Context

In a Communication[1] published in early 2009 the European Commission invited Member States to. ...Organize regular exercises for large-scale networks security incident response and disaster recovery....

During the Tallinn Ministerial Conference[2] in April 2009 the Ministers declared that a joint EU exercise on Critical Information Infrastructure Protection should be organised and staged by 2010, in line with the Commission's action plan...

Finally the Council Resolution of Dec 2009[3] mentions that Member States should organise national exercises and/or participate in regular European exercises in the area of Network and Information Security..., and that ENISA participate with Member States on exercises to provide appropriate responses to emergencies...

1 Communication on Critical Information Infrastructure Protection (CIIP) *Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*, COM(2009)149 of 30 March 2009, Action Plan:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

2 **http://www.tallinnciip.eu/**

3 **http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:EN:PDF**

Next steps

The events after the exercise will include a de-briefing session immediately after the exercise and a large workshop, as well as the publication of a report on the exercise in early 2011.

The preparation and post-evaluation of the national part of the exercise will be done by each Member State.

Right after the exercise a warm de-briefing session captured the main impressions from the participants. The overall conclusion was that the exercise was successful and the objectives were met.
The detailed analysis of the data collected during the exercise will conclude in a report, with all observations and recommendations, published in early 2011.
Following that a large workshop in Brussels with all involved stakeholders will validate the results and open the way towards the next pan European exercise. In parallel ENISA will continuously support national exercises at all Member States, while international collaborations will be further explored.

enisa
European Network and Information Security Agency

JRC
EUROPEAN COMMISSION

Contact details

Dr Panagiotis TRIMINTZIOS
Resilience and CIIP Program
Technical Competence Department
European Network and Information Security Agency – ENISA
Email: **resilience@enisa.europa.eu**
www.enisa.europa.eu/act/res

CYBER EUROPE 2010

CYBER EUROPE 2010:

the first pan-European exercise on CIIP

enisa
European Network and Information Security Agency

JRC
EUROPEAN COMMISSION

Organisation and setup

In this context ENISA is facilitating the first ever pan-European exercise known as CYBER EUROPE 2010.

The first phase of CYBER EUROPE 2010 was the dry-run session at the end of September 2010.

The second phase, the actual exercise, will be conducted at the beginning of November 2010.

ENISA is undertaking the overall management of the exercise, while the Joint Research Centre (JRC) of the European Commission is providing technical support.

Profile of participants

Participants will be public authorities in Member States of the European Union (EU) and the European Free Trade Association (EFTA).

The participants from each Member State may vary, as they will be authorities that represent national ministries, national regulatory agencies, CIIP and information security related organisations, national computer security incident response teams (CSIRTs) and other related stakeholders.

Currently, 30 countries are involved, with 22 playing an active role while the rest are participating in the planning workshops and will observe the exercise from the exercise control centre.

Objectives and scope

CYBER EUROPE 2010 is testing the measures in place to ensure cooperative responses during cross-border events and how communication channels can be optimised. The scenario will pave the way to improving intra-European relations regarding security incidents.

The exercise scenario will concern incidents that involve the resilience of the Internet. The incidents will affect all participating countries.

The actual scenario will not be the focus of the test but will support the test. Based on a cyber incident:

a. *the impact will be on IP networks – large operators – cross-country interconnections;*
b. *voice (PSTN/mobile) communications will not affected;*
c. *similarly, supporting facilities, such as power supplies, will not be affected.*

The list of objectives of the exercise includes:

a. *building trust among the participants;*
b. *increasing the understanding on how cyber incidents are handled in European Member States (MSs);*
c. *testing communication points and procedures between participating MSs;*
d. *understanding interdependencies between key actors within each MS;*
e. *promoting mutual support between MSs;*
f. *establishing contacts and new national as well as international relations;*
g. *learning about exercises from the planning phase to their actual conduct and evaluation;*
h. *supporting the already-existing communication channels;*
i. *building and adding new knowledge;*
j. *becoming familiar with cross-country events and the response mechanism, because impacts have 'no borders';*
k. *taking an important step towards creating a CIIP community.*

Lessons Learnt

Some of the interim findings and recommendations of Member States (MS) participants include:

- The exercise fully met its objectives. The scenario was well balanced between technical and communication requirements.
- Exchanging 'lessons-learnt' with other (national or international) exercises would be useful.
- The private sector should be part of the next pan-European exercise.
- There is a lack of pan-European preparedness measures to test. This reflects the fact that many Member States are still refining their national approaches.
- The exercise was only the first step towards building trust at pan-European level. More co-operation and information exchange is needed.
- Incident handling in Member States varies a lot due to the different roles, responsibilities and bodies involved in the process. The Member States had difficulties in fully grasping how incidents are managed in other MS.
- There is no need for creating a new pan-European directory of contacts. The existing ones are sufficient but need to be updated and completed regularly.
- ENISA's role in organising and managing future exercises is highly recommended by MS.
- Member States support future pan-European exercises, but more time should be allocated to plan and execute the exercise.