The EU approach to Cybersecurity and Cybercrime

Ralf Bendrath
Policy advisor to Jan Philipp Albrecht MEP, Greens/EFA

ISODARCO.it, 12 January 2012

Outline

1. Information & Coordination
2. Internal Security Strategy
3. „Virtual Schengen Border“
4. Criminal Law

1) Information & Coordination

mostly DG INFSO,

Commissioner Neelie Kroes

ENISA

European Network and Information Security Agency

ENISA

- European Network and Information Security Agency
- Set up by Regulation (EC) 460/2004, 10 March 2004
- Operations in Heraklion, Crete, since September 2005
- around 50 staff

EUROPEAN COMMISSION

Brussels, 30.9.2010
COM(2010) 521 final

2010/0275 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

Concerning the European Network and Information Security Agency (ENISA)

ENISA revision

- mostly about the location
  - no direct flights to Brussels
  - no international school
- Deal: offices elsewhere, too
  - staff in Athens, liaison in Brussels
- mandate will be widened
  - cooperation with law enforcement
- but no CERT coordination role
  - we tried…

EU-CERT

- Computer Emergency Response Team for the EU institutions
  - pre-configuration Team, June 2011
  - full-scale CERT expected in June 2012
- based on “Digital Agenda for Europe“
- Member states shall set up CERTS
  - Council conclusions, May 2011

2) Internal Security Strategy

DG HOME

Commissioner Cecilia Malmström

Internal Security

- Cybersecurity among 5 priorities of EU Internal Security Strategy (Council, 2010)
  1. Serious and organised crime
  2. Terrorism
  3. Cybercrime
  4. Border Security
  5. Natural and man-made disasters
- Action Plan (COM, 11/2010)

Action Plan

- Coordination / Law Enforcement
  - existing High Tech Crime Centre at Europol
  - New Cybercrime Centre „within existing structures“ (2013)
- Reporting
  - Cybercrime Alert Platform / Safer Internet Prg
- Resilience
  - European Public-Private Partnership for Resilience (EP3R)

Action Plan

- „Illegal Content“
  - Contact Initiative against Cybercrime for Industry and Law Enforcement (CICILE)
  - Notice & take-down guidelines (2012)
  - „radicalisation“ and „intellectual property theft“ (!)
- Incident response
  - ENISA, national CERTs
  - European Information Sharing and Alert System (EISAS) (2013)
  - „Member states should develop national contingency plans“

Issues

- No real coordination
  - No EU-wide CERT coordination
  - Institutional competition between ENISA, Europol and others
  - Member states are left to themselves
- Heavy involvement of industry
  - Private-public partnerships = private policing?
  - Defence industry is smelling new income
  - Regulatory capture

4) „Virtual Schengen Border“

Hungarian Presidency

1st half 2011

Council Law Enforcement WP

- Outcome of proceedings, 17 February 2011

- 8. Cybercrime
  The Presidency of the LEWP presented its intention to propose concrete measures towards creating a single secure European cyberspace with a certain "virtual Schengen border" and "virtual access points" whereby the Internet Service Providers (ISP) would block illicit contents on the basis of the EU "black-list".

ISPs as „border crossing points“

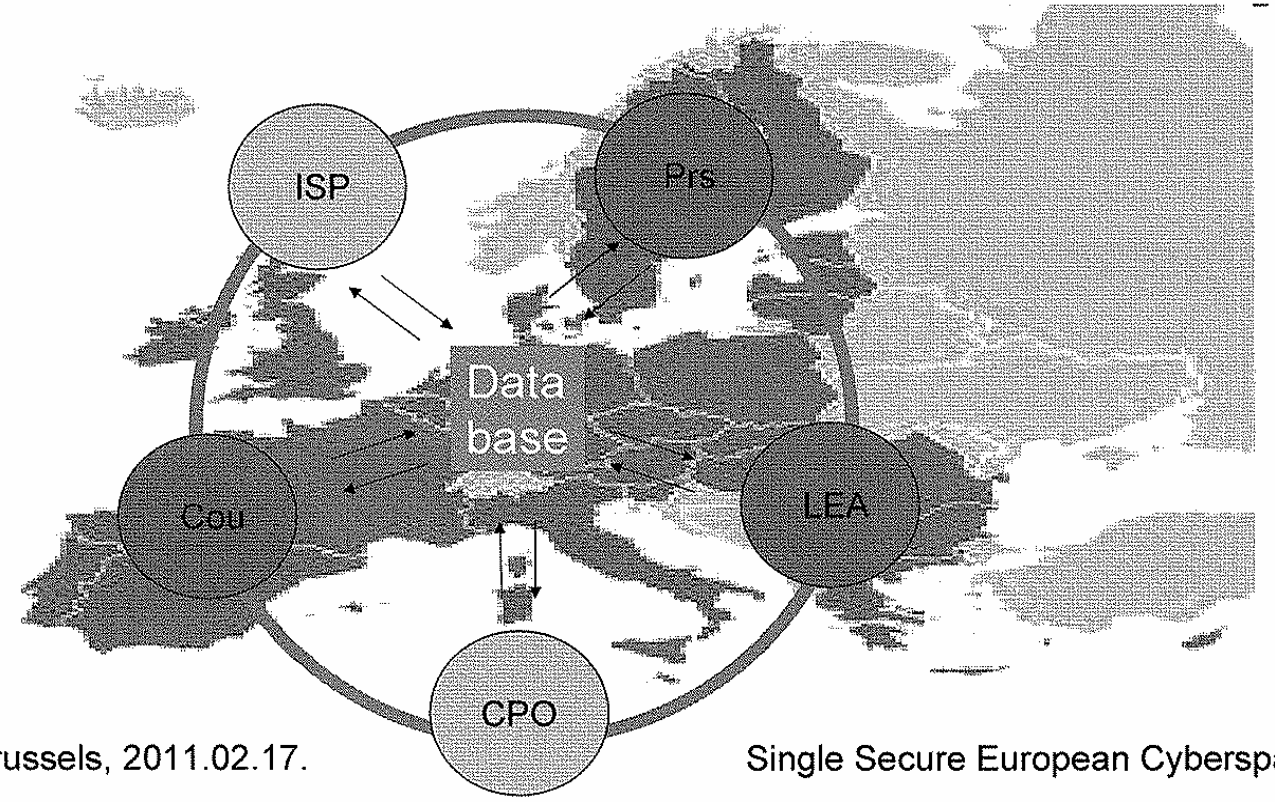
At the real Schengen borders, border guards stop the persons, who want to enter without a required permit, similarly – at the “virtual access points” of the ISP’s of the EU, illicit contents can be stopped that violate EU norms.

The Internet Service Providers are the virtual “border crossing points” at the EU’s computer technology and internet „borders”.

Considering that the Internet - as a network - provides several ways to access the content, the action can only be effective, if all the ISPs located in the EU use it in a coordinated manner, and at the same time.
For updating, “maintaining” the “black-lists”, the support and contribution is necessary from the law enforcement and judicial authorities and NGOs operating in that area.

Blacklist database

The common EU-database, regarding the illegal contents on the whole Internet – should be accesible only by the partners



Backpaddling

Council Law Enforcement WP

- Outcome of proceedings, 17 February 2011
- Corrigendum

- **The Hungarian expert** presented **certain ideas** relating to a single secure European cyberspace with a certain "virtual Schengen border" and "virtual access points" whereby the Internet Service Providers (ISP) **c**ould block illicit contents, **in particular websites publishing paedophile material**, on the basis of an EU "black-list".

Happy ending

- The proposal was immediately as dead as it could possibly be.
- Internet blocking was not made mandatory in the child abuse directive.
- But beware of ACTA, N & TD, ...
- Example of „border control“ mind-set?

4) Criminal Law

DG HOME

Commissioner Cecilia Malmström

Cybercrime Convention

- Council of Europe Conventio 185 (2001)
- contested by NGOs
  - possession of hacker tools
  - copyright violations
  - additional protocol on „publication of racist and xenophobic propaganda via computer networks“
- ratified by 18 EU member states

(Acts adopted under Title VI of the Treaty on European Union)

COUNCIL FRAMEWORK DECISION 2005/222/JHA

of 24 February 2005

on attacks against information systems

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Articles 29, 30(1)(a), 31(1)(e) and 34(2)(b) thereof,

Having regard to the proposal from the Commission,

Having regard to the opinion of the European Parliament [1],

(5) Significant gaps and differences in Member States' laws in this area may hamper the fight against organised crime and terrorism, and may complicate effective police and judicial cooperation in the area of attacks against information systems. The transnational and borderless character of modern information systems means that attacks against such systems are often trans-border in nature, thus underlining the urgent need for further action to approximate criminal laws in this area.

EUROPEAN COMMISSION

Brussels, 30.9.2010
COM(2010) 517 final

2010/0273 (COD)

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on attacks against information systems and repealing Council Framework Decision 2005/222/JHA

New Cyber-Attacks Directive

- Higher penalties (up to 5 years instead 3)
- „Illegal interception“ criminalised
- Hacker „devices“ criminalised
- More aggravating circumstances
  - before: only when organised crime
  - now: when using stolen identity or botnets
- 24/7 contact points
- reporting / statistics

Our response

- Who believes penalties have any effect?
- hacker „devices“ - WTF?
- Don‘t criminalise using neighbour‘s wifi
- ID theft should be left to other instruments
- Protect benign hackers as immune system
- In general, strengthen prevention
  → extenuating / alleviating circumstances
  → Liability for operators / vendors

Draft Amendments

Article 3 Illegal Access to Information Systems

1. Member States shall take the necessary measures to ensure that**, when committed intentionally,** the intentional access, without right – meaning entering the whole or any part of an information system – is punishable as a criminal offence, ~~**at least**~~ for cases which are not minor.

2. **The conduct referred to in paragraph 1 shall be incriminated only where the offence is committed by infringing a security measure and provided that the operator or vendor of the system is not informed of the vulnerability afterwards.**

Draft Amendments

Art. 11 (New) Duty to Care

4. Where legal persons are considered to have failed to provide a reasonable level of protection (…), and where these offenses are considered to have been carried out with clear criminal intent, then these offenses will be considered to have been carried out under alleviating circumstances when applying criminal penalties.

5. Where legal persons have clearly failed to provide a reasonable level of protection (…), and in cases where the damage caused as a result of this failure is considerable, then Member States shall ensure that is possible to prosecute this legal person under the provisions of Article 8 paragraph 1 *[instigating, aiding and abetting]*.

Our tactics

- Bring in the hackers!
- LIBE committee hearing, 4th October 2010
  - CCC member „Scusi“ presented
  - first contact with hacker for many officials
  - He is now in high demand
- Quite successful
- But:
  - Nobody willing to address liability issue
  - Malmström: „afraid of Microsoft“

Timing

- Draft report presented today in Committee
- Deadline for amendments: 26th Jan, 17:00
- Committee vote: 28th Feb
- Then trilogue with Council & Commission
- Agreement and plenary vote: late 2012

Summary

Typical approach?

- No real coordination
- Addressing symptoms
- Public-private partnership ideology
- Shying away from hard measures
- Border control ideology

- Typical for EU and for „cyber“ policies?
- We try to fix what we can…

Thanks for listening!

ralf.bendrath@europarl.europa.eu
http://bendrath.blogspot.com
@bendrath