Octopus Conference , 21 – 23 November 2011
WS 3 Cybercrime strategies

Cybercrime strategies

Alexander Seger
Council of Europe
alexander.seger@coe.int

www.coe.int/cybercrime

1

Octopus Conference , 21 – 23 November 2011, WS 3 Cybercrime strategies

Cybersecurity

Typically defined as:

the protection of the confidentiality, integrity and availability of computer data and systems in order to enhance security, resilience, reliability and trust in ICT

Motivated by:

- Reliance on ICT -> national interest
- Economic potential of ICT
- CIIP -> National security

Protection against:

- Non-intentional incidents
- Intentional attacks by state and non-state actors against ICT (c-i-a attacks)

Measures:

- Protection, mitigation, recovery through technical, procedural, institutional measures (vulnerability analyses, early warning/response, CERT/CSIRTs, etc)
- Cybercrime legislation, investigation, international cooperation

www.coe.int/cybercrime

2

Octopus Conference , 21 – 23 November 2011, WS 3 Cybercrime strategies

Cybercrime

Defined as:

- Offences against computer data and systems (c-i-a offences) (Articles 2-6 Budapest Convention)
- Offences by means of computers (such as Articles 7-10 Budapest Convention)

Motivated by:

- Crime prevention and criminal justice

Protection against:

- Intentional attacks against and by means of computers
- Any crime involving electronic evidence on a computer system

Measures:

- Investigation, prosecution, adjudication
- Conditions and safeguards
- Prevention
- Technical and other measures

www.coe.int/cybercrime

3

Octopus Conference , 21 – 23 November 2011, WS 3 Cybercrime strategies

Cybercrime and/vs cybersecurity?

4

Octopus Conference , 21 – 23 November 2011, WS 3 Cybercrime strategies

Objective of cybercrime strategies:

Overall objective:

- to ensure that the rule of law applies and that legitimate rights are protected also in the ICT/online environment

Specific objective:

- effective criminal justice response to offences against and by means of computers as well as to any offence involving electronic evidence

Elements of cybercrime strategies:

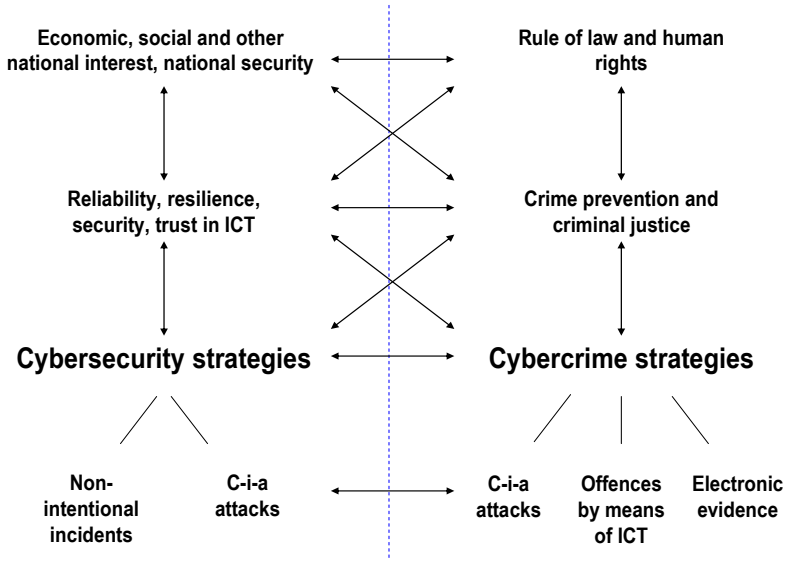
- Cybercrime reporting
- Prevention
- Legislation, incl. safeguards and data protection
- Specialised units
- Interagency cooperation
- Law enforcement training
- Judicial training
- Public/private cooperation
- Effective international cooperation
- Financial investigations and fraud/ML/TF prevention
- Protection of children

www.coe.int/cybercrime

5

Octopus Conference , 21 – 23 November 2011, WS 3 Cybercrime strategies

Cybersecurity and cybercrime strategies: differences and complementarity



6

Octopus Conference , 21 – 23 November 2011, WS 3 Cybercrime strategies

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Conclusion:

Cybercrime and cybersecurity related/complementary but different concepts

Options

Specific cybercrime strategies in addition to cybersecurity strategies

Or

Enhance cybercrime components within cybersecurity strategies

Consider:

- Ensure that criminal justice/rule of law principles – including safeguards – are taken into account, also in cybersecurity strategies
- Cost and impact of cybercrime justify investment in cybercrime strategies
- Cybercrime strategies may help mobilise technical assistance
- Multi-stakeholder approaches to be pursued
- Attacks as cybercrime: de-escalate situations
- Clarification of concepts may favour international agreements

www.coe.int/cybercrime

7

Octopus Conference , 21 – 23 November 2011, WS 3 Cybercrime strategies

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

1. Cybercrime and cybersecurity strategies

- What concepts?
- Is there a need to reconsider cybersecurity concepts?
- What differences and intersection?
- How to ensure synergies and complementarity?

2. Cybercrime strategies

- Justification: Is there a need for specific cybercrime policies or strategies?
- Or enhance cybercrime components in cybersecurity strategies?
- One or more strategies?
- By public and private sectors?
- What objectives and measures would make up such strategies?

3. Stakeholders

- Who is responsible for cybercrime strategies?
- What role for public and private sector organisations?
- What are reasons for the success or failure of public/private cooperation?

8