A simulated cyber attack to boost preparedness for the real thing by:

- Testing existing mechanisms for cooperation between public authorities
- Evaluating cooperation between relevant public & private players
- Identifying gaps & challenges for how large-scale cyber attacks could be handled in a more secure and effective way

Why are they important?

Cyber attacks are a grave threat to the economy & society of Europe, posing a risk to companies as well as individuals' 'wallet issues', wellbeing, health and safety. Ensuring that we are protected requires seamless co-operation between countries and organisations as well as complex systems and processes that have to be instantly activated.

ENISA CYBER SECURITY EXERCISES HELP MAKE THIS POSSIBLE

ENISA’s role:

1. Organise Pan-European Exercises
2. Support the organisation of national exercises

Case study: Cyber Europe 2012

The largest cyber security exercise ever carried out in Europe

- 339 Public & private sector organisations
- 4,000 Injects (Simulated cyber incidents)
- 517 Individuals
- 29 Countries

Future Exercises

- Cyber Europe 2014
- Cyber Atlantic 2014

Needs

- Frequent cooperation between public and private players
- Adaptability & scalability of operational procedures
- Up-to-date technical infrastructures and tools
- Efficient planning

Challenges

- Knowledge of procedures
- Different public–private cooperation structures
- Crisis management decision making

Key findings

Testing existing mechanisms for cooperation between public authorities
Evaluating cooperation between relevant public & private players
Identifying gaps & challenges for how large-scale cyber attacks could be handled in a more secure and effective way

Recommendations

- More exercises to improve cooperation and effectiveness, scalability, and knowledge.
- More training in crisis procedures
- Increased private sector involvement for future exercises, especially from critical sectors (e.g. energy, transportation)

Securing Europe’s Information Society