# PROTECTING EUROPE'S NETWORK INFRASTRUCTURE

Udo Helmbrecht
Executive Director

2nd International Conference
on Cyber Crisis Cooperation and Exercises

Athens, 23-24th September 2013

# Topics

- ENISA’s role
- EU Cyber Security Strategy & EU NIS Directive
- Protecting Critical Information Infrastructure
- Assisting Operational Communities
- CERTs
- Securing New Business Models & New Technologies
- Security & Data Breach Notification
- Data Protection

# ENISA
# &
# EU CYBERSECURITY STRATEGY
# EU NIS[1] DIRECTIVE

[1] Network and Information Security

# ENISA Objectives

1. Advice for EU & MS-political support
2. Supporting new business models & threat landscape analysis
3. "Hands on" – Computer Emergency Response Teams; building up CERTs

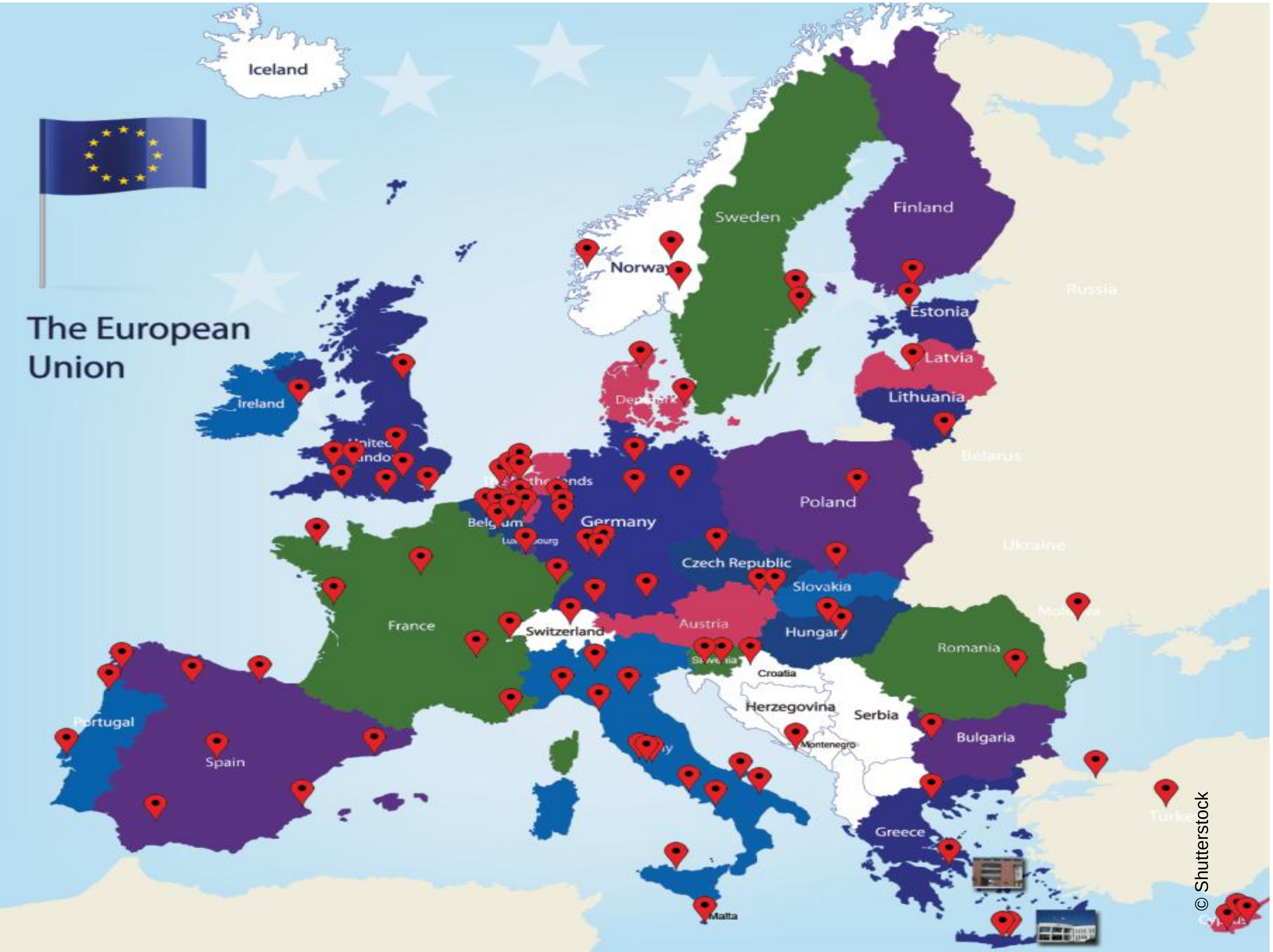
REGULATION (EU) No 526/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 21, MAY, 2013

# ENISA’s new regulation

- Strong interface re fight against cybercrime - focusing on prevention & detection - with Europol’s European Cybercrime Centre (EC3)
- Supporting development of EU cyber security policy & legislation
- Supporting research, development & EU standardisation, for risk management & security of electronic products, networks & services
- Supporting prevention, detection of & response to cross-border cyber-threats
- Aligning ENISA more closely to EU Regulatory process, providing EU countries & Institutions w. assistance & advice

REGULATION (EU) No 526/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 21, MAY, 2013

# Recent ENISA Missions



© Shutterstock

# EU Cybersecurity Strategy

I. EU's core values apply both in digital & physical world

II. Protecting fundamental rights, freedom of expression, personal data & privacy

1. Achieving cyber resilience
2. Drastically reducing cybercrime
3. Developing cyberdefence policy & capabilities
4. Develop industrial & technological resources for cybersecurity
5. Establish a coherent international cyberspace policy for EU & promote core EU values

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Cybersecurity Strategy of the EU, 7.2.2013 JOIN(2013) 1

# Articles of the NIS Directive

5: National NIS strategy & national NIS cooperation plan

6: National competent authority on the security of network & information systems

7: Computer Emergency Response Team

8: Co-operation Network

9: Secure information-sharing system

10: Early warnings

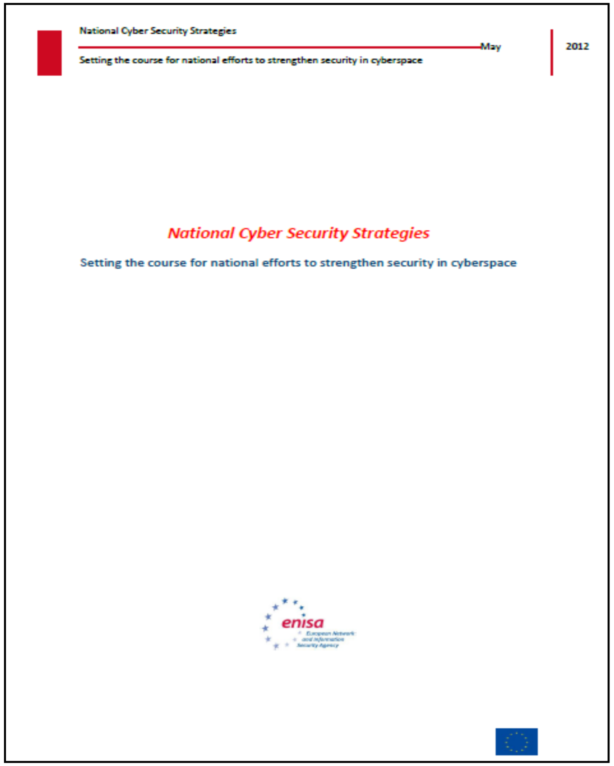
11: Coordinated response

12: Union NIS cooperation plan

14: Security requirements & incident notification

16: Standardisation

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union, 7.2.2013 COM(2013) 48



National Cyber Security Strategies

May 2012

Setting the course for national efforts to strengthen security in cyberspace

*National Cyber Security Strategies*

Setting the course for national efforts to strengthen security in cyberspace

enisa European Network and Information Security Agency

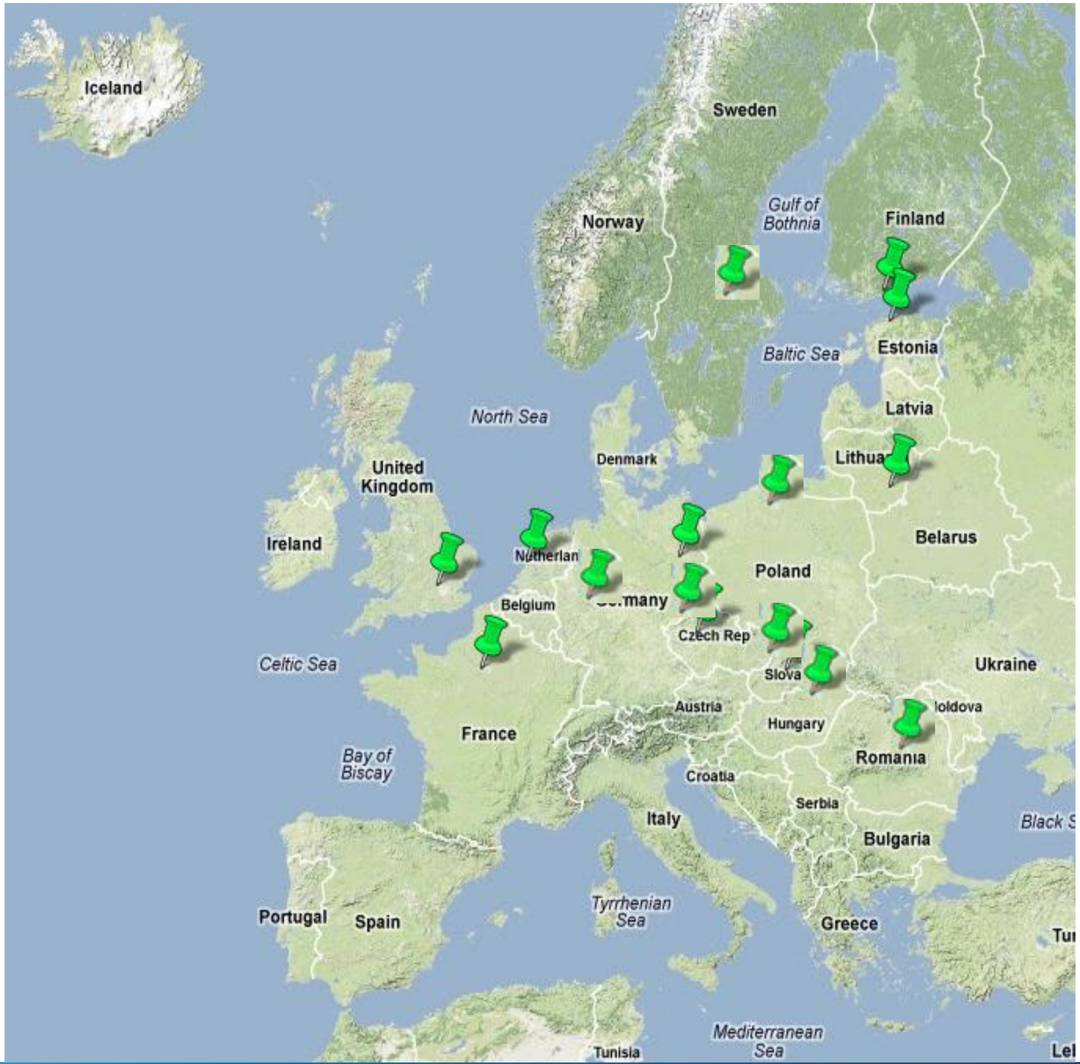
## Example

# GOOD PRACTICE GUIDE ON NATIONAL CYBER SECURITY STRATEGIES (NCSS)

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper

# EU Member States with NCSS

- ✓ Austria
- ✓ Czech Republic
- ✓ Estonia
- ✓ Finland
- ✓ France
- ✓ Germany
- ✓ Hungary
- ✓ Lithuania
- ✓ Luxemburg
- ✓ The Netherlands
- ✓ Poland
- ✓ Romania
- ✓ Slovakia
- ✓ Sweden
- ✓ United Kingdom



## Example

# CYBER SECURITY EXERCISES

# Cyber Security Exercises

- Cyber Europe 2010
  - Europe’s 1st ever international cyber security exercise
- EU-US exercise, 2011
  - 1st transatlantic cooperation - COM/MS
- Cyber Europe 2012
  - Built on 2010 & 2011 exercises
  - Involved MS, private sector & EU institutions.

https://www.enisa.europa.eu/media/press-releases/largest-cyber-security-exercise-cyber-europe-report-published-in-23-languages-by-eu-agency-enisa

# 1st Joint EU-US Exercise - key facts

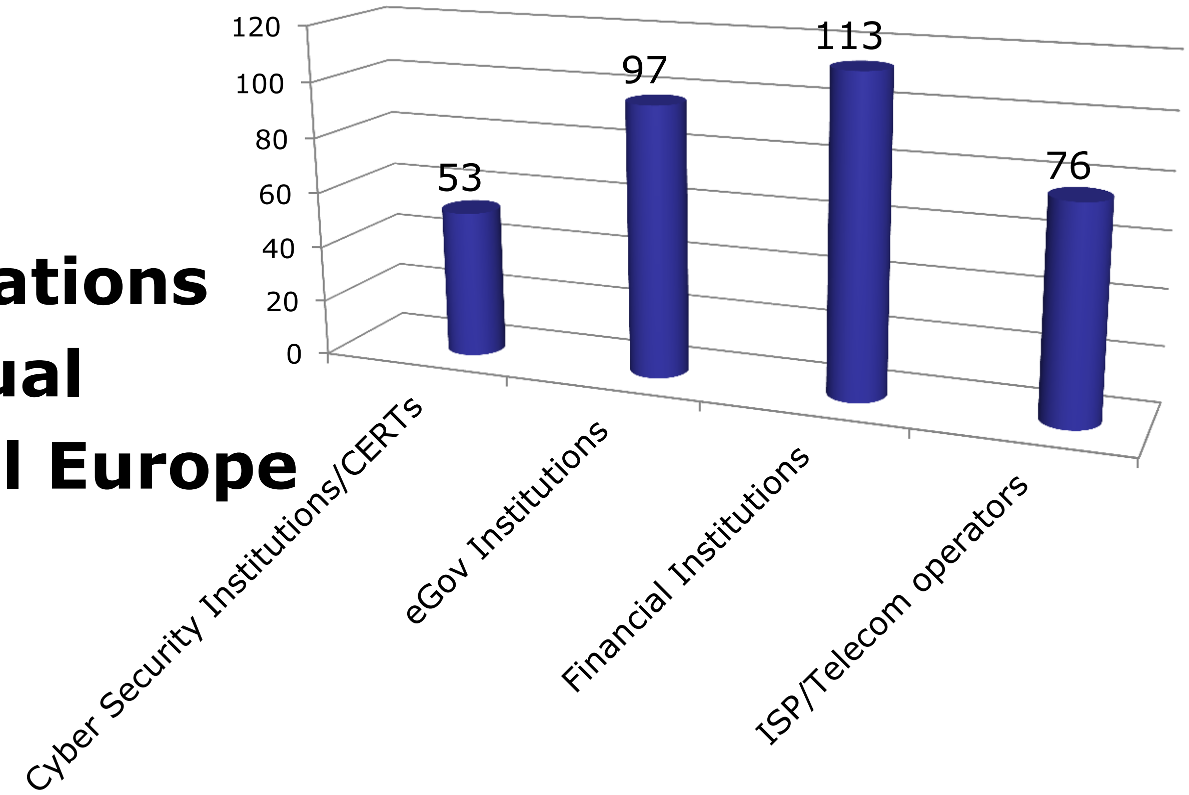
CYBER
ATLANTIC
2011

- **Announced in April 2011 during the Hungary Ministerial Conference**
- Table top, centralised, discussion based
- Exploratory nature
  - how do we engage each other?
- **Planning team with experts from 15 countries**
- **Exercise conducted on 03.11.11**

# FACTS ABOUT CE2012

# Playing Organisations

- ○ **339 organisations**
- ○ **571 Individual**
- ○ **Players in all Europe**

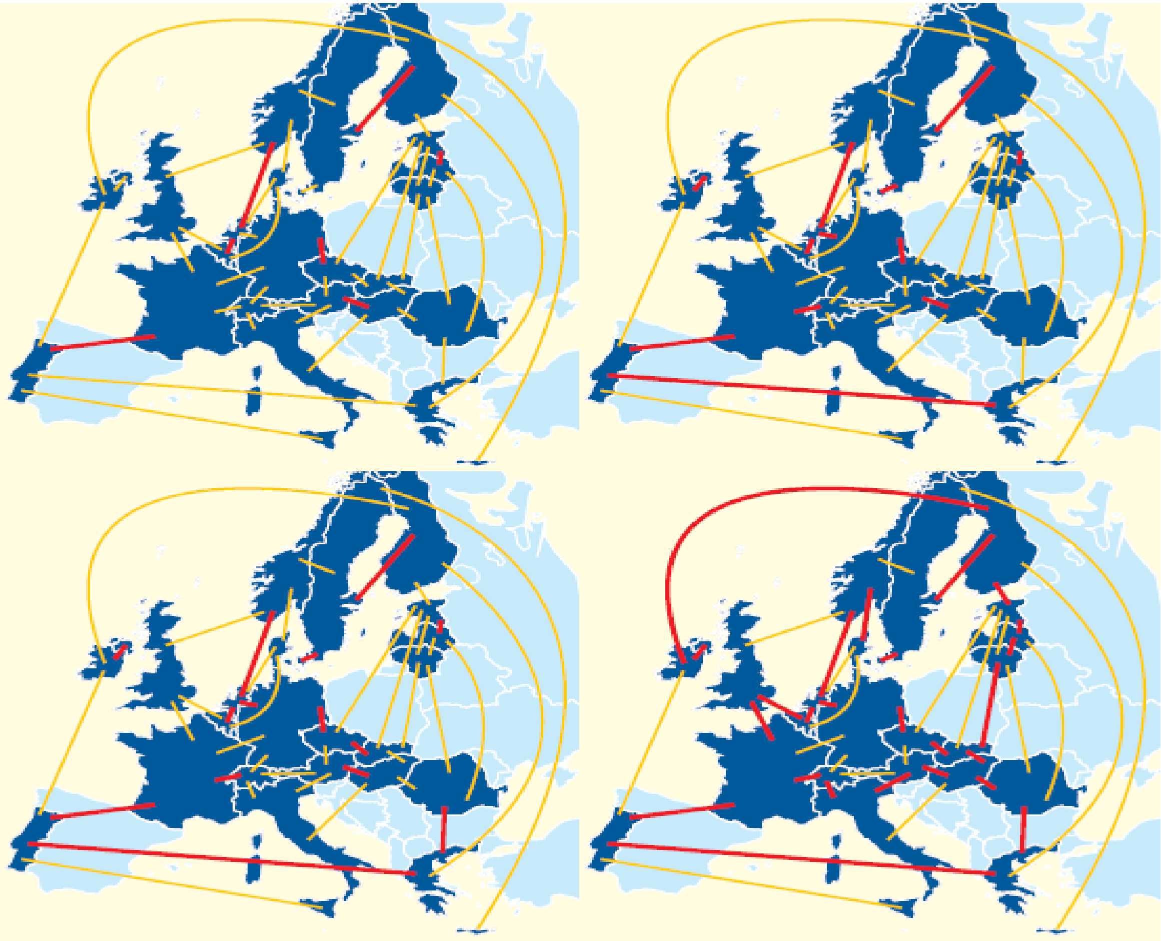


# Scenario overview

- **Attackers:**
  - A hactivist group
- **Motivation:**
  - To bring down European governments and financial institutions
- **How:**
  - Exploit vulnerabilities
  - Create massive botnet
  - Distributed Denial of Service attacks on their public facing online IT systems (e-Gov, e-Tax, eBanking etc)
  - Puzzle solving to enforce cooperation

# CE2012 Findings

- European cooperation procedures worked well
  - But scalability proves a challenge
- A lot of bilateral and multilateral international contacts
- Encrypted information exchange proved to be challenging
- A common operational picture was created with the international teleconferences
- Frequent cooperation and information exchange between public and private sector
- Public-Private cooperation structures are effective
- Real life incidents could affect the exercise(!)



CYBER EUROPE 2010 CYBER EUROPE

www.enisa.euro

# EU Cyber Security Strategy

## § 2.1 Achieving Cyber Resilience

The Commission asks ENISA to:

- Assist the Member States in developing strong national cyber resilience capabilities, notably by building expertise on security and resilience of industrial control systems, transport and energy infrastructure
- Continue supporting  the Member States and the EU institutions in carrying out regular pan-European cyber incidents exercises which will also constitute the operational basis for the EU participation in international cyber incidents exercises.

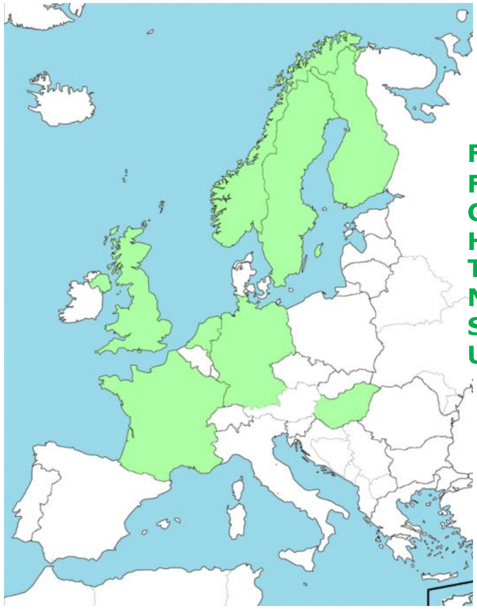
**Example**

# CERT - COMPUTER EMERGENCY RESPONSE TEAM

http://www.enisa.europa.eu/activities/cert

# National/governmental CERTs the situation has changed…

## ESTABLISHED IN 2005:



Finland
France
Germany
Hungary
The Netherlands
Norway
Sweden
United Kingdom

## ESTABLISHED IN 2013:

Armenia
Austria
Belgium
Bulgaria
Croatia
Czech Republic
Denmark
Estonia
Finland
France
Georgia
Germany
Greece
Hungary
Iceland
Ireland
Israel
Italy

Latvia
Lithuania
Luxembourg
Malta
Netherlands
Norway
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Sweden
Switzerland
Turkey
Ukraine
United Kingdom
EU Institutions

- We are building & actively supporting a growing network of national/governmental CERTs
- CERT Interactive MAP:

**http://www.enisa.europa.eu/activities/cert/background/inv/certs-by-country-interactive-map**

# EU Cyber Security Strategy
# § 2.1 Achieving Cyber Resilience

The Commission asks ENISA to:

Examine in 2013 the feasibility of Computer Security Incident Response Teams for Industrial Control Systems (ICS-CSIRTs) for the EU.

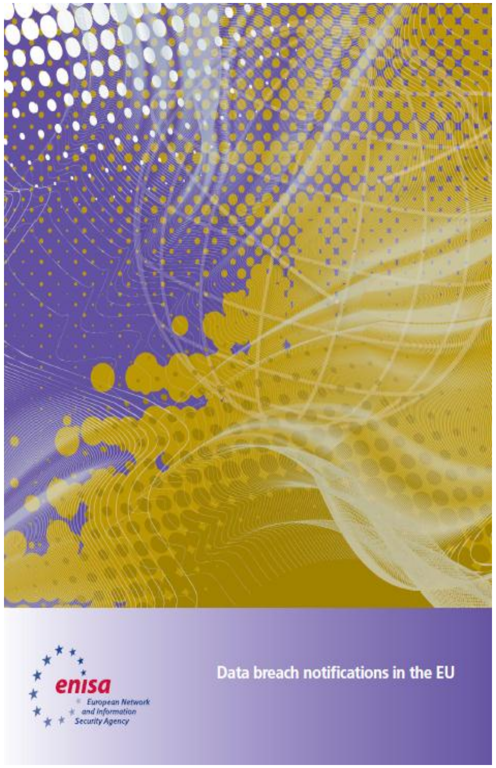
**Example**

Annual Incident Reports 2012

*Analysis of Article 13a incident reports*

enisa

www.enisa.europa.eu



enisa European Network and Information Security Agency

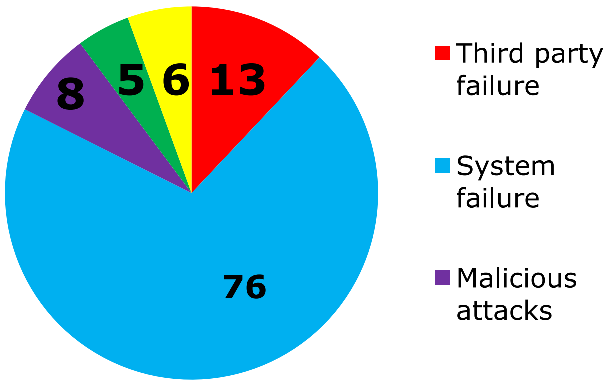
Data breach notifications in the EU

# BREACH NOTIFICATION

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting
http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn

# Major Incidents 2012 - “Article 13a”

- 1st report in 2012 (on 2011’s incidents - 51)
- 2nd report in 2013 (on 2012’s incidents);
- 79 incidents from 18 countries,
- 9 countries without incidents,
- 1 country without implementation (9 in 2011)
- Most incidents affect mobile comms (50% of incidents, 1.8 Mn/incident)
  - Natural disaster, power cuts outages affected 2.8 Mn/incident
- Ca 40% impact on emergency number 112



https://www.enisa.europa.eu/media/press-releases/new-major-incidents-in-2012-report-by-eu-cyber-security-agency-enisa

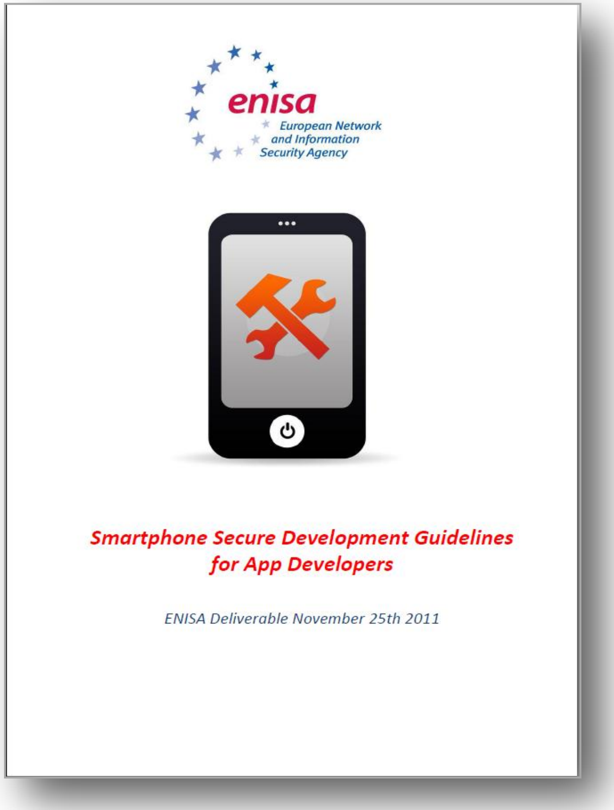
Example

# SECURING NEW BUSINESS MODELS & NEW TECHNOLOGIES

# Smartphone Security

ENISA report:

- Guide for developers on how to develop secure apps
- Presents top 10 controls to implement, based on the top 10 most important risks for mobile users



enisa
European Network
and Information
Security Agency

*Smartphone Secure Development Guidelines for App Developers*

*ENISA Deliverable November 25th 2011*

http://www.enisa.europa.eu/act/application-security/smartphone-security-1/smartphone-secure-development-guidelines

# Cloud Computing

Objectives for Cloud Computing:

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

Report defines minimum baselines for:

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

Cloud Computing

November | 09

Benefits, risks and recommendations for information security

www.enisa.europa.eu/act/application-security/rm/files/deliverables/cloud-computing-risk-assessment

# Smart Grid Security

ENISA recommendations include:

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

enisa
European Network
and Information
Security Agency

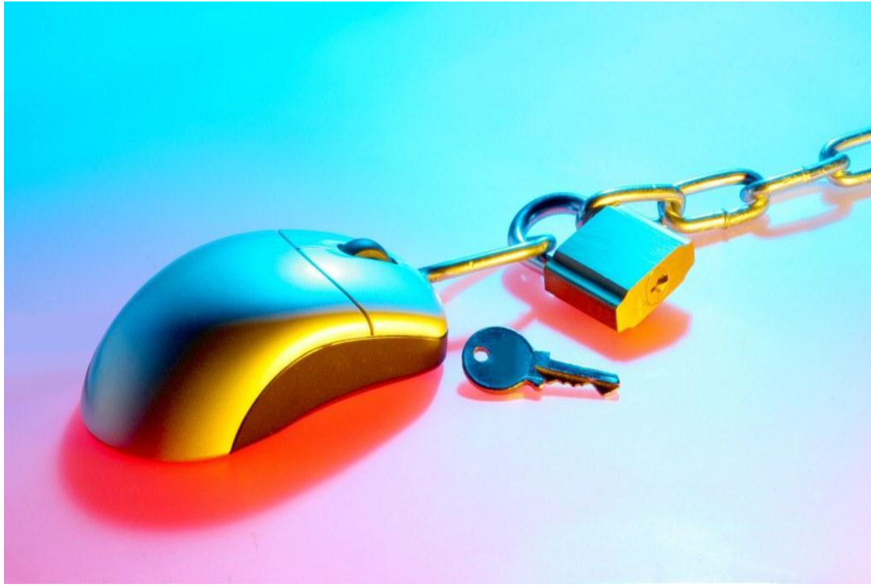
Smart Grid Security

Recommendations for Europe and Member States

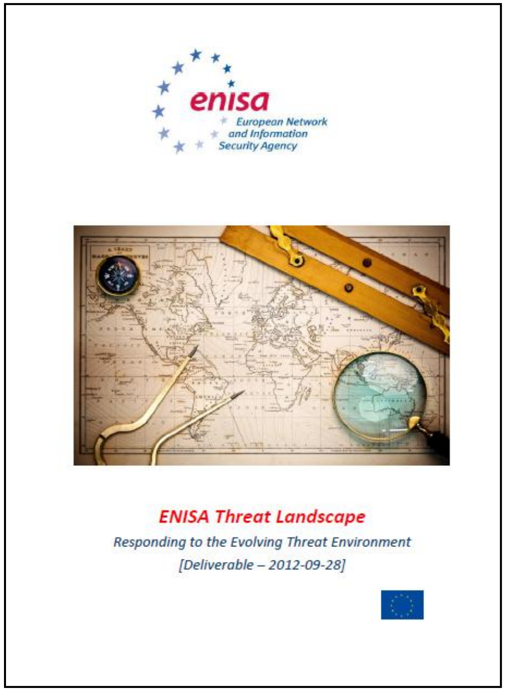
[Deliverable – 2012-07-01]

www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA-smart-grid-security-recommendations

# EU Cyber Security Strategy § 2.4 Promoting a Single Market for Cybersecurity Products



The Commission asks ENISA to:
Develop, in cooperation with relevant national competent authorities, relevant stakeholders, International and European standardisation bodies and the European Commission Joint Research Centre, technical guidelines and recommendations for the adaptation of NIS standards and good practices in the public and private sectors.



enisa
European Network
and Information
Security Agency

ENISA Threat Landscape

Responding to the Evolving Threat Environment

[Deliverable – 2012-09-28]

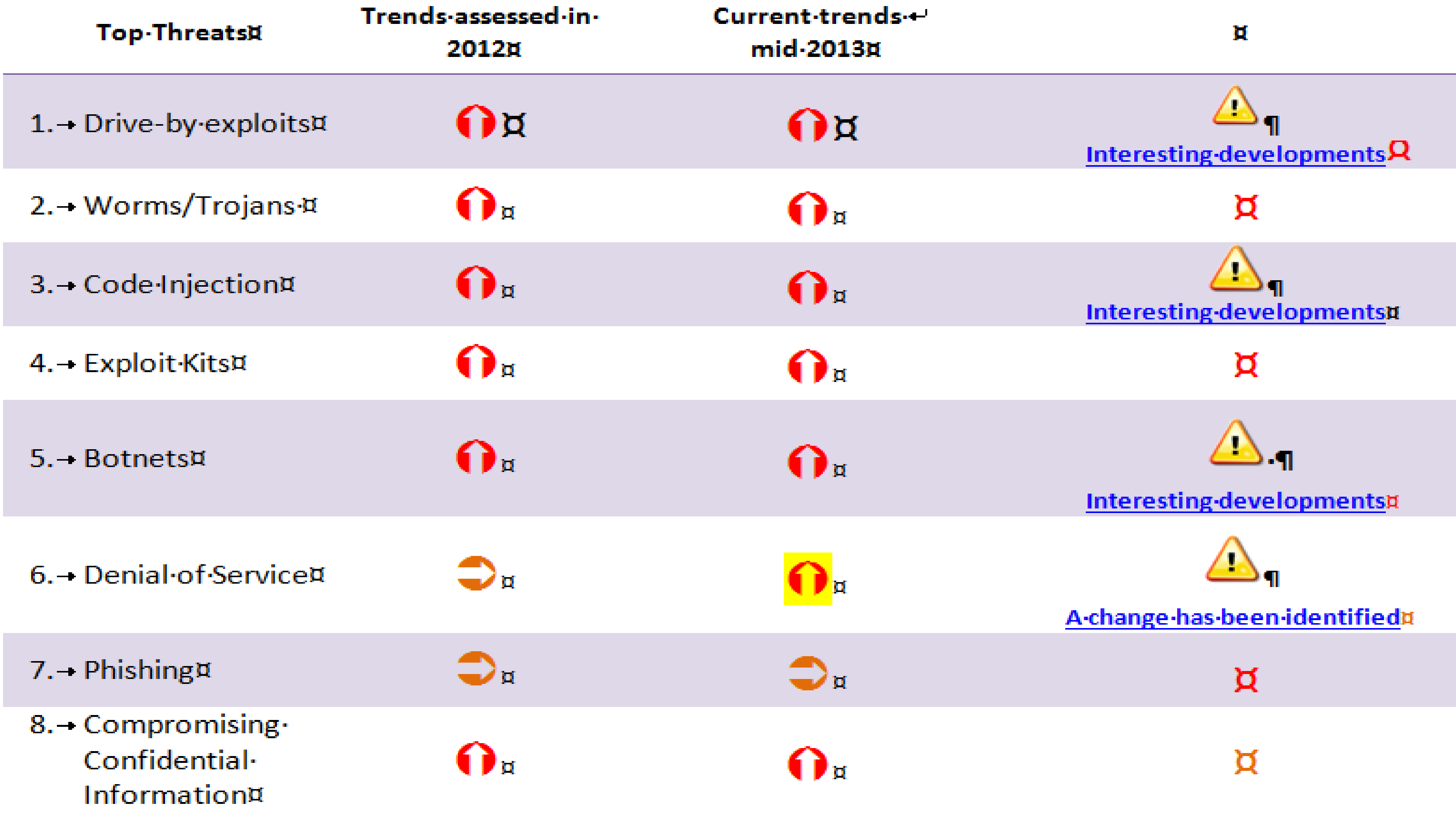
## Example

# SECURITY LANDSCAPE

***Risk =***
***Asset, Threat****,* ***Impact***

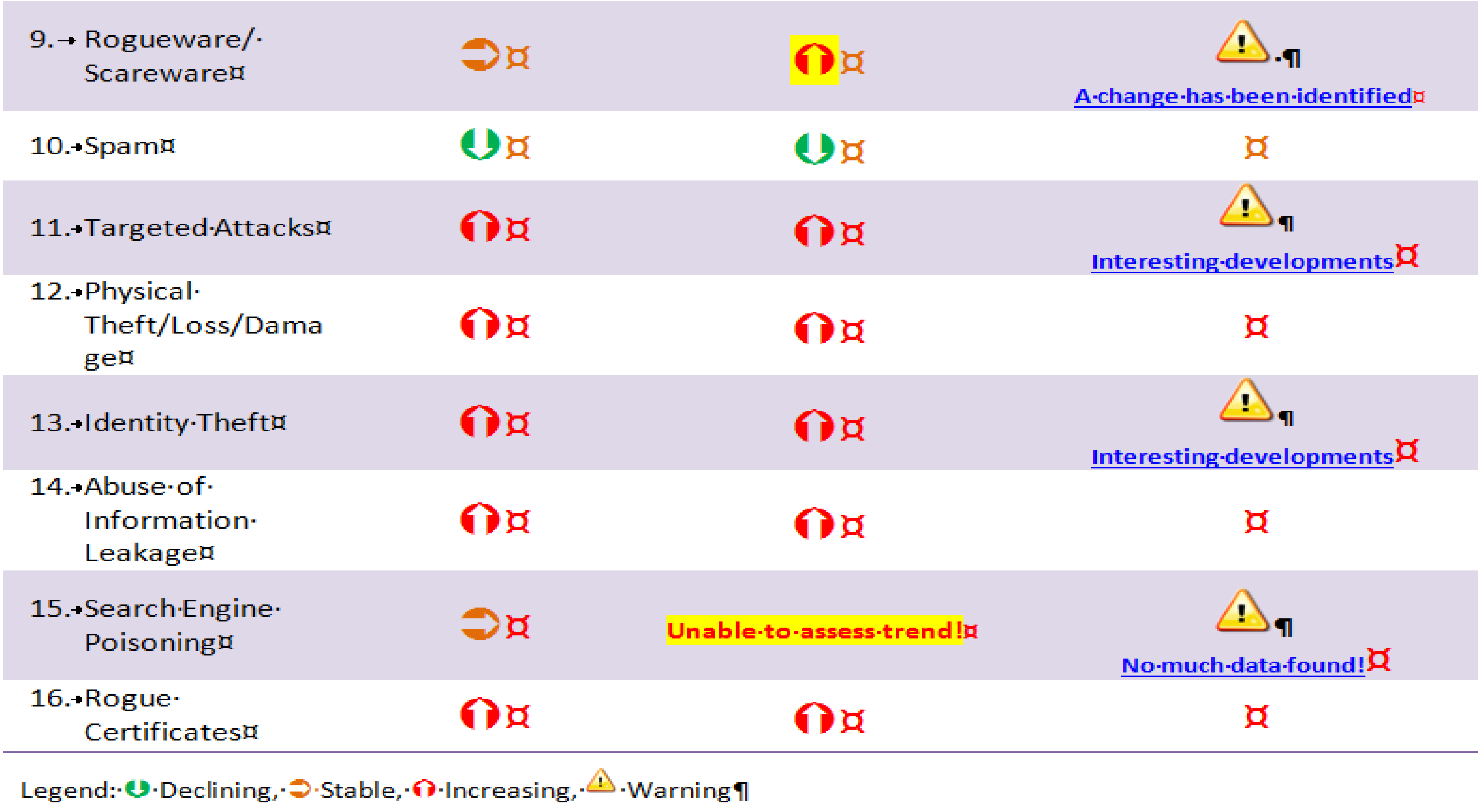
http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape

# Threats & Trends (1)



| Top·Threats¤ | Trends·assessed·in·<br>2012¤ | Current·trends·↵<br>mid·2013¤ | ¤ |
|---|---|---|---|
| 1.→ Drive-by-exploits¤ | ↑¤ | ↑¤ | ⚠¶<br>Interesting·developments¤ |
| 2.→ Worms/Trojans·¤ | ↑¤ | ↑¤ | ¤ |
| 3.→ Code·Injection¤ | ↑¤ | ↑¤ | ⚠¶<br>Interesting·developments¤ |
| 4.→ Exploit·Kits¤ | ↑¤ | ↑¤ | ¤ |
| 5.→ Botnets¤ | ↑¤ | ↑¤ | ⚠·¶<br>Interesting·developments¤ |
| 6.→ Denial·of·Service¤ | →¤ | ↑¤ | ⚠¶<br>A·change·has·been·identified¤ |
| 7.→ Phishing¤ | →¤ | →¤ | ¤ |
| 8.→ Compromising·<br>Confidential·<br>Information¤ | ↑¤ | ↑¤ | ¤ |

# Threats & Trends (2)



| | | | |
|---|---|---|---|
| 9. Rogueware/ Scareware | ➡ | ⬆ | ⚠<br>A change has been identified |
| 10. Spam | ⬇ | ⬇ | |
| 11. Targeted Attacks | ⬆ | ⬆ | ⚠<br>Interesting developments |
| 12. Physical Theft/Loss/Damage | ⬆ | ⬆ | |
| 13. Identity Theft | ⬆ | ⬆ | ⚠<br>Interesting developments |
| 14. Abuse of Information Leakage | ⬆ | ⬆ | |
| 15. Search Engine Poisoning | ➡ | Unable to assess trend! | ⚠<br>No much data found! |
| 16. Rogue Certificates | ⬆ | ⬆ | |

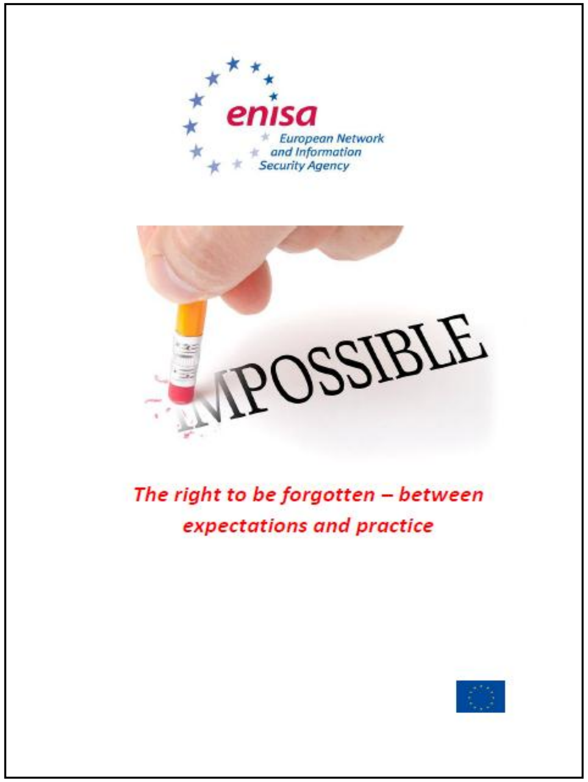
Legend: ⬇ Declining, ➡ Stable, ⬆ Increasing, ⚠ Warning

*Figure 1: Overview of Trends assessed in 2012 vs. 2013 mid-year*

# EU Cyber Security Strategy
## § 2.4 Fostering R&D investments & innovation

The Commission asks Europol and ENISA to:

Identify emerging trends and needs in view of evolving cybercrime and cybersecurity patterns so as to develop adequate digital forensic tools and technologies.



enisa

European Network
and Information
Security Agency

The right to be forgotten – between expectations and practice

## Example

# PRIVACY

http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten?searchterm=The+right+to+be+forgotten

# “The Right To Be Forgotten” - *between expectations & practice*

- Included in proposed EC regulation of Jan 2012 on “the processing of personal data & on free movement of such data”
- ENISA addressed technical means of assisting enforcement of ”the right to be forgotten”
- A purely technical & comprehensive solution to enforce the right in open Internet is not possible
- Technologies do exist that minimize amount of personal data collected & stored online

➢ Personal Data is the new currency in Cyberspace !

# European Cyber Security Month (ECSM) Kick Off Event 11th of Oct, Brussels

European Cyber Security Month is an EU advocacy campaign that takes place in October. The ECSM aim is to promote cyber security awareness among citizens, to modify their perception of cyber threats and to provide updated security information through education, good practices and competitions.

ENISA role to brokerage

Lithuanian Presidency of the Council of the European Union 2013

For further information: http://cybersecuritymonth.eu/ Twitter @enisa_eu and @CyberSecMonth #OctoberNIS #CyberSecMonth

http://www.enisa.europa.eu/activities/identity-and-trust/whats-new/european-cyber-security-month-ecsm-kick-off-event

# Contact details

**European Union Agency for Network and Information Security**
**Science and Technology Park of Crete**
**P.O. Box 1309**
**71001 Heraklion**
**Crete**
**Greece**

**http://www.enisa.europa.eu**

Follow us on: