

# **CYBER SECURITY EXERCISES ROUNDTABLE**

## **ORGANIZATION of AMERICAN STATES MEETING**

**MIROSŁAW MAJ**  
CYBERSPACE SECURITY FOUNDATION

<MIROSLAW.MAJ@CYBSECURITY.ORG>





- 7-9 November 2011, Washington DC
- CERTs
- GOVs
- NGOs
- Invitation via TERENA







# OBJECTIVE

- to discuss the work that has been done in developing cyber security technical exercises
- exchange best practices and recommendations for improvements to existing exercise frameworks
- explore opportunities for future collaboration



# OAS exercise 2011

- Mexico, Brasil, Argentina, Venezuela
- OAS coordination
- Mainly based on CERT experiences in these countries
- Four fictitious countries
  - CERTs
- Hands on exercises
- Coordination in mitigation of attacks on critical infrastructure



# OAS exercise 2011



- TECHNICAL BACKGROUND
  - Virtual environment
  - Injects system
  - Incident management ticketing tool
  - Email client
  - Log analysis





# CYBERSTORM I - III

- ORGANIZED BY DHS/NCSD
- 3rd edition – September 2010
- 3-days exercise
- Cross-section oriented on CIIP
- Microsoft support
- 11 states, 12 international partners, 60 private sector companies



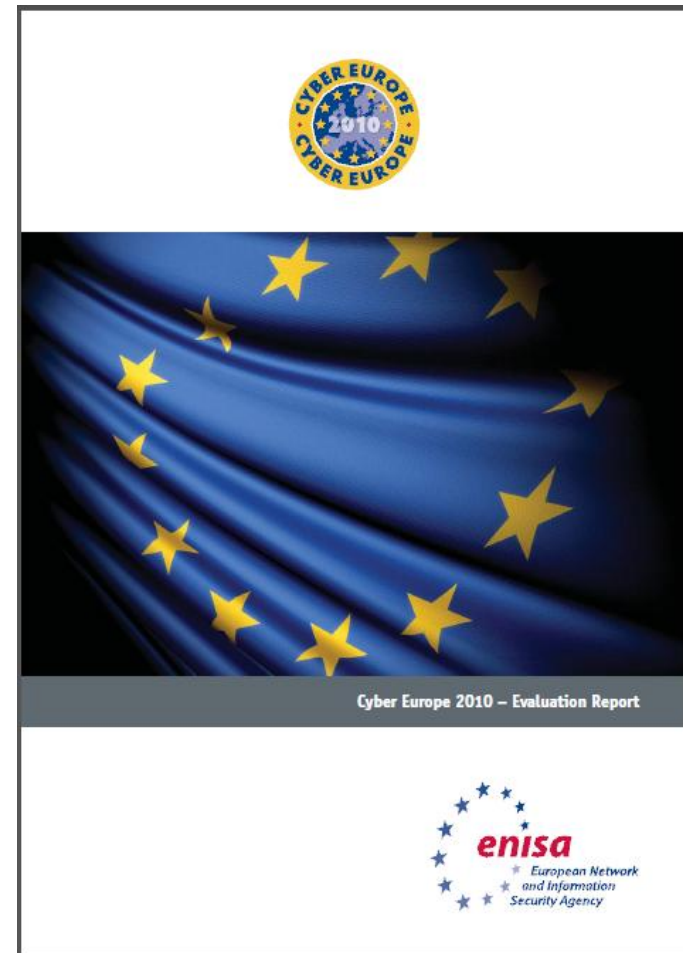


# CYBERSTORM I - III

- the primary vehicle to exercise the newly-developed National Cyber Incident Response Plan (NCIRP)
  - Roles
  - Responsibilities
  - Authorities
- information sharing mechanisms between the public and private sectors and improve their working relationship



# CYBER EUROPE



# ORGANISED BY ENISA

- TABLE TOP EXERCISE
  - On site / from offices
- 22 Member States
- 8 Observers (with the narrator)
- 50 players
- EU + EFTA
- planners group [DK, FI, FR, HU, IT, PT, SE, UK, ENISA, JRC]



# INTERNET INTERCONNECTION SITES PROBLEM



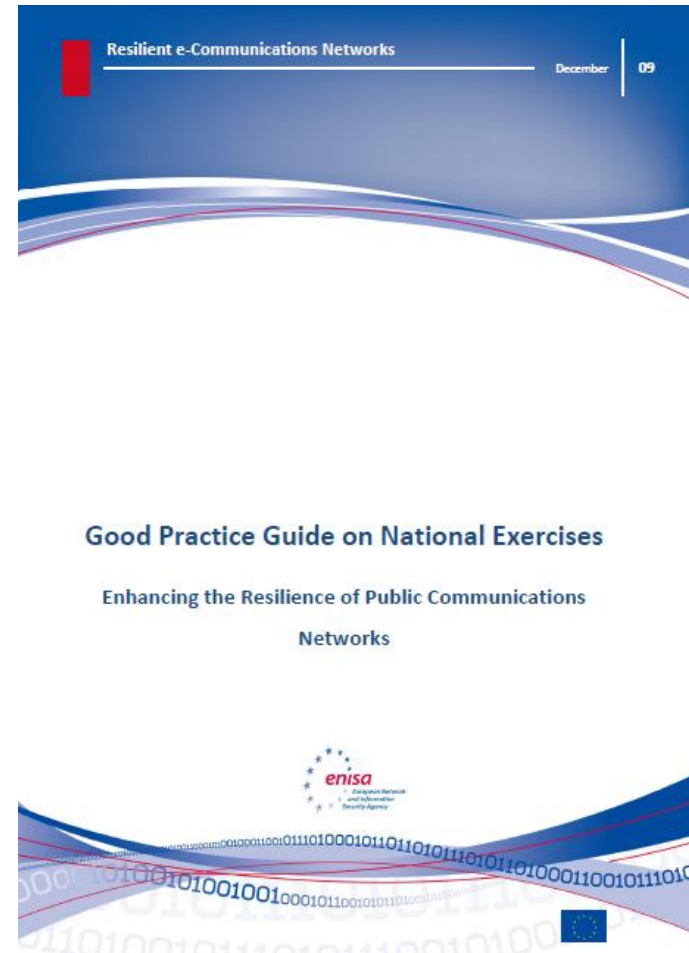
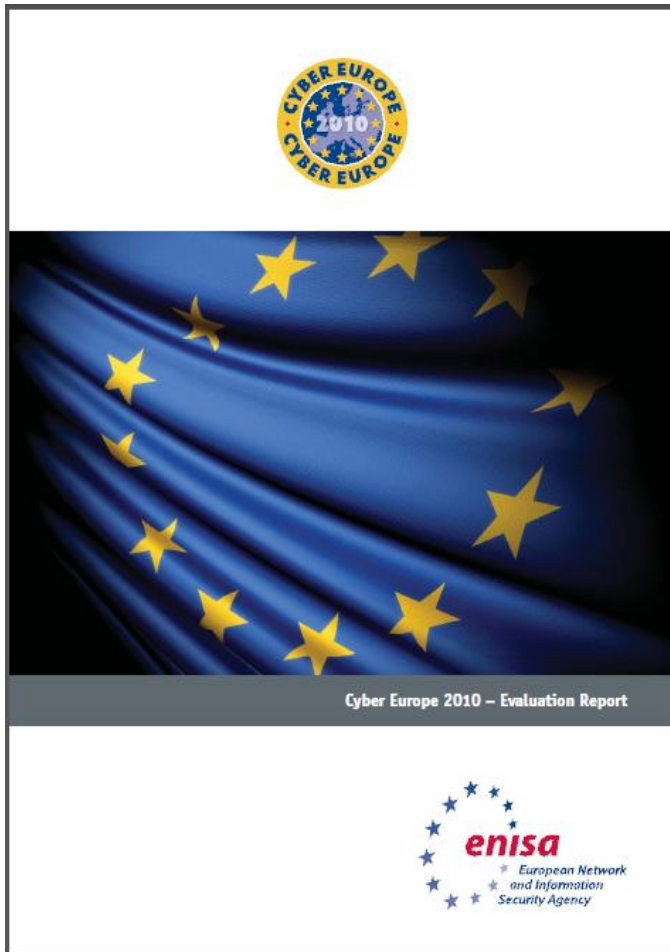












# KEY CONCLUSIONS



nothing really new!

- In international environment the legal component should be included
- Information sharing policies must be strong and accessible
- Operational procedures must be standardized
- Point of contact for each CERT team should be identified to liaise between entities and expedite communication



# IDEAS for the future

- Development of cyber exercises metrics
  - To show quantitatively how well players attended incidents, and where gaps and vulnerabilities remain
- With these data, coordinators would be able to compare exercises and give valuable feedback to the participants



- number of tickets closed,
- time elapsed in responding to and resolving an incident,
- the percent of incidents successfully resolved,
- how many successful communications were exchanged
- etc.

# CYBER EXERCISES IN POLAND



# CYBER SECURITY EXERCISES IN POLAND



- ROCK in Poland (Protection of Critical Cyberspace Year)
- September 2012
- Long preparation period (similar to CYBER EUROPE) will start in February
- Umbrella from National Security Bureau
  - „National Security Bureau is a body providing aid and support to the President of the Republic of Poland in executing security and defence tasks.”
- SECTORS
  - GOV
  - EDU
  - COM
  - ORG







**THANK YOU FOR YOUR ATTENTION!**