Update to the Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries for assisting Computer Security Incident Response Teams (CSIRTs)

ENISA Workshop December 2005
Brussels

Dr Lorenzo Valeri & Neil Robinson,
RAND Europe

Outline of presentation

- The challenges of cyber-crime in Europe
- The need for the CSIRT Legal Handbook
- Aims
- The evolution of the project
- Findings
  – Part 1: Breadth & depth of law
  – Part 2: Sanctions
- Conclusions
- Demo of the CD-ROM & website

Why a Legal Handbook for CSIRTs?

- **“In the eEurope Action Plan 2005 the enhancement of Europe’s CSIRT’s is a pivotal step in fostering the development of European secure information infrastructures.”**
- **Trust is key for progressing the information society**
  - **A key is to bridge the gap between the technical people at the operational level and the lawyers who must deal with the after-effects**
- **The Handbook helps understand these legal issues**

The challenge of cyber-crime in Europe

- **Incidents are cross border**
- **Legal frameworks differ**
  - **What may be illegal and highly punishable in one country is legal in another**
- **Better co-operation is needed**
  - **Operationally, between the technical experts and the lawyers**
  - **For policy makers: to design appropriate & relevant policy**

The need for the Legal Handbook

- **Can a prosecution be launched?**
  - **E.g. Account Compromise is not illegal in Spain**
- **What can we expect to get?**
  - **Type of sanction – administrative or penal?**
  - **Length of sentence?**
- **Who do we talk to?**
  - **What Law Enforcement agencies exist? What are they responsible for? Are there other reporting mechanisms?**
- **Is it worth the effort?**
  - **Have we already destroyed the evidence?**
- **Are there any special considerations we need to be aware of?**
  - **For example: in regard to forensics?**

Aim of the project

- Produce an update of the 2003 Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries
  - Take into account recent developments in legal framework of EU
  - Extend its scope to ten new Member States
- The Handbook will be available in print and on line.

What we found – national law + sanctions

- Varying degrees of response amongst the MS
- Some misuses are not illegal (especially Target Fingerprinting)
- Some are punishable by many different pieces of law
- Universal presence of anti-spam legislation
- Punishments vary
  - Fines are commonplace
  - Prison sentences vary from 1-15 years for serious offences (e.g. Unauthorised Modification of Information)

What we found - 2

- Rapidly evolving environment:
  - Council of Europe Convention on Cyber-Crime
  - EU Framework Decision on Attacks against Information Systems
- More administrative provisions were present than in the previous Handbook
- Many countries still rely exclusively upon penal sanctions

What we found - 3

- Reporting capabilities vary across the MS
  - E.g. in BE, NL and UK there are good models
  - Many, however, only have set-ups for reporting illegal content

- CSIRTs & CERTs
  - CSIRTs / CERTs are understandably quite inward looking & difficult to reach
  - Most CSIRTs / CERTs are still public sector (either university or govt based)
  - Constituencies are small & v. focused

What we found - 4

- **Most Law Enforcement reporting goes via Europol / Interpol contact points**
  - **Need to keep up to date contact points and effective communication**
- **CSIRTs refer to their own Law Enforcement first in cross border incidents**
  - **Is this effective?**
  - **Can this be sped up?**

Detailed legislative analysis

- The following charts reflect
  - The options available to lawyers for a particular incident (i.e. the breadth of law available for them to use) in each Member State
  - Consistency of the breadth (how much law) and gaps (legality and illegality) in the law across the Member States
  - The maximum penal sanctions available for each incident, in each Member State

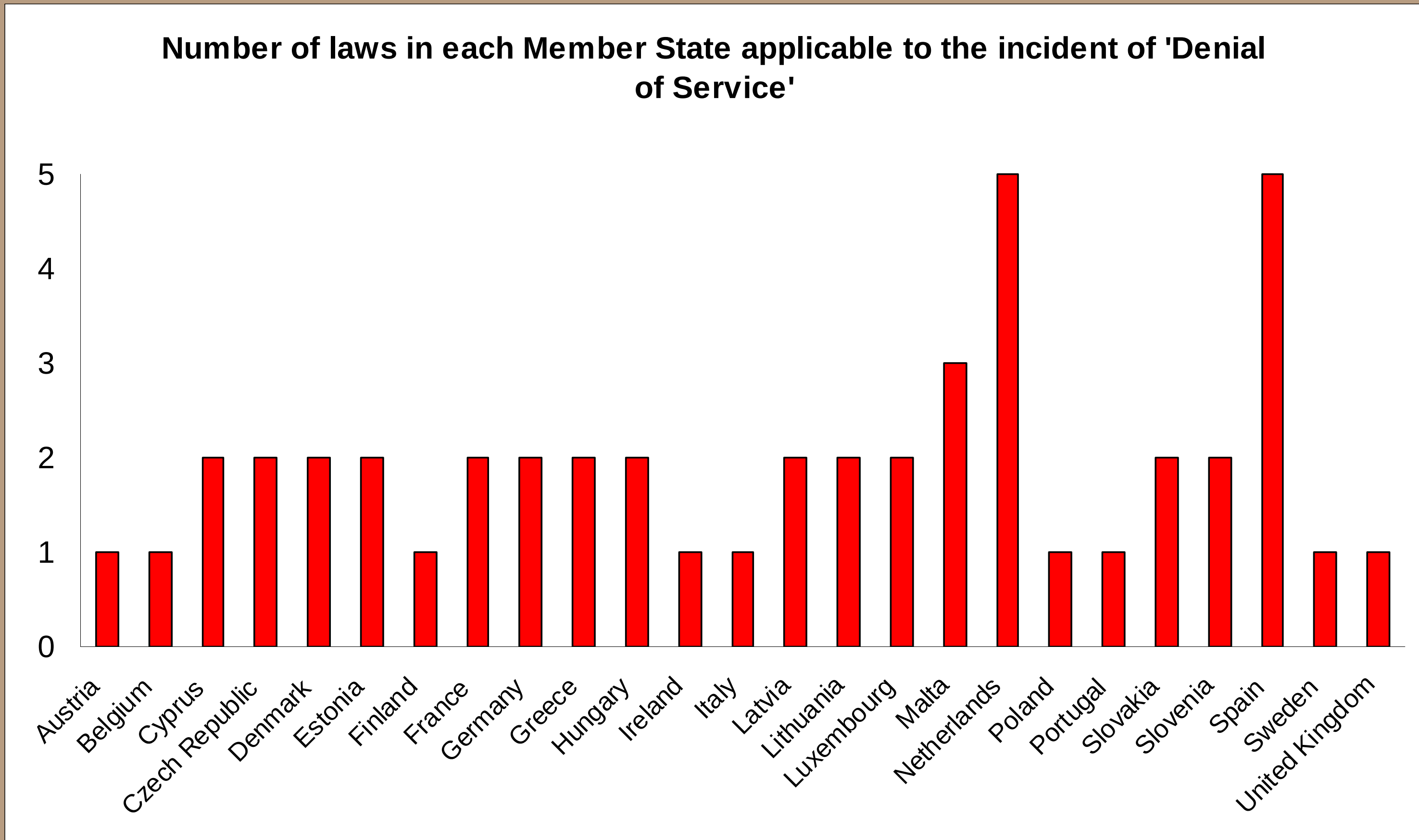
- Care!
  - This does not reflect the decisions of judges (e.g. case law in the UK or Ireland), or different legal systems
  - This does not cover state law in federated Member States (e.g. Germany)

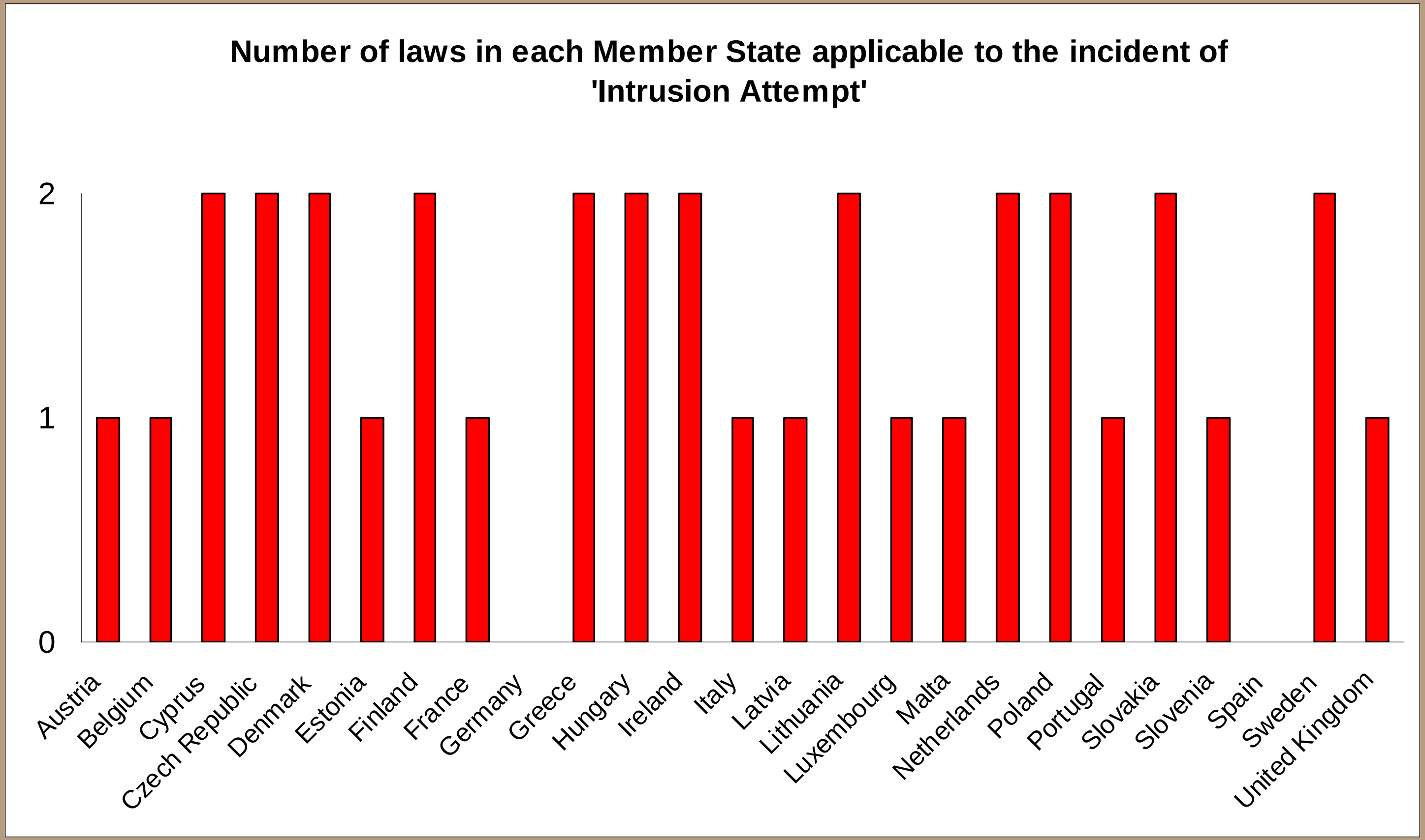
Part 1: Comparison of the breadth of cyber-crime law

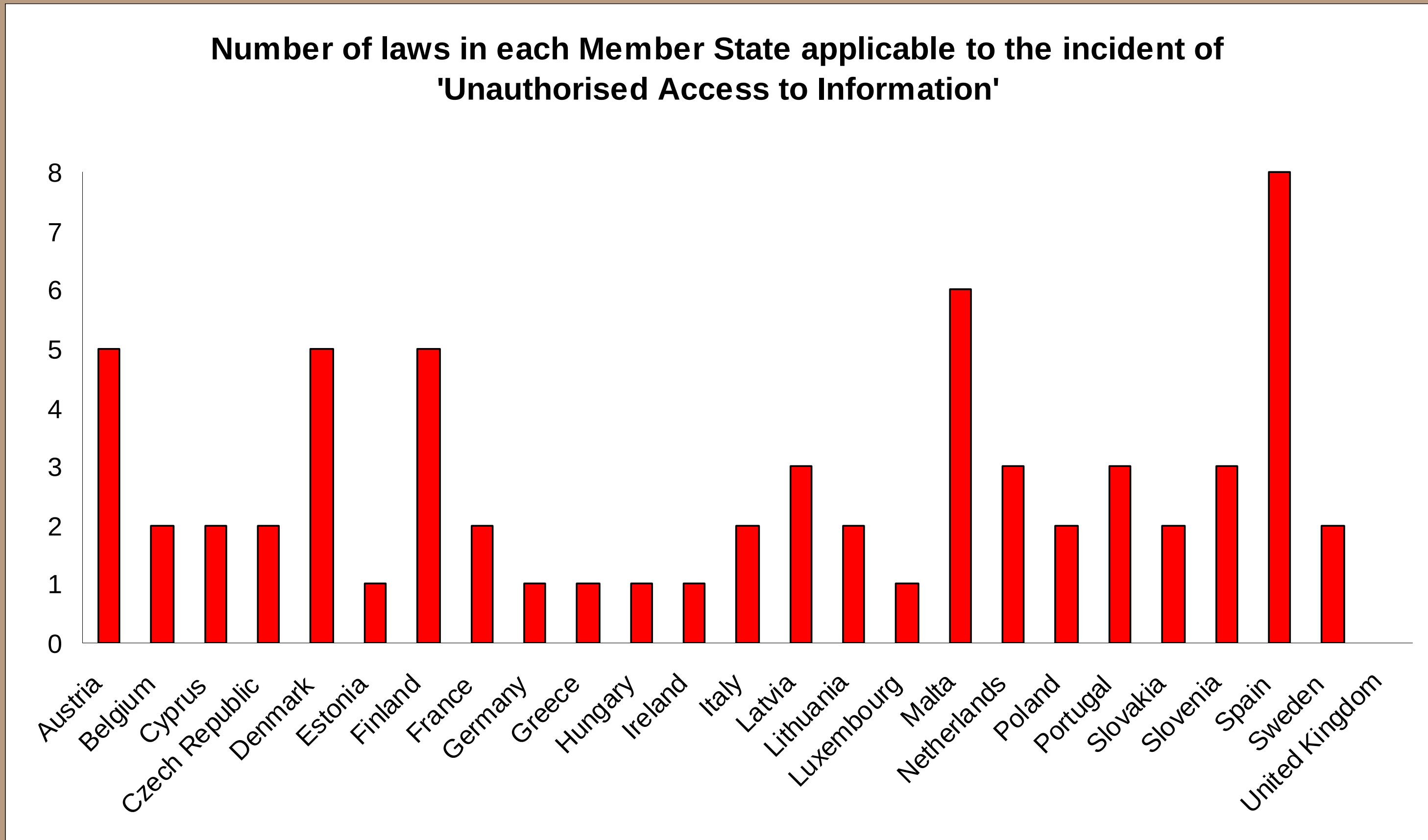
Law - overview

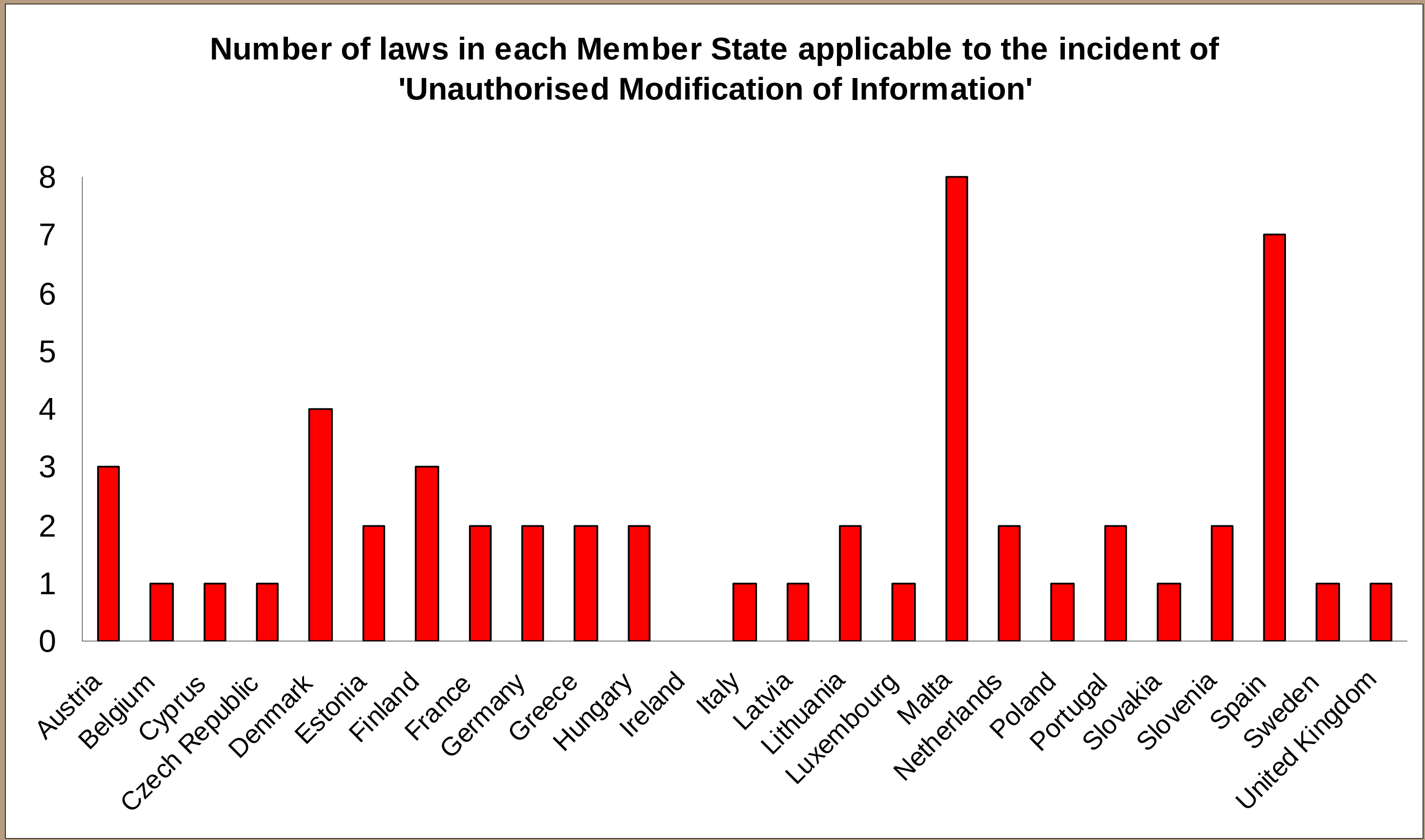
- Many countries have passed legislation which can be applied to a number of incidents (e.g. The Netherlands, Spain, Estonia)
- In the UK, legal precedent plays a very important role, as does use of other legislation (e.g. fraud) hence there is a smaller legal 'footprint'
- There is comparatively little law covering Account Compromise (possibly because this is thought to be dealt with internally to an organisation) & Target Fingerprinting
- Lawyers have the option of many different laws when it comes to Unauthorised Access to Communications Systems
- Incidents relating to Unauthorised Modification of Information are narrowly defined in law (there are generally only one or two laws) available per Member State

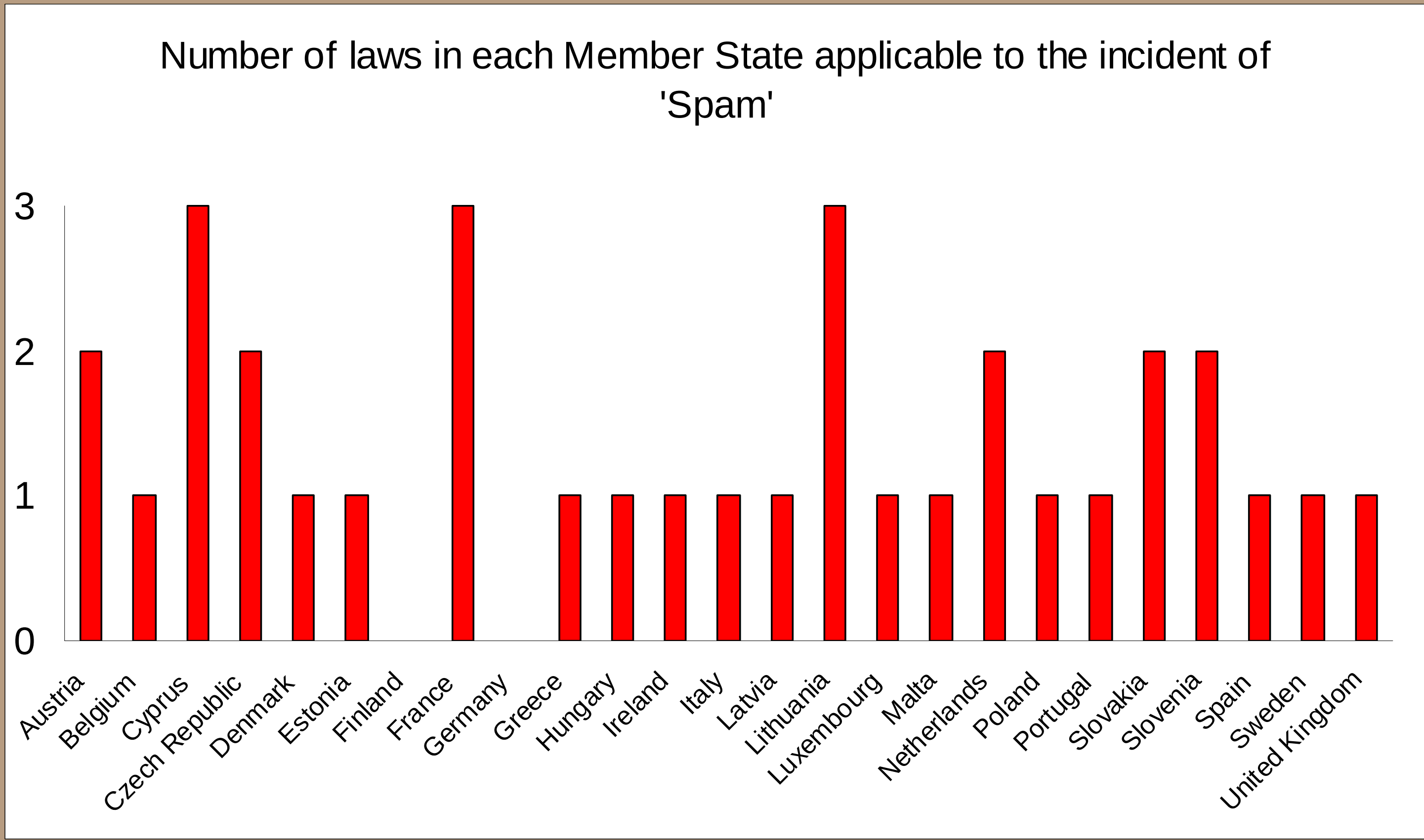
Some highlights of the analysis:


Number of laws in each Member State applicable to the incident of 'Denial of Service'
5
4
3
2
1
0
Austria
Belgium
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Latvia
Lithuania
Luxembourg
Malta
Netherlands
Poland
Portugal
Slovakia
Slovenia
Spain
Sweden
United Kingdom


Number of laws in each Member State applicable to the incident of 'Intrusion Attempt'
2
1
0
Austria
Belgium
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Latvia
Lithuania
Luxembourg
Malta
Netherlands
Poland
Portugal
Slovakia
Slovenia
Spain
Sweden
United Kingdom


Number of laws in each Member State applicable to the incident of 'Unauthorised Access to Information'
8
7
6
5
4
3
2
1
0
Austria
Belgium
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Latvia
Lithuania
Luxembourg
Malta
Netherlands
Poland
Portugal
Slovakia
Slovenia
Spain
Sweden
United Kingdom


Number of laws in each Member State applicable to the incident of 'Unauthorised Modification of Information'
0
1
2
3
4
5
6
7
8
Austria
Belgium
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Latvia
Lithuania
Luxembourg
Malta
Netherlands
Poland
Portugal
Slovakia
Slovenia
Spain
Sweden
United Kingdom



Number of laws in each Member State applicable to the incident of 'Spam'
3
2
1
0
Austria
Belgium
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Latvia
Lithuania
Luxembourg
Malta
Netherlands
Poland
Portugal
Slovakia
Slovenia
Spain
Sweden
United Kingdom

Part 2: Comparison of penal sanctions

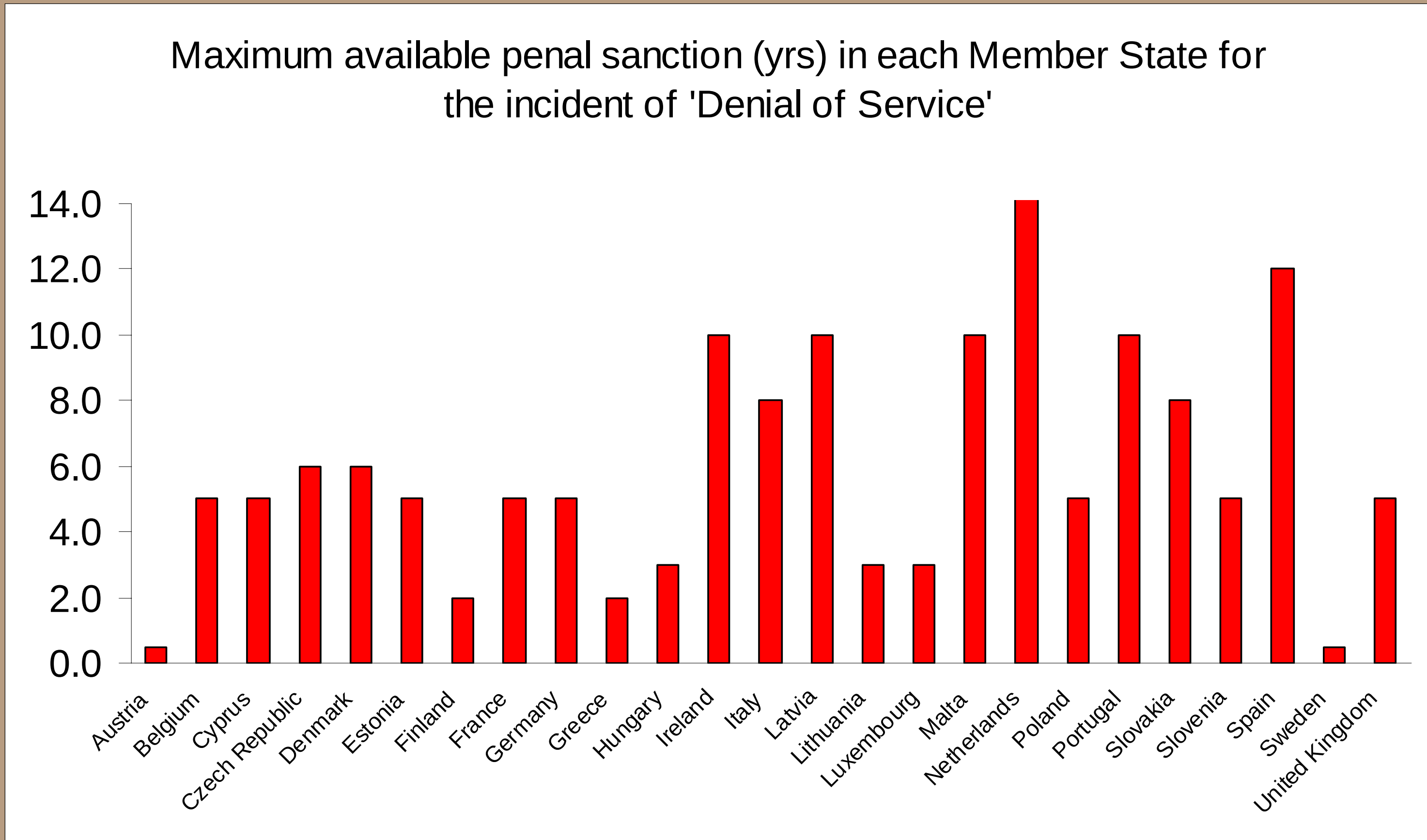
Penal sanctions - overview

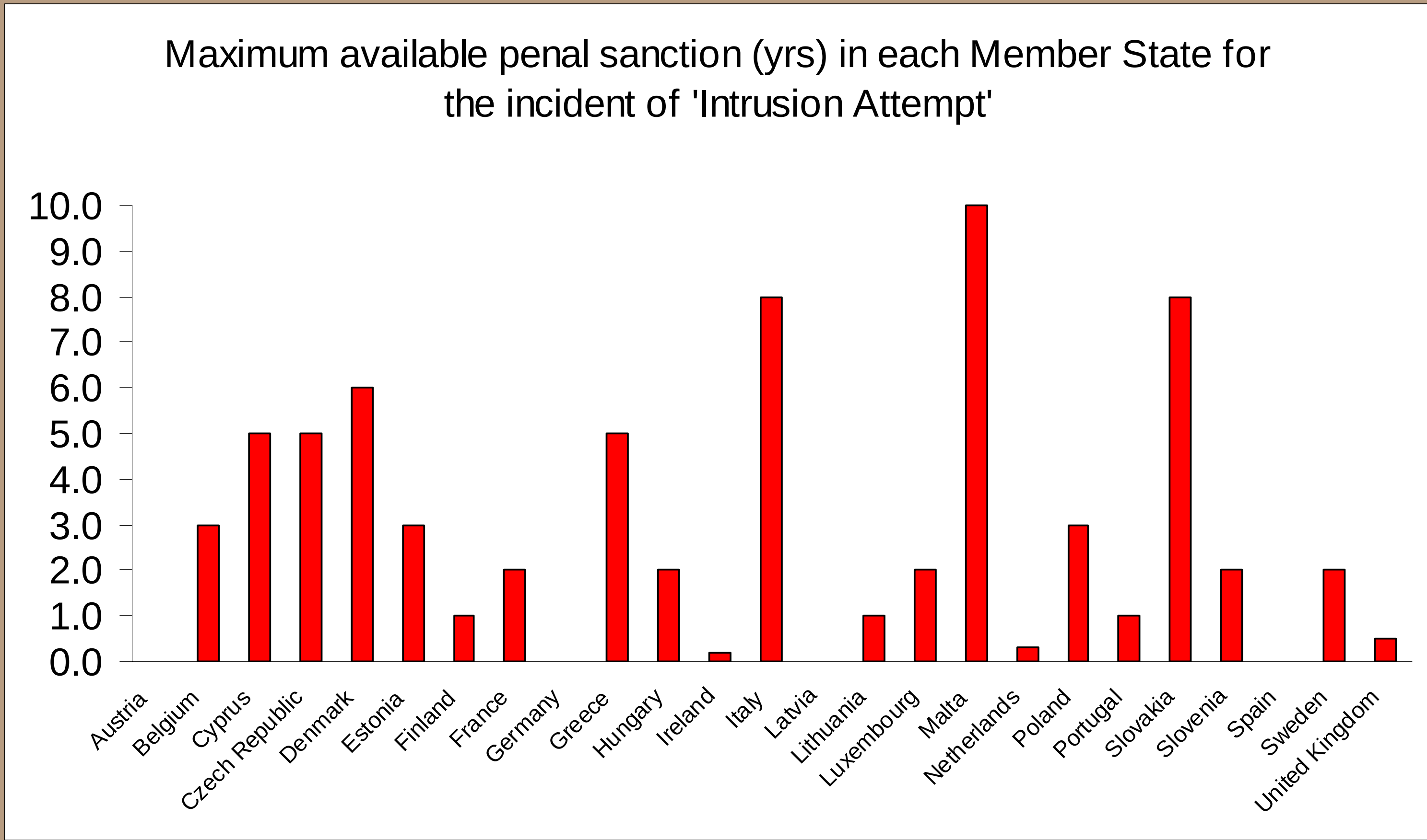
– The penalties can range from 30 days to 15 years
– Stiffer penalties are generally reserved for
  - Incidents conducted as part of a conspiracy (2 or more individuals)
  - Repeat offences (where someone has been successfully convicted of the same offence previously)
  - Incidents involving state secrets or sensitive computer systems or networks part of national security infrastructure
  - Incidents that may endanger life or serious damage to property
– Penal sanctions are combined with administrative sanctions (fines)

Penal sanctions - overview

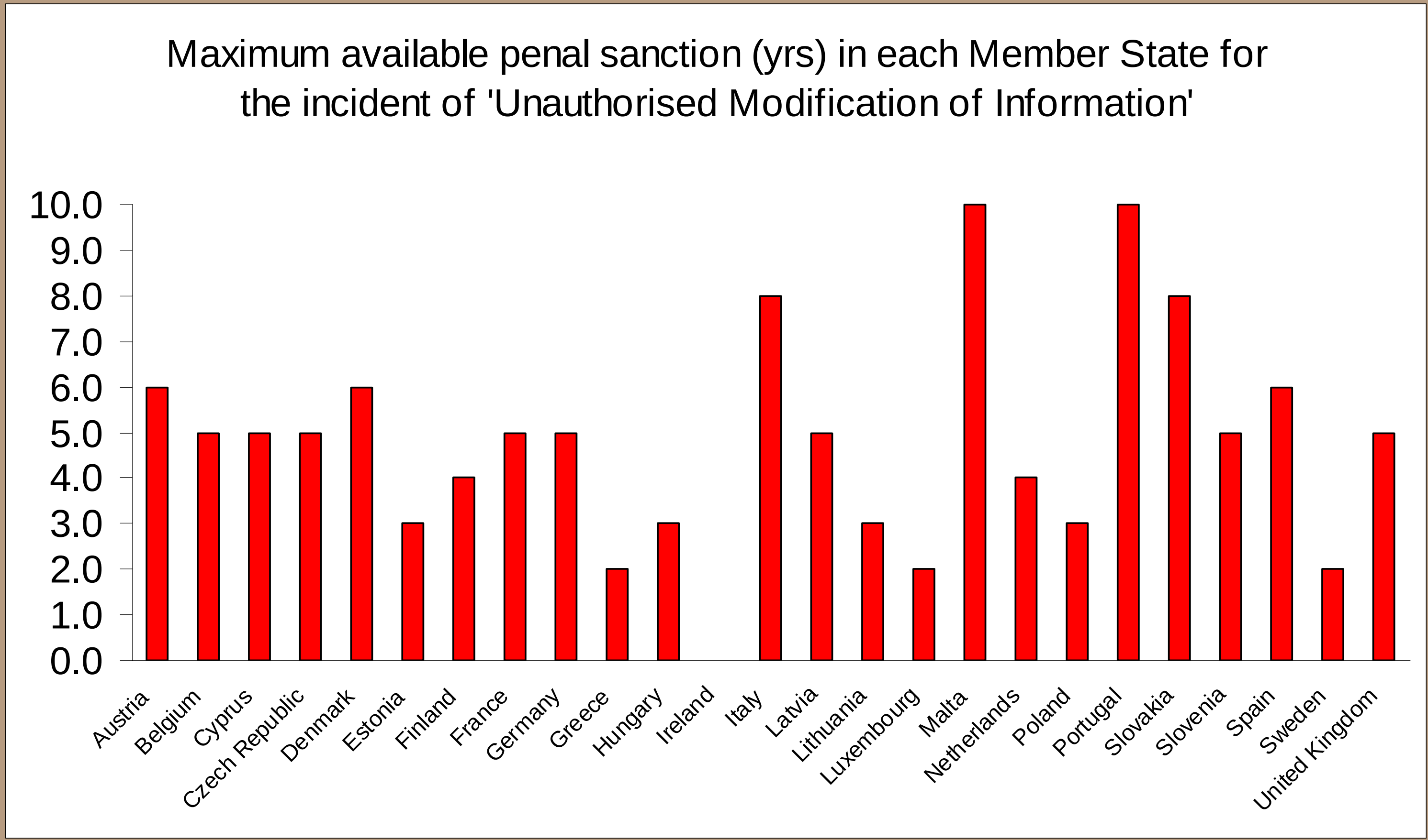
- Malicious Code, Denial of Service and Unauthorised Modification of Information are generally penalised with a prison term of at least a year
- Spam & target fingerprinting are not generally highly penalised (usually with administrative or financial sanctions)
- Some nations have recognised the effects that DoS have on the critical infrastructure by setting a large maximum prison sentence (e.g. NL)

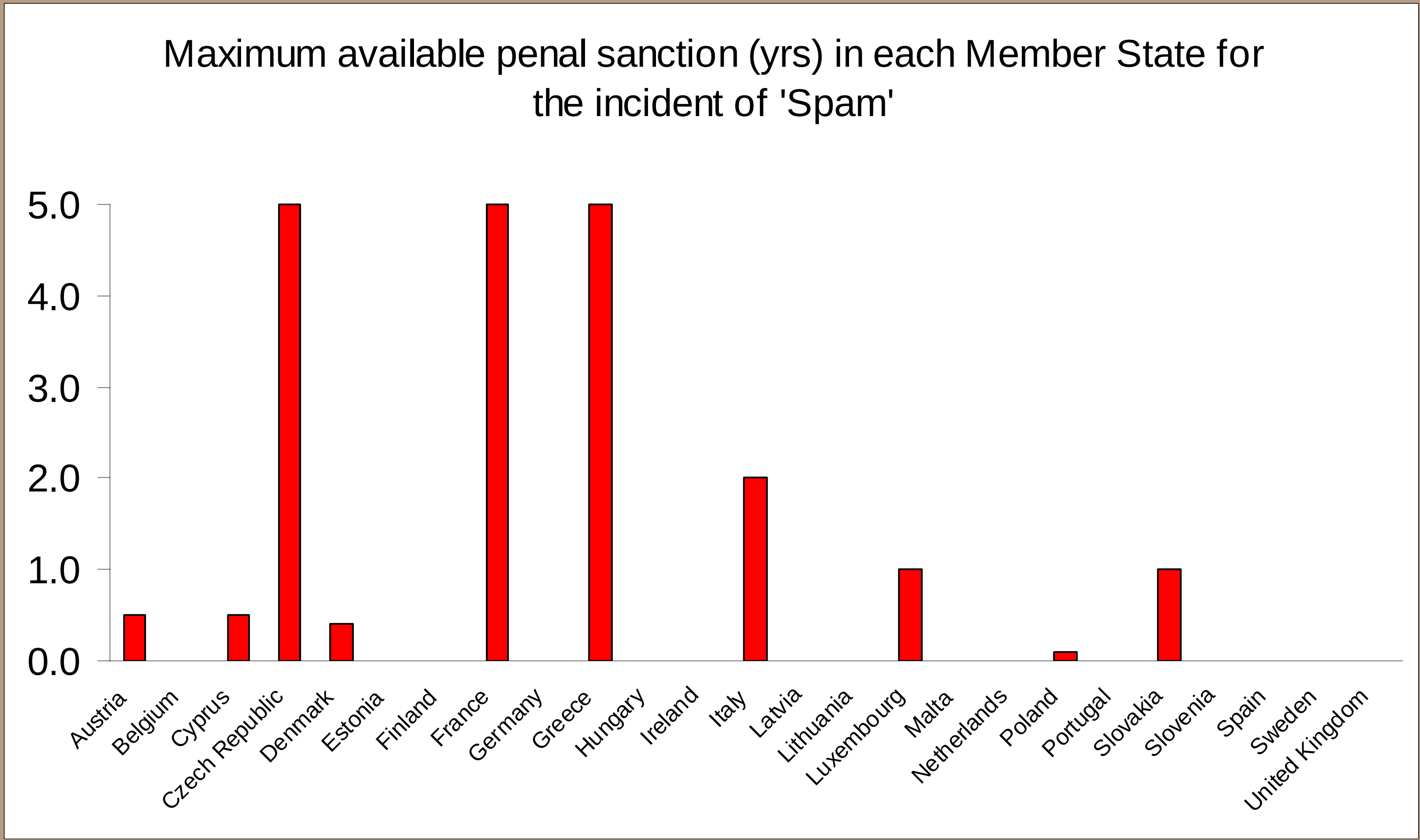
Some highlights of the analysis:


Maximum available penal sanction (yrs) in each Member State for the incident of 'Denial of Service'
14.0
12.0
10.0
8.0
6.0
4.0
2.0
0.0
Austria
Belgium
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Latvia
Lithuania
Luxembourg
Malta
Netherlands
Poland
Portugal
Slovakia
Slovenia
Spain
Sweden
United Kingdom



Maximum available penal sanction (yrs) in each Member State for the incident of 'Intrusion Attempt'
10.0
9.0
8.0
7.0
6.0
5.0
4.0
3.0
2.0
1.0
0.0
Austria
Belgium
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Latvia
Lithuania
Luxembourg
Malta
Netherlands
Poland
Portugal
Slovakia
Slovenia
Spain
Sweden
United Kingdom


Maximum available penal sanction (yrs) in each Member State for the incident of 'Unauthorised Modification of Information'
10.0
9.0
8.0
7.0
6.0
5.0
4.0
3.0
2.0
1.0
0.0
Austria
Belgium
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Latvia
Lithuania
Luxembourg
Malta
Netherlands
Poland
Portugal
Slovakia
Slovenia
Spain
Sweden
United Kingdom


Maximum available penal sanction (yrs) in each Member State for the incident of 'Spam'
5.0
4.0
3.0
2.0
1.0
0.0
Austria
Belgium
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Latvia
Lithuania
Luxembourg
Malta
Netherlands
Poland
Portugal
Slovakia
Slovenia
Spain
Sweden
United Kingdom

Conclusions

- The cyber-crime environment in Europe is rapidly evolving
- Some countries are ahead in passing ‘catch all’ laws (e.g. Malta, Denmark, Slovakia) which have a consistent level of sanction for many forms of incident
- Some are still behind (e.g. UK) in providing a ‘appropriate’ level of penal sanction to act as a deterrent

For more information contact
Neil Robinson
neilr@rand.org
or
Lorenzo Valeri
lvaleri@rand.org