The Directive on attacks against information systems

A Good Practice Collection for the implementation and application of this Directive

Jo De Muynck – Operational Security Unit

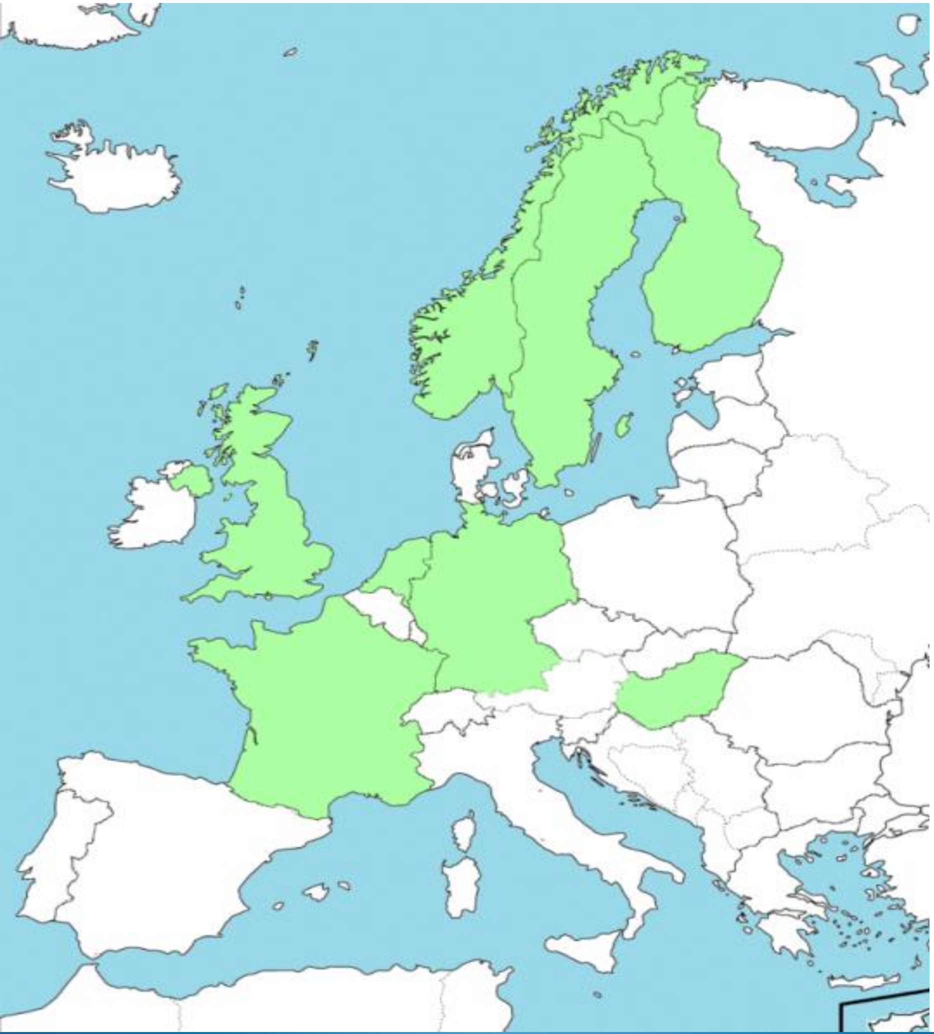
ENISA?

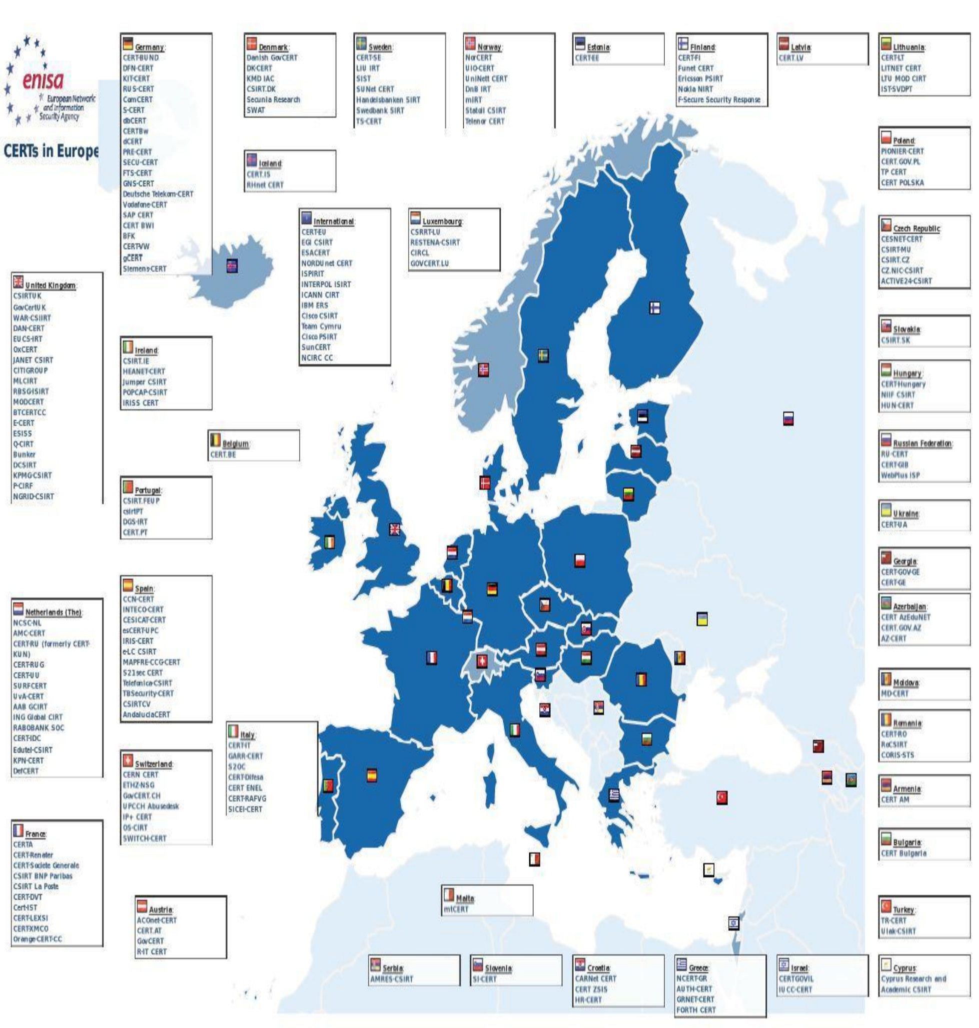
- The European Union Agency for Network and Information Security (ENISA) was formed in 2004.
- Centre of Expertise that supports the Commission and the EU Member States in the area of information security.
  - Computer Emergency Response Teams
  - CIIP & Resilience
  - Risk Management-Risk Assessment
  - Identity & Trust
- We facilitate the exchange of information between EU institutions, the public sector and the private sector.

ENISA and CERTs

- CERT: Computer Emergency Response Team
- ENISA supports the Member States and their CERTs by:
  - Providing help with the setting-up, training and exercising of the teams
  - Definition of “baseline capabilities” for new and established teams
  - Helping CERTs to enhance their capabilities by providing good practice guides

CERTs in Europe – 2005 to 2013





About the Directive

- Framework Decision Attacks against Information Systems
  - Adopted in 2005, “EU version of the 2001 Cybercrime Convention”
  - Scope: illegal access, illegal system/data interference, liability, jurisdiction and EU information exchange (24/7 contact points)
- Directive on Attacks against Information Systems
  - Proposed in 2010, abrogates Framework Decision
  - Adopted 22.7.2013, published 14.8.2013 as Directive 2013/40/EU
  - Must be transposed by 4 September 2015

What’s new?

- Largely the same as Framework Decision
- But some innovations as well:
  - Criminalisation of tools and illegal interception
  - Aggravating circumstances for crimes committed through organised crime, botnets, identity theft, causing serious damage, or against critical infrastructure
  - Response time of 8 hours for urgent requests
  - Statistical data collection obligations

Methodology

- Legal analysis of the Directive
  - What are the changes and expected impacts?
  - What are the likely challenges and possible good practices?
- Interviews with national stakeholders
  - Semi-structured phone interviews, based on a common script
  - Invitations to all categories of stakeholders in all Member States
  - Participants in 18 Member States
- Analysis of responses

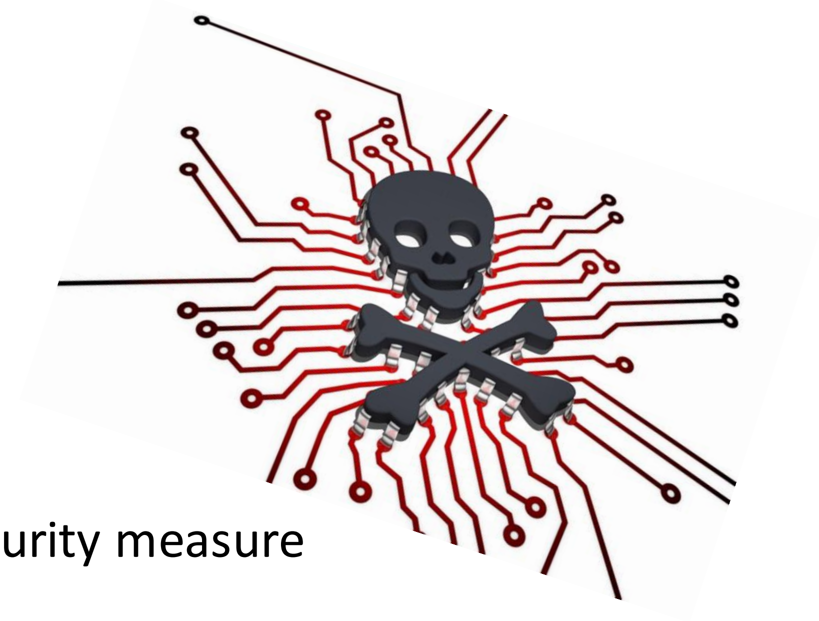
Impact on stakeholders

Stakeholder Change	Policy makers / Decision makers	National / Governmental CERTs	Other CERTs	Electronic communications service providers (e.g. ISPs)	Law enforcement / investigators	DPAs, NRAs and other supervisory authorities
New definitions of crimes	Limited impact	Identify new incidents and investigate them	Identify new incidents and investigate them	No impact	Investigate incidents and decide whether to prosecute	Limited impact
Expanded minimal maximum penalties	May have an interest in alignment of penalties to ensure consistency	No impact	No impact	No impact	May have an interest in alignment of the penalties they seek in prosecutions	No impact
Aggravating circumstances - botnets and ID theft	Support effective cross border investigations and prosecutions. Allow action to shut down botnets expediently	Interact effectively with law enforcement / investigators and take action	Interact effectively with law enforcement / investigators and take action	Interact effectively with law enforcement / investigators to signal incidents and take action	Set up effective cross border investigations and prosecutions and take action	DPAs may have data protection concerns with respect to investigations and information exchanges. NRAs may have operational concerns
Information exchange – 8 hour response period and minimal response requirements	Support effective cross border information exchanges, provide resources and communication mechanisms and designate responsible parties	Comply with assistance requests, which implies resources and guidance	Comply with assistance requests, which implies resources and guidance	Comply with requests (rapid response requires cooperation of service providers)	Make clear information requests and provide answers when needed.	DPAs may have data protection concerns with respect to investigations of suspects and information exchanges.
Monitoring and reporting of incidents	Implement procedures and resources for registration of incidents, prosecutions and convictions. Must implement reporting mechanisms.	No impact (unless they are tasked with monitoring/reporting under national law)	No impact (unless they are tasked with monitoring/reporting for their specific networks under national law)	No impact (unless they are tasked with monitoring/reporting for their specific networks under national law)	Provide information on prosecutions and convictions to national data collection points. May also be implicated in reporting.	DPAs may have data protection concerns with respect to the systematic registration of sensitive (judicial) personal data, including anonymisation.

Outcomes

- Examining substantive provisions, aggravating circumstances, cooperation/information exchange, and data collection/statistics
- Summary of interviews, identified good practices, and recommendations
- Largest difficulty: moving target
  - Interviews on the basis of the proposed Directive
  - GPC adapted to the final version

Findings – crimes

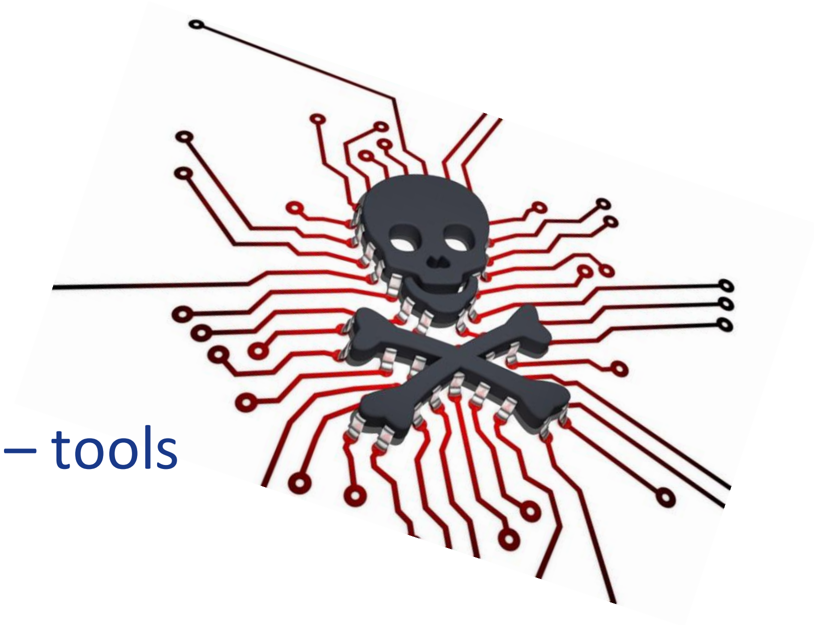


- Illegal access
  - Where committed by infringing a security measure
- Illegal interception
  - *"to ensure that the intentional interception by technical means, of non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data, is punishable as a criminal offence when committed without right."*

Findings – crimes

- Tools
  - *“ensure that the intentional production, sale, procurement for use, import, distribution or otherwise making available, of one of the following tools, without right and with the intention that it be used to commit any of the offences referred to in Articles 3 to 6, is punishable as a criminal offence, at least for cases which are not minor:”*
    - *a computer program, designed or adapted primarily for the purpose of committing any of the offences above;*
    - *a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed.*

Findings – crimes



- Illegal access – illegal interception – tools
- Major concerns?
  - Role of breaching security measures
  - Lawful use of tools by CERTs, academia, researchers
- Good practices:
  - Publication of prosecution guidelines or jurisprudence overviews
  - Implementing legislation should be clear and explicit, and include clear carve-outs for lawful actions (including at the lawful request of businesses, governments and end users).

Findings – ID theft and botnets

- Aggravating circumstances
- Major concerns?
  - Technological neutrality (mainly for botnets)
  - Freedom of expression, including parody (mainly for ID theft)
- Good practices:
  - Legislation should avoid technology specific terminology.
  - CERTs benefit from standardised processes / playbooks for responses to botnets or ID theft.
  - Partnerships with DPAs, and representatives of key sectors through ISACs (Information Sharing and Analysis Centers).

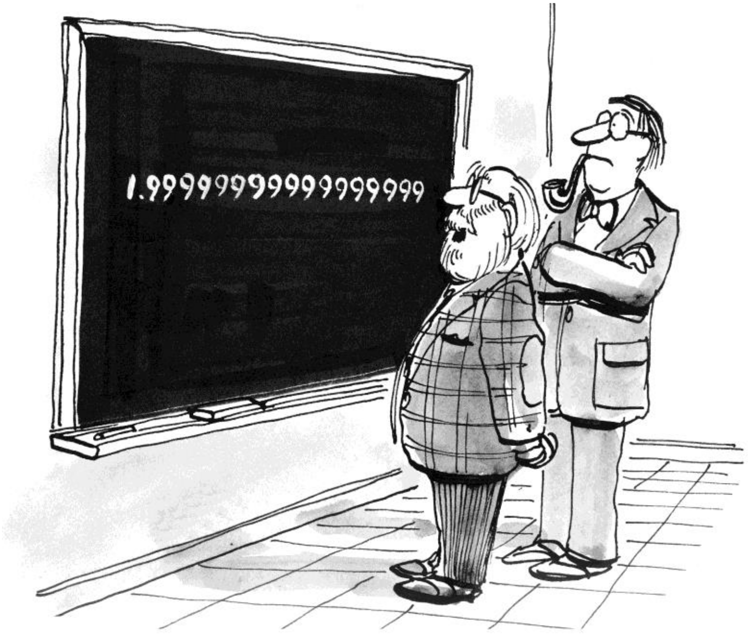
Findings – International collaboration and the role of CERTs

- Major concerns?
  - When should CERTs cooperate and with who?
  - What are their responsibilities and competences?
- Good practices:
  - Clear mandate: private CERTs benefit from agreements with their constituency; public CERTs benefit from a legal framework.
  - Integration of public CERTs and law enforcement is efficient but can harm their 'fire brigade' role (no informal consultation). In such cases, effort is required maintain a trust relationship.

Findings – 8 hour response period and minimal response

- Major concerns?
  - Doesn’t really impact CERTs too much
  - Skepticism: legal action requires more time
- Good practices:
  - Close link with DPAs can help CERTs, as noted above.
  - For efficiency reasons, every country needs a single contact point for information requests, irrespective of national competences or organisational model. This doesn’t always exist right now.

Findings – data collection and statistics



"I don't think only 2 can solve this."

- Major concerns?
  - Does the data exist, and where?
  - Is it comparable?
- Good practices:
  - Close link with DPAs can help CERTs, as above.
  - Statistical data is often scattered (CERTs, police/law enforcement, prosecutors, courts, etc), coordination and bundling is very rare. A coordinating body can be designated to collect and report.

Possible actions for the future - CERTs

Topic	Recommended future action
All substantive criminal provisions (illegal access, illegal interception, tools for committing offenses)	Collection and dissemination of **guidance on the interpretation and application of the law** at the EU level could help to ensure homogeneous application of the law across the European territory. Guidance should also explicitly cover conduct that is considered lawful, such as the activities of CERTs or security professionals.
Enforcement strategies	**Joint coordinated actions** between law enforcement, CERTs and the private sector (such as network operators) are recommended. **CERTs and the private sector should avoid taking actions without law enforcement support**, as this might solve a single attack but ultimately leaves the criminals unharmed.
Enforcement strategies	Simple cases (e.g. of identity theft) can often be solved by requesting service providers to take **voluntary action**, such as removal of the offending materials from any public website. This approach is often more efficient than formal legal proceedings. However, such requests must be **carefully considered in order to minimise the impact on potential future proceedings**. Deletion could result in the destruction of evidence, making future legal actions against criminals impossible or at least substantially harder. For this reason, **alignment is needed between CERTS and law enforcement** to agree upon appropriate action for specific instances, including e.g. determining when making data inaccessible is more appropriate than requesting deletion.
Communication between CERTs and law enforcement	It would be advisable to examine how **feedback could be provided from law enforcement to CERTs** on any matters reported by the CERT or in which the CERT intervened. To protect the secrecy of ongoing investigations, such information could only be provided at the aggregate (non-case specific) level.

Possible actions for the future - Policy

Topic	Recommended future action
Implementation strategy	Member States should **assess carefully whether new legislation is necessary** to achieve the effects of the Directive under existing law, and if so, to implement the required changes through **generic and technology neutral language**. This would achieve the desired outcome while avoiding the risk of putting in place language that creates new technical discussions or escape routes for criminal behaviour.
Liability and responsibility for ICT incidents	Future policy initiatives should **consider the responsibility and liability of service providers**, e.g. operators of websites which run outdated software with known security vulnerabilities. Some degree of responsibility/liability for damages resulting from the hacking of such systems should lie with the operators, in order to provide economic incentives for proper security practices.
Data protection compliance	With respect to data sharing, **pragmatic guidance at the EU level, e.g. from the Article 29 Working Party, on the interpretation and impact of data protection rules for CERTs and network operators in their day-to-day security related activities** is still needed. While the theoretical framework and the potential consequences are well known, CERTs and service providers are still largely experimenting on what type of monitoring, analysis and reporting activities (to customers, CERTs or LEA) are lawful, and which activities are excessive. This has a stifling effect on the fight against cybercrime.
Identity theft	National laws should clarify the **importance of the criminal intent of the alleged ID thief**, and to stress that the provisions should be interpreted and applied taking into account the legitimate exercise of the fundamental right to freedom of expression. The primacy of this fundamental right should be recognized. The **interpretation of the balance between criminal conduct and controversial but legal free speech should be left to the court**s; CERTs should at any rate not play a role in assessing the balance.

Possible actions for the future - Policy

Topic	Recommended future action
Assistance requests	Even within the EU, replies to information requests were often delayed or partial. Misunderstandings with respect to the scope of requests were commonly a part of the cause. **Streamlining/standardisation of communications between the 24/7 network might be useful**, which could be done by **establishing templates** for the most common information requests. For assistance requests sent via Europol/Interpol, the possibility exists to append codes to the information requests that indicate which information may be disseminated to other contact points. This is a minor but useful example of a standardisation mechanism that can be very effective.
International cooperation	**International cooperation with partners outside of the EU** (e.g. with non-EU Southeast European countries, Asian and African countries) is still at an immature level. This should also be supported through face-to-face meetings between law enforcement representatives, as a key first step to building trust and identifying effective contacts. This is important to address current policy gaps: **bullet proof hosting services are a challenge that is currently unaffected by EU initiatives**, as these services are almost universally established outside the EU.
Data collection and statistical analysis	In the longer term, **better alignment is needed with respect to semantics and prosecutorial policies across the EU, if the goal is to obtain comparable statistics** across the EU. Crimes have different meanings in different countries, and identical incidents can be qualified differently from country to country, making statistics incomparable.

8th ENISA Workshop - Part II – ENISA/EC3 Workshop

- 02-03 October 2013
- Co-organised with Europol (EC3)
- Hosted in the Europol Premises in The Hague, Netherlands
- Topic: cooperation between CERTs and Law Enforcement
  - Keynotes/presentations
  - ENISA training sessions
  - Round table discussion – TLP Red

8th ENISA Workshop
Part II – ENISA/EC3 Workshop

QUESTIONS???

For more information on ENISA’s CERT/CSIRT support activities, visit http://www.enisa.europa.eu/activities/cert

Follow ENISA: