www.enisa.europa.eu

# Q&As on

# the first, pan-European Cyber Security Exercise

# 'CYBER EUROPE 2010'

### Why exercises, and especially a pan-European exercise?

Exercises are an important mechanism to assess preparedness measures against cyber threats, natural disasters, and technology failures. They enable authorities to target specific weaknesses and increase cooperation among relevant stakeholders. Exercises identify interdependencies, stimulate continuity planning, train and educate people.

### What is the objective of 'CYBER EUROPE 2010'?

The main objective of the exercise is to bring the Member States together and enhance the Member States' communication and coordination efforts during a crisis. The exercise will test Member States' abilities to find the right contacts and assess the competences in the other Member States during a large scale crisis.

### Who participates in the exercise?

Participants in CYBER EUROPE 2010 are only public authorities of EU Member States. The players involved include ministries, national regulatory agencies, CIIP and information security related organisations, national computer security incident response teams (CSIRTs).

### How many Member States take part in the CIIP exercise?

All EU Member States and 3 EFTA countries take part. More specially, 22 Member States actively participate having in total 70 player organisations around Europe, while 8 countries take the role of observer.

### What is the private sector's role in this exercise?

The Member States decided from the very beginning that it is already a very ambitious exercise. Having the private sector taking part in this first pan-European exercise would add an additional complexity factor, which is the reason for including only the public sector in this exercise.

## Who organises and plans the exercise?

The exercise is facilitated, organised and managed by ENISA, the European Network and Information Security Agency, and supported by JRC, the European Commission's Joint Research Centre. Several Member States volunteered to help organise and plan the exercise. The team of planners involved staff from DK, FI, FR, HU, IT, PT, SE, UK, and was done with the contribution of staff from ENISA and the EU's Joint Research Centre, JRC.

## Can you briefly present the general idea of the scenario?

The exercise scenario concerns incidents affecting the availability of Internet in several European countries. The basic idea is that Internet interconnectivity between countries becomes gradually unavailable. As a result citizens, businesses and public institutions will have difficulties in accessing critical online services, unless the traffic from affected interconnections is rerouted. As the phenomenon continues, one country after the other will increasingly throughout the day suffer from this problem, over phone and mails, as a desktop exercise. In that case, all playing Member States will have to co-operate to jointly respond to such fictitious crisis.

## Where will the pan-European exercise take place?

The exercise is distributed to the participating Member States, but the head quarter of the exercise will be in ENISA's office in Athens. The head quarter will control the exercise and have the infrastructure to distribute injects. The actual players of the exercise will be located in their respective premises in their Member States.

## What is the policy context of this first, pan-European CIIP exercise?

'CYBER EUROPE 2010' was first envisioned in EU Commission's Critical Information Infrastructure Protection 'CIIP'[1] Action Plan and reinforced by the Tallinn Ministerial Declaration[2] and the Council Resolution.
Supporting EU-wide cyber-security preparedness exercises is one of the main actions of the Digital Agenda[3] for Europe, the new policy plan of European Commission.
ENISA's new proposed mandate[4] also highlights the importance of cyber-security preparedness exercises for enhancing trust and confidence in online services across Europe.

## What are the next steps, following this first pan-European exercise?

The exercise will be evaluated, and a public report on the results of the exercise will be published beginning of next year. A consultation workshop will be organised in order to

[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://ec.europa.eu/information_society/digital-agenda/index_en.htm
4 http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/459

collect experiences and opinions from the participating Member States. The dialogue with the Member States will be extended on topics for future exercises, create future scenarios based on their input and create a roadmap for more complex exercises.
ENISA plans collaborate very closely with EuroCybex, a European project that will deliver an exercise next year. Next year ENISA will also start planning for the second pan-European exercise.

**What are your recommendations in general when it comes to CIIP?**

One of the important recommendations for Member States is to run national exercises. Exercises help to test measures and support decisions on taking actions. If all Member States become experienced in running national exercises the readiness in Europe will be enhanced. In this way the Member States will also be able to collaborate better at a pan-European level.

**Does ENISA have any tools for the Member States' national exercises?**

ENISA has developed a good practice guide[5] that can be used for organising and planning national exercises. ENISA can also host seminars in the Member States upon request and try to communicate the importance of these national exercises.

**For further information about ENISA's Resilience and CIIP Program, see:**
http://www.enisa.europa.eu/media/news-items/enisa-teams-up-with-member-states-on-pan-european-exercise

**For further details contact:**
**Ulf Bergstrom**, ENISA's Spokesman
press@enisa.europa.eu, Mobile: +30 6948 460143

[5] http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises