lifecycle of an Exercise

The Exercise Lifecycle

Identify → Plan → Conduct → Evaluate

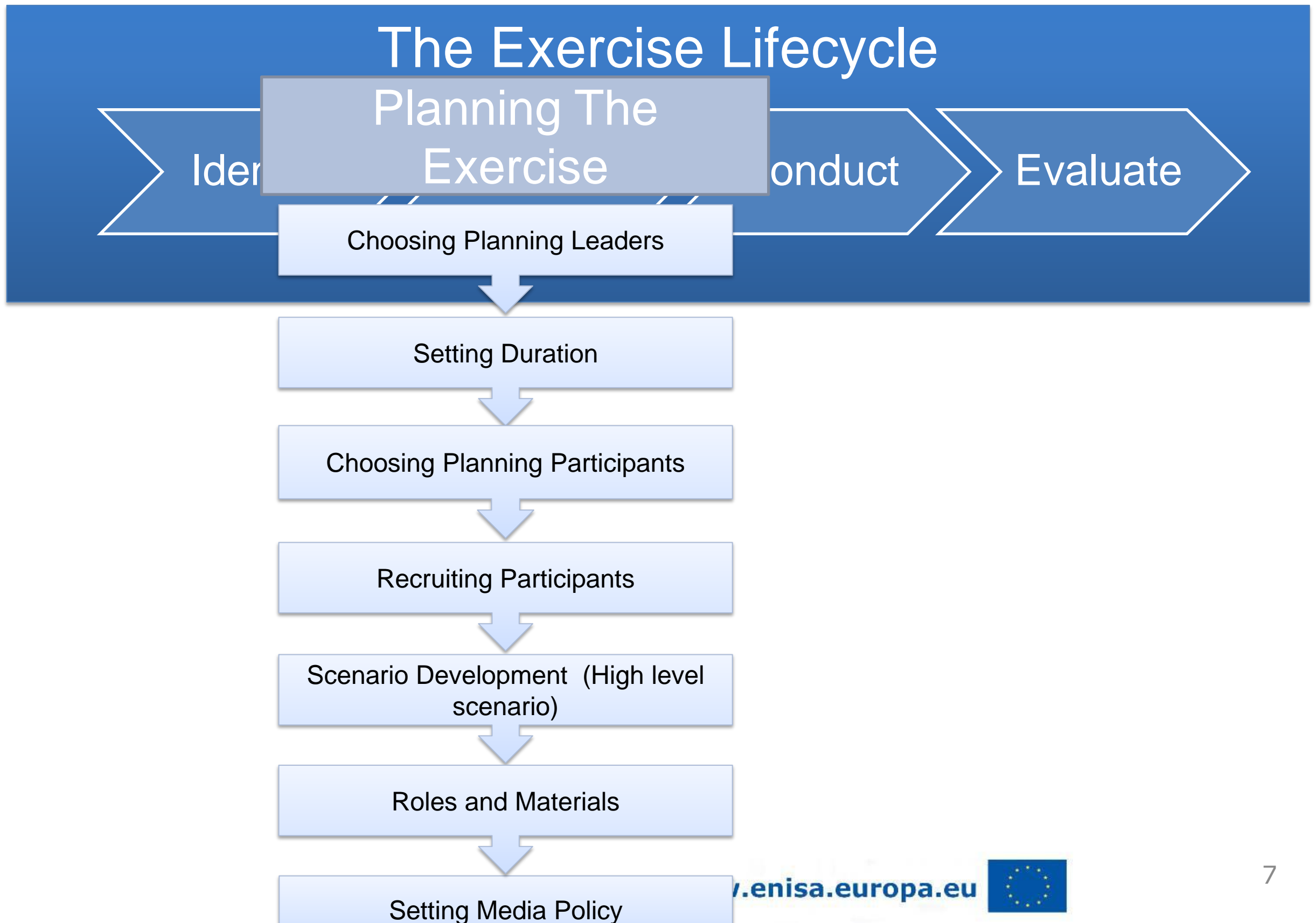**Identifying The Exercise**

- Identify Clear Objectives
- Choose a High-Level Scenario
- Choose a Type of Exercise
- Identify Key Participants
- Set The Size and Scope

Lifecycle of an Exercise

The Exercise Lifecycle

Ide... **Planning The Exercise** ...onduct > Evaluate

Choosing Planning Leaders

↓

Setting Duration

↓

Choosing Planning Participants

↓

Recruiting Participants

↓

Scenario Development (High level scenario)

↓

Roles and Materials

↓

Setting Media Policy

.enisa.europa.eu

Lifecycle of an Exercise

The Exercise Lifecycle

Identify → Conducting The Exercise → Evaluate
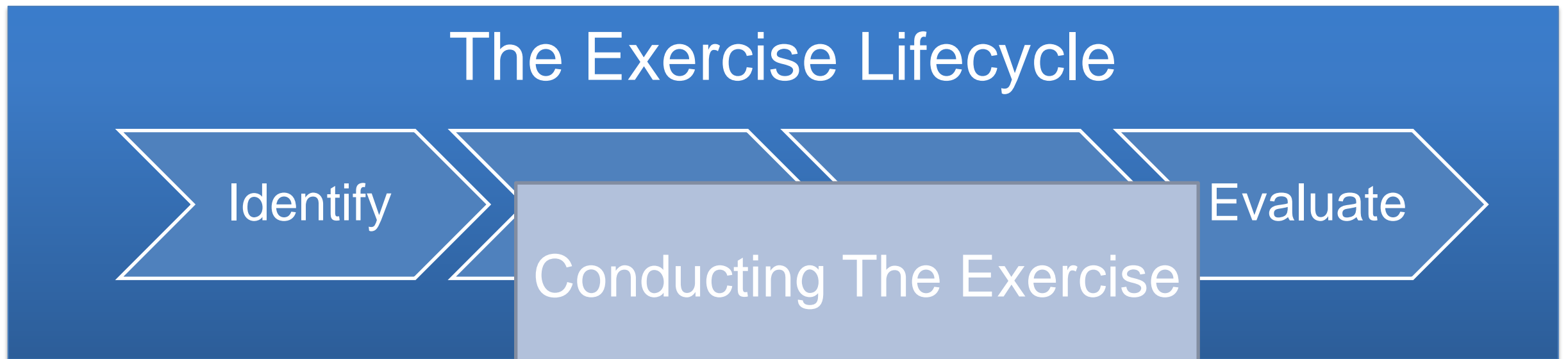
Training Participants

↓

Executing Roles and Tasks

↓

Managing The Scenario and Injects

Lifecycle of an Exercise

The Exercise Lifecycle

Identify → Plan → Con...

Evaluating The Exercise

Setting Evaluation Objectives
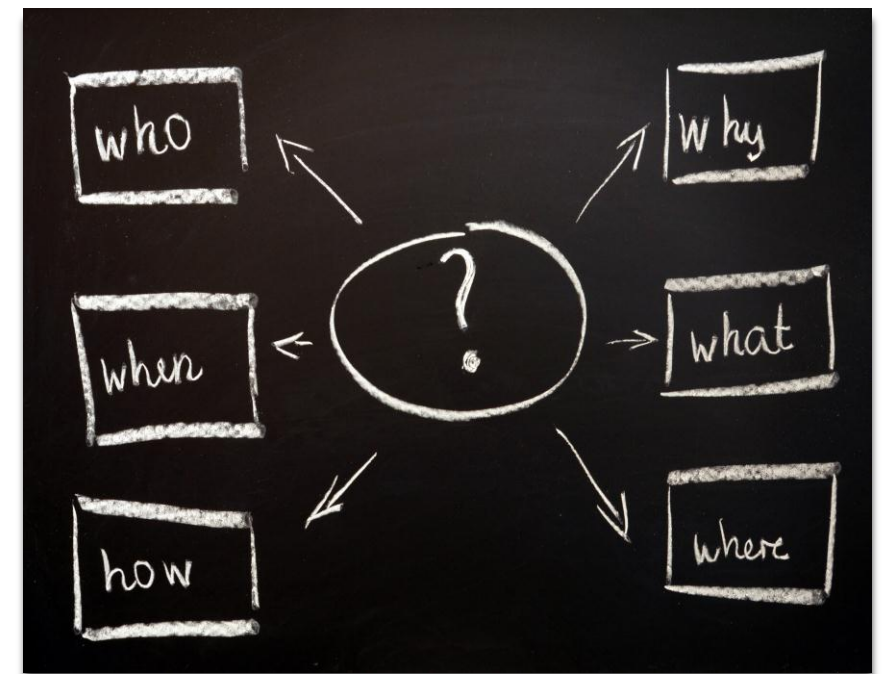
↓

After-Action Review

↓

Measuring Success

ENISA Good Practice Guide

- Available online at:

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/exercises

- Full day seminars

Agenda

- Introduction
  - Cyber Exercises Area at ENISA
- Good Practices on Cyber Exercise Organisation
  - The Cyber Exercise Lifecycle
- Case studies
  - Cyber Europe
  - Cyber Atlantic
- Cyber Exercises Stocktaking

Cyber Europe 2010:
First Pan European Exercise

- Table top exercise

- Incidents affecting all EU Member States

- Tested mainly communication & cooperation

- Involvement of public authorities/bodies only

- Concentrated on members of the CIIP community – no political escalation

- Test Carried out on 4 November 2010

- Utilised the ENISA Good Practice Guide

Objectives

- Increase understanding of how cyber incidents are handled by Member States

- Test communication points and procedures between participating Member States

- Build trust among participants - help to establish mutual support procedures

- Create a CIIP community with a focus on exercises

The Scenario

- The scenario was not the focus of the test but was used to support the test.

- Based on a Cyber Incident.

  - The impact is on IP networks - large operators – cross country interconnections.

  - Assumed that voice (PSTN/Mobile) communications and power networks are not affected.

- Implemented as 320 injects.

Participation

- All EU Member States and 3 EFTA countries participated

- Profile of Participants:

  - Ministries, National Regulatory Agencies, CIIP and Information Security related organisations, CSIRTs and other related stakeholders

  - 70 organisations and 150 experts

- The role of ENISA was to help Member States to prepare - facilitation and project management.

- The role of the JRC was to provide scientific and technical support for the exercise itself.

Findings

- Findings have been published as a report on the ENISA web site.

- These findings have been grouped:
    - Planning & Structure.
    - Building Trust.
    - Understanding.
    - Points of contact.

- A set of recommendations can also be found in the final report.

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe

Agenda

- Introduction
  - Cyber Exercises Area at ENISA
- Good Practices on Cyber Exercise Organisation
  - The Cyber Exercise Lifecycle
- Case studies
  - Cyber Europe
  - Cyber Atlantic
- Cyber Exercises Stocktaking

1st Joint EU-US Exercise - key facts

★ Announced in April during the Hungary Ministerial Conference

★ Table top, centralised, discussion based

★ Exploratory nature

  ★ how do we engage each other?

★ Planning team with experts from 15 countries

★ Exercise completed on 03.11.11

CYBER
ATLANTIC
2011

.europa.eu

Exercise lessons learned

- Modern communication and conferencing facilities are needed for crisis cooperation of large groups

- Mechanisms/structures for cross-border cooperation do exist; however, each country needs awareness of all communications options

- Exercises need increased participation from all three: Technical, Law Enforcement, Policy/Political

- Single Point of Contacts would help but are not compulsory

- More exercises/workshops are needed!

Agenda

- Introduction
  - Cyber Exercises Area at ENISA
- Good Practices on Cyber Exercise Organisation
  - The Cyber Exercise Lifecycle
- Case studies
  - Cyber Europe
  - Cyber Atlantic
- Cyber Exercises Stocktaking

Contact and Questions

Contact Details:

Dr Panagiotis TRIMINTZIOS
(panagiotis.trimintzios@enisa.europa.eu)
European Network and Information Security Agency (ENISA)

Science and Technology Park of Crete

P.O. Box 1309, 71001 Heraklion - Crete – Greece

Tel: +302810391386

http://www.enisa.europa.eu

www.enisa.europa.eu