GR
2014
eu

Hellenic Presidency of the Council
of the European Union

Cyber security initiatives in European Union and Greece

The role of the Regulators

Constantinos Louropoulos

President of Hellemic Telecoms and Post Commission

EETT

HELLENIC TELECOMMUNICATIONS & POST COMMISSION

Agenda

- Cyberspace challenges
- EU security initiatives
- EU strategic priorities
- Achieving cyber resilience in European Union
- ENISA – An Agency for pan-European cooperation
- Greece – Authorities and Responsibilities

Cyberspace

- has an impact on all parts of **society** and key sectors of **economy**
- should remain **open, free and safe**, protected by incidents and misuse
- it is **vulnerable**; cyber security incidents can disrupt the supply of essential services (water, healthcare, electricity, mobile services, government services, bank transactions, etc.)

Cyber security involves practically everyone:

governments, private companies, organisations, banks, institutions, citizens and many other organised groups of interest.

GR 2014 eu

Hellenic Presidency of the Council of the European Union

EETT

HELLENIC TELECOMMUNICATIONS & POST COMMISSION

Cyber security initiatives in EU

*The strategy of the EU: **"An Open, Safe and Secure Cyberspace"***

The EU's vision and the actions required to make the EU's online environment the safest in the world:

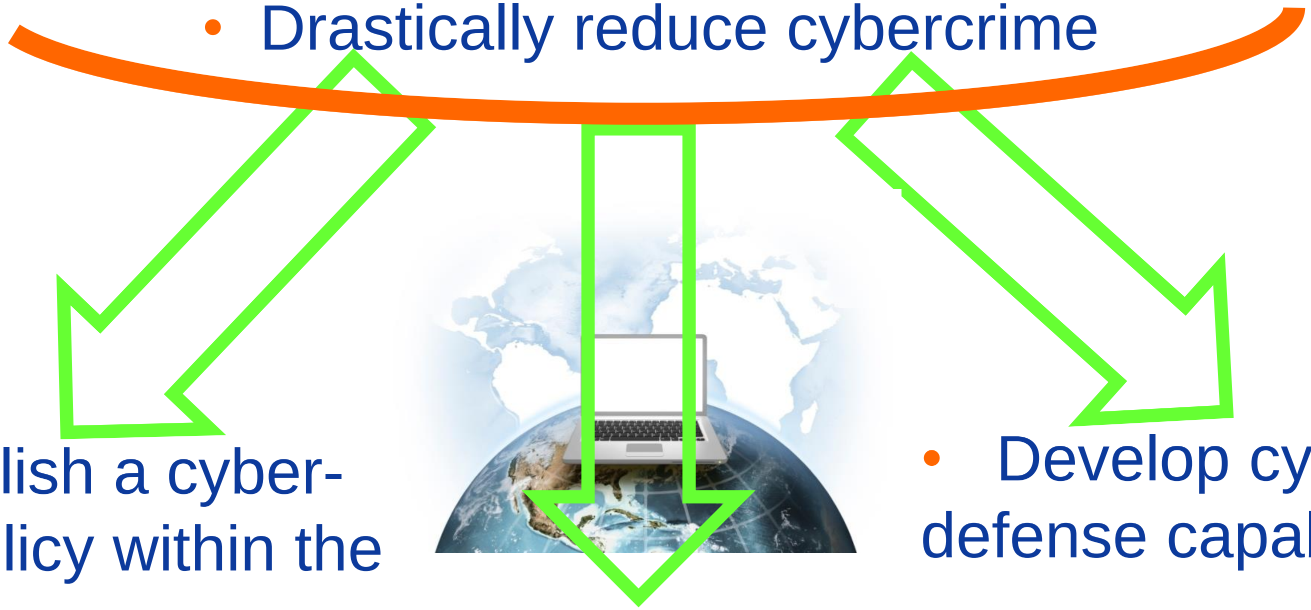
- defines **principles** for cyber security
- Suggests strategic **priorities** and **actions**
- addresses **international cooperation** as a key priority

GR
2014
eu
Hellenic Presidency of the Council
of the European Union

EETT
HELLENIC TELECOMMUNICATIONS & POST COMMISSION

EU Strategic priorities

- Achieve cyber resilience
- Drastically reduce cybercrime



- Establish a cyber-space policy within the EU.
- Develop cyber defense capabilities
- Develop the industrial and technology resources for cyber security

EU initiatives – Achieving cyber resilience

Proposal for a Directive on a common high level of Network and Information Security (NIS)

Establish common minimum requirements for NIS at national level.
The Member States will be obliged to:

- designate national competent authorities for NIS
- set up a well functioning CERT (Computer Emergency Response Team)
- adopt a national NIS strategy and a national NIS cooperation plan.
- Enable information sharing and mutual assistance among the national NIS competent authorities

EU initiatives – Achieving cyber resilience

Proposal for a Directive on a common high level of network and Information Security (NIS)

Players in a number of key areas (energy, transport, banking, stock exchanges etc)

- Assess cyber security **risks**, ensure n/w and information systems are reliable and resilient via appropriate **risk management**
- **Report incidents** to the national NIS authorities, incidents with significant impact on the continuity of core services and supply of goods, relying on n/w and information systems

EU initiatives – Achieving cyber resilience

Framework Directive – Article 13a and b of Directive 2002/21/EC

(as amended by 2009/140 Directive)

Member States shall ensure that providers of Networks:

- Take measures and manage risks posed to security of networks and services.
- Guarantee the integrity of their networks,& ensure continuity of supply of services
- Notify the competent National Regulatory Authority of a breach of security or loss of integrity

Implementation by the Member States

- Transposition in national law
- Issuance of specific regulation
- Implementation of art 13 facilitated by ENISA

ENISA
Achieving cyber resilience

ENISA: European Union Agency for Network and Information Security

- The Agency's Mission is essential to achieve a high and effective level of Network and Information Security within the European Union.
- Together with the EU-institutions and the Member States, ENISA seeks to develop a culture of Network and Information Security for the benefit of citizens, consumers, business and public sector organisations in the European Union.
- ENISA is helping the European Commission, the Member States and the business community to address, respond and especially to **prevent** Network & Information Security problems.

ENISA
Achieving cyber resilience

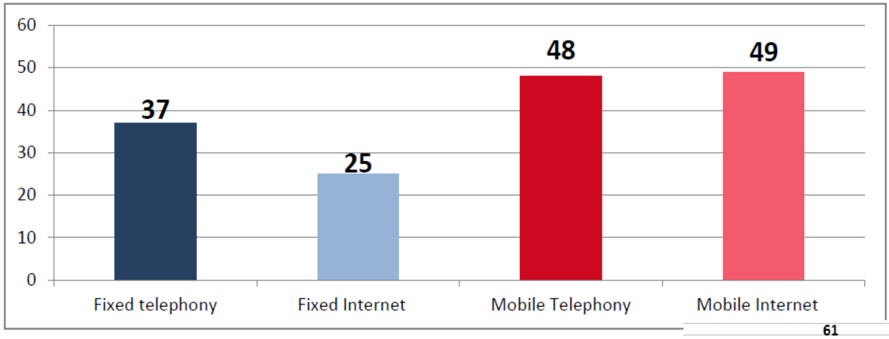
Framework Directive – Article 13a and b of Directive 2002/21/EC

Publishes an annual report to provide industry and government bodies in the EU with data about significant incidents.

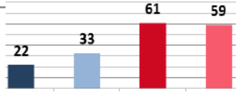
Once a year, NRAs submit to the Commission and ENISA a summary report of the breach notifications received.

Reports are submitted according to ENISA's guidelines "Technical Guidelines for Incident Reporting".

ENISA - Annual Incident Reports 2012



Incidents per service (percentage)



(2011)

- Mobile networks (mobile telephony or mobile Internet) most affected: about 50 % of the incidents respectively.
- Mobile network outages affect many users (around 1,8 million users per incident).
- Emergency Services are affected by incidents: In 37 % of the incidents there was impact on emergency calls using the emergency number 112.

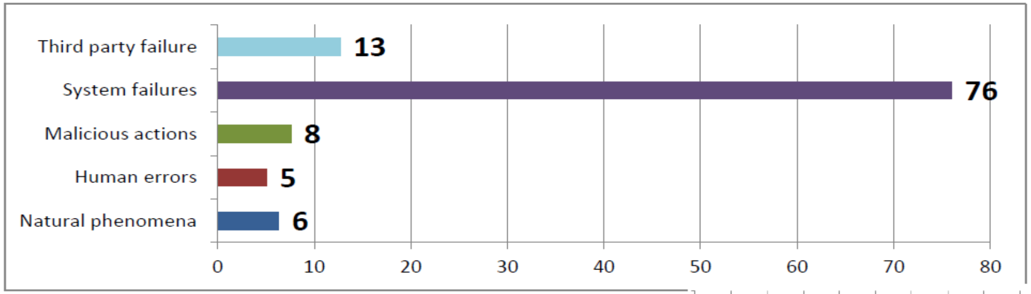
Source: ENISA - Annual Incident Reports 2012
Analysis of Article 13a annual incident reports
August 2013

GR
2014
eu
Hellenic Presidency of the Council
of the European Union

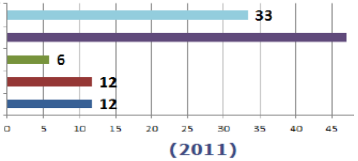
EETT
HELLENIC TELECOMMUNICATIONS & POST COMMISSION

ENISA - Annual Incident Reports 2012

- 76 % System failures. Assets most affected were **switches (e.g. routers and local exchange points)** and home location registers.
- Incidents categorized with root cause third party failures, mostly power supply failures, affected around **2.8 Million user connections** on average.
- **Natural phenomena** cause long lasting incidents: Incidents caused by natural phenomena (mainly storms and heavy snowfall) lasted around 36 hours on average.
- **Overload and power failures** have most impact in terms of number of users and time duration.



Incidents per root cause category (percentage).



Source: ENISA - Annual Incident Reports 2012 Analysis of Article 13a annual incident reports August 2013

GR 2014 eu

Hellenic Presidency of the Council of the European Union

EETT

HELLENIC TELECOMMUNICATIONS & POST COMMISSION

Cyber Security Management in Greece

CERT name	Date of establishment	Constituency	Additional information
NCERT-GR		National / Governmental	www.cert.gov.gr
AUTH-CERT	Q2 2004	Research and Education	www.auth.gr
FORTHcert	Q3 2007	Service Provider	www.forth.gr/forthcert
GRNET-CERT	Q2 2000	Research and Education	http://cert.grnet.gr

Organization	Responsibilities	Additional information
ADAE **“Privacy”**	Assurance of wired, wireless and mobile communications privacy	www.adae.gr
EETT **“Telecoms”**	Regulation and supervision of telecommunications and postal market	www.eett.gr
DPA **“Data”**	Protection of personal data	www.dpa.gr
Hellenic Police	Prevention, investigation and repression of crimes that are committed through means of electronic communication	http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=8194&Itemid=378&lang=

Implementation of Article 13 in Greece

Hellenic Authority for Communication Security and Privacy (ADAE)

- Issues regulation related to the security measures according to art 13
- Performs audits related to conformity with aforementioned regulation
- Forwards audit reports to EETT

GR 2014 eu

Hellenic Presidency of the Council of the European Union

EETT

HELLENIC TELECOMMUNICATIONS & POST COMMISSION

Implementation of Article 13 in Greece

Hellenic Telecommunications and Post Commission (EETT)

- Receives significant incident reports from providers in the context of art 13a and forwards them to ADAE
- Submits to ENISA the annual report
- May issue binding instructions related to the security measures of art. 13
- May ask from operators related data in order to assess conformity with security measures of art.13

Moreover:

- Produces regulation according to Directive 2002/22 related to the availability of telephone services in cases of force majeure and catastrophic network breakdown
- Performs audits related to conformity with regulation

GR 2014 eu
Hellenic Presidency of the Council of the European Union

EETT
HELLENIC TELECOMMUNICATIONS & POST COMMISSION

EETT in more detail…

EETT is responsible for the management and assignment of the **.gr Domain Names**

- If a law enforcement agency detects webpages with illegal content, EETT can order the hosting provider to **remove this webpage**
- If the hosting provider cannot be located and the domain name of the web page is a *.gr* domain name, the law enforcement agency can order EETT at first to **temporarily deactivate** the assigned domain name and secondarily to delete the assigned domain name.
- In cases where the webpage is not hosted in Greece and the domain name is not .gr domain name, access of users in Greece to this webpage via the ISPs **can be blocked.**

GR
2014
eu
Hellenic Presidency of the Council
of the European Union

EETT
HELLENIC TELECOMMUNICATIONS & POST COMMISSION

Greece: Police Cybercrime Division

A Division of Hellenic Police.
Mission: to prevent, investigate and repress crimes that are committed through the internet or other means of electronic communication.

The cybercrime unit, among others, deals with:

- crimes against juveniles,
- illegal penetration in computer systems,
- theft, destruction or illegal transport of software, digital data or audiovisual material,
- crimes against the privacy of electronic communications

Source: Cybercrime unit webpage

GR 2014 eu
Hellenic Presidency of the Council of the European Union

EETT
HELLENIC TELECOMMUNICATIONS & POST COMMISSION

Thank you for your attention

Costas Louropoulos

President of EETT

GR
2014
eu
Hellenic Presidency of the Council
of the European Union

EETT
HELLENIC TELECOMMUNICATIONS & POST COMMISSION