

Securing Critical Information Infrastructures and Services

Evangelos OUZOUNIS
Head of CIIP & Resilience
ENISA



2011: Attacks on governments



2012: Flamer



Iran
189

Israel
Palestine
98

Sudan
32

Syria
30

Lebanon
18

Saudi
Arabia
10

Egypt
5

Cyber Exercises, the Big Three



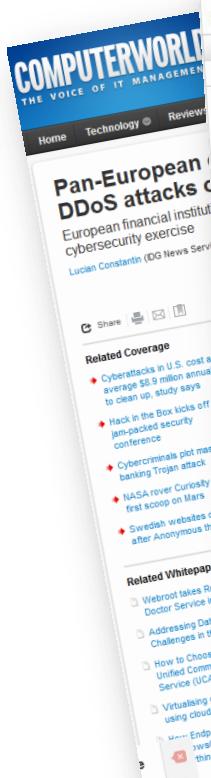
- Europe's first ever international cyber security exercise, 2010
- First ever EU-US exercise, 2011. Work with Comm. & MS to build transatlantic cooperation
- Cyber Europe 2012. Developed from learning in 2010 & 2011 exercises. Involves MS, private sector and EU institutions. Highly realistic exercise, Oct 2012



2nd Pan - European
Cyber Exercise

Cyber Europe 2012 – media coverage

- More than 100 news stories so far – Europe, plus USA
- Most online and broadcast media
- Follow-up media requests still coming in (@ 08/10/2012)



Pan-European DDoS attacks continue

The European financial institutions' cybersecurity exercise

Lucian Constantin (CG News Service)



EU hosts large-scale cyber-security exercise

The European Union is hosting what it describes as its biggest cybersecurity exercise.

The EU intends to clamp down on security hackers, that are costing its economy huge amounts of money. (Ugoer Tramper/pixelio.de)



EU and banks stage DDoS cyber-attack exercise

The European Union is hosting what it describes as its biggest cybersecurity exercise.

In a separate incident, governments, businesses and ISPs (Internet Service providers) are being faced with 1,200 separate incidents during a simulated DDoS (distributed denial of service) attack.

A similar event was staged in 2010, but this is the first time that the bloc's banks have been involved.

The results will be used to find ways to improve co-operation.

However, one computer security expert warned that the effort would be of only limited use when it came to protecting organisations against real-world attacks.

"We want to test how member states co-operate with each other during a crisis," Evangelos Ouzounis, head of Enisa's resilience and critical information infrastructure unit, told the BBC.

"We have developed some draft operating procedures over the last two years and we would like to test how they are applied in a crisis. We hope that after the exercise we can then identify any gaps in the information flow, and by improving them we can become stronger."



Cyber Europe Ramps Up Cyber Attack Testing With Second Simulated Pan-Europe DDoS

Three hundred IT security professionals from across Europe are locking horns in a simulated cyber war exercise taking place today which — if it were a real attack — would be capable of disrupting services for millions of Europeans. The exercise, known as **Cyber Europe 2012**, is being run by ENISA: the European Network and Information Security Agency, and is part of ongoing efforts to bolster cyber crisis cooperation, preparedness and response across Europe. This is first Cyber Europe event to include participants from the private sector — specifically the finance industry — not just the public sector.

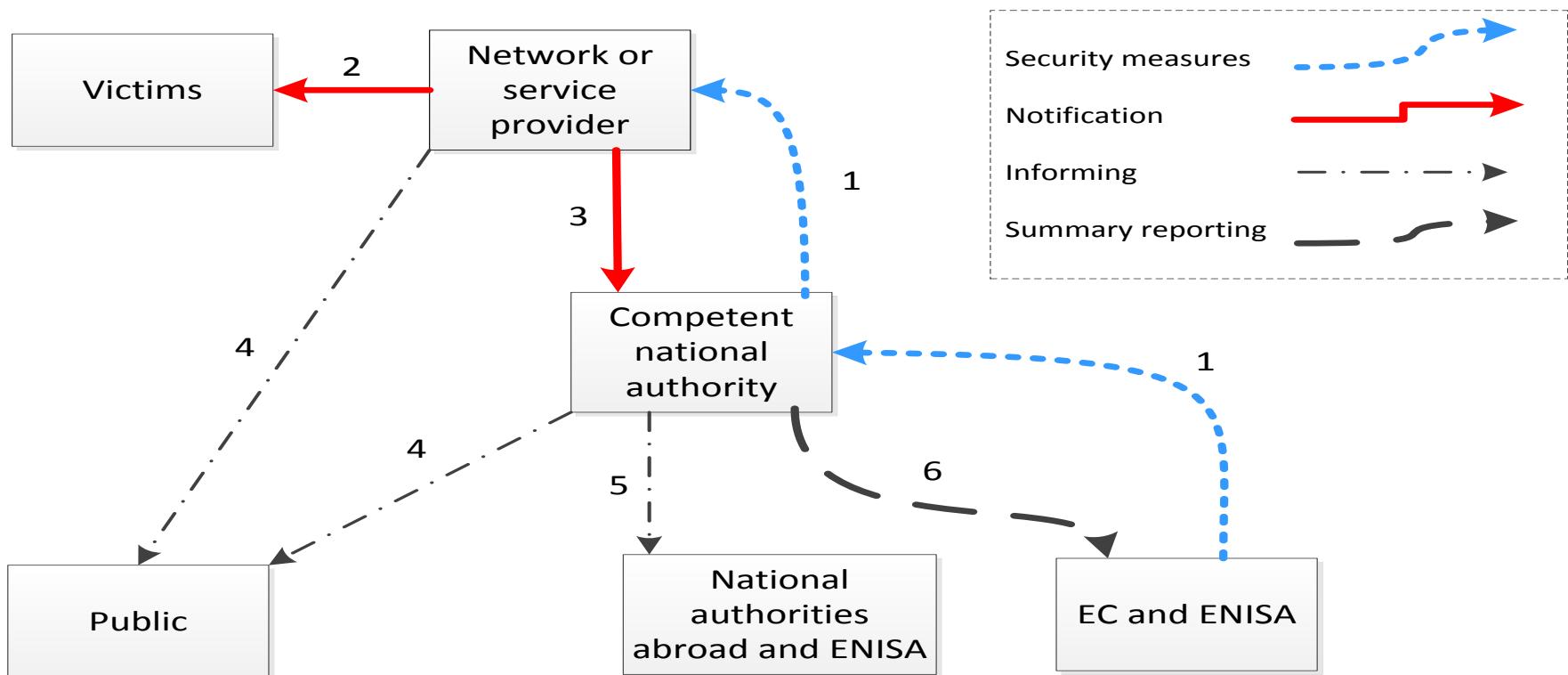
Udo Helmbrecht, Executive Director of ENISA, in a statement, said:

- the cyber crisis community in improving the resilience of critical information infrastructure in Europe;
- scalability of existing mechanisms, procedures and information flow for between public and private stakeholders in Europe;
- changes on how large scale cyber incidents could be handled more effectively.

"I took place in 2010 but this event is larger and more complex — with 300 participants (more than 70 who took part in 2010) and enough 'cyber incidents' being injected by the end of the exercise vs 300+ in the testing.

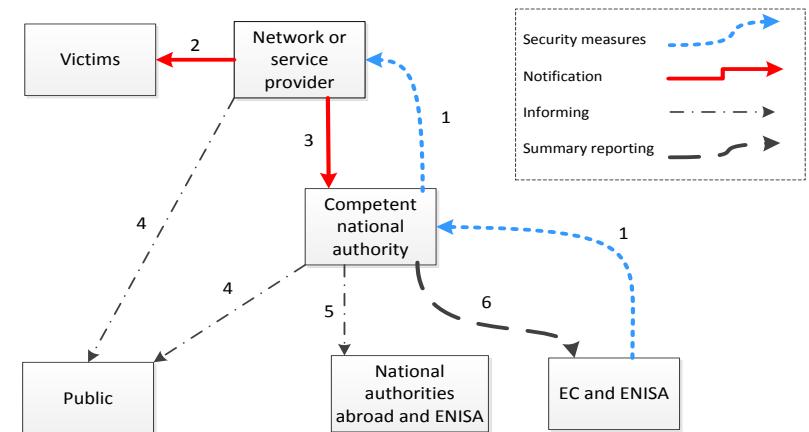
Overview of Article 13a

- Appropriate security measures for e-comms providers
- Incident reporting for e-comms providers

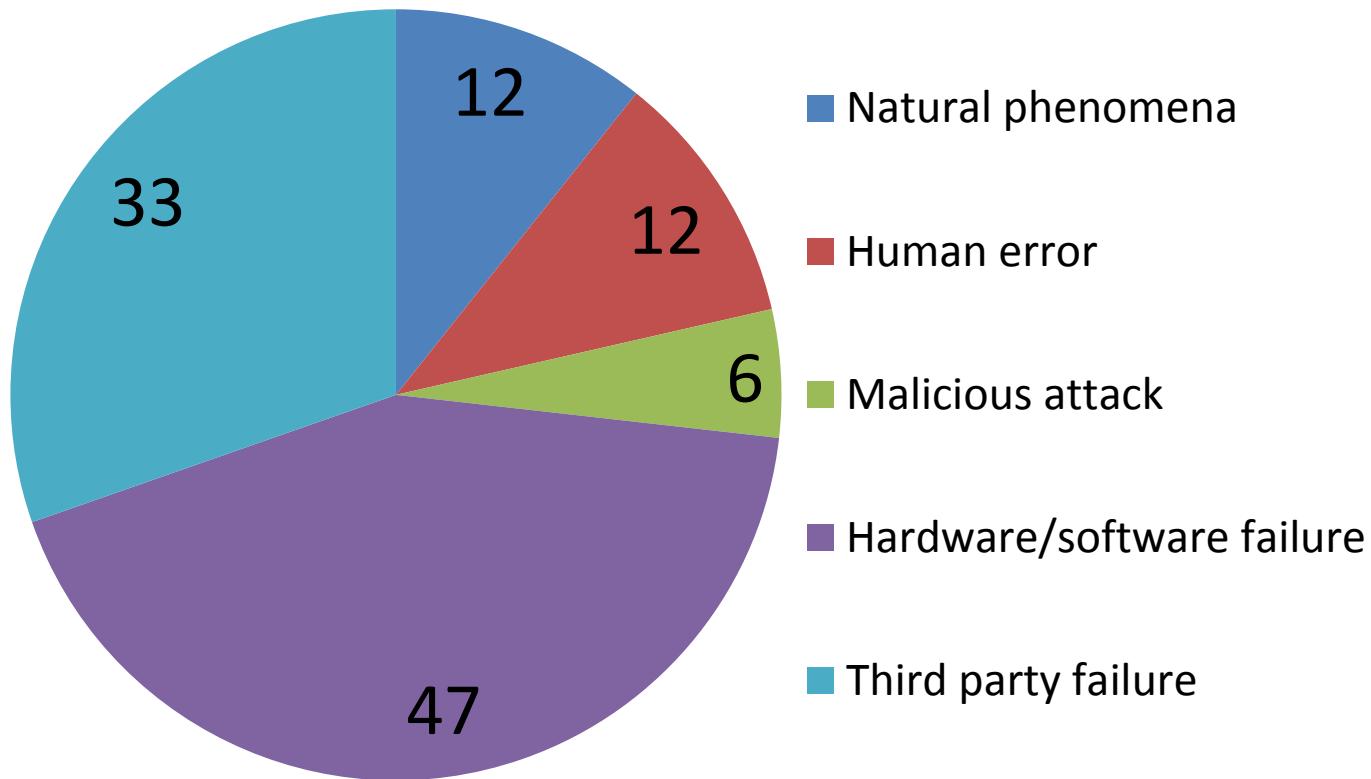


Article 13a - Incidents 2011

- 51 incidents from 11 countries, 9 countries without significant incidents, 9 countries with incomplete implementation
- Most incidents
 - affect mobile comms (60%)
 - are caused by
 - hardware/software failures (47%)
 - third party failures (33%),
 - natural disasters (12%)
- Many involve power cuts (20%)
- Natural disasters (storm, floods, et cetera)
 - often cause power cuts, which cause outages
 - cause incidents lasting an average of 45 hours
- Next report spring 2013, expected around 500 incident reports



Root Causes of 2011 incidents



EP3R - Public Private Partnership for Resilience

- provide a platform for information sharing and stock taking of good policy and industrial practices
- discuss public policy priorities, objectives & measures
- improve coherence and coordination of policies for security and resilience in Europe;
- 3 Working Groups
 - WG 1: Interdependencies of ICTs to critical Sectors
 - WG 2: Baseline requirements for security and resilience of electronic communication networks
 - WG 3: Coordination and cooperation mechanisms
 - Botnets
 - Pan European exercise



Cloud Computing

Objectives for Cloud Computing at ENISA

- Help governments and businesses to leverage the cost benefits of cloud computing, with due consideration of security requirements and new risks
- Improve transparency on security practices to allow informed decisions
- Create trust and trustworthiness by promoting best practice and assurance standards

Report defines minimum baselines for:

- Comparing cloud offers
- Assessing the risk to go Cloud
- Reducing audit burden and security risks



Smart Grid Security

- ENISA recommendations include:
 - Establishing of clear regulatory and policy framework on smart grid cyber security at national and EU level – currently missing.
 - The EC, with ENISA, MS, and private sector, should develop minimum set of security measures based on existing standards and guidelines
 - EC and MS authorities should promote security certification schemes for the entire value chain of smart grids components, including organisational security



Smart Grid Security

- ENISA recommendations include:
 - Establishing of clear regulatory and policy framework on smart grid cyber security at national and EU level – currently missing.
 - The EC, with ENISA, MS, and private sector, should develop minimum set of security measures based on existing standards and guidelines
 - EC and MS authorities should promote security certification schemes for the entire value chain of smart grids components, including organisational security



Contact us, follow us
resilience@enisa.europa.eu

twitter
twitter.com/enisa_eu

website
www.enisa.europa.eu