Project Cybercrime@Octopus

Regional Cybercrime / Cybersecurity Assessment Conference
11-12 November 2015
Manila, Philippines

Session 1

Cybercrime versus Cybersecurity

www.coe.int/cybercrime

1

Session 1: Cybercrime v. cybersecurity

Session objective: To clearly define cybersecurity and cybercrime

- **Distinction between cybersecurity and cybercrime**
- **Relation between the two concepts**
- **Pros and cons of uniting, separating, and/or linking the two concepts**

2

Session 1: Cybercrime vs. Cybersecurity

Examples of cybersecurity strategies:

- Australia: Cyber Security Strategy (2009)
- Bangladesh: National Cybersecurity Strategy (2014)
- India: National Cyber Security Policy – 2013
- Maroc: Stratégie Nationale pour la Société de l'Information et de l'Économie Numérique
- Mauritius: National Cyber Security Strategy 2014 – 2019
- South Africa: (draft 2011) National Cybersecurity Policy Framework
- United Kingdom: UK Cyber Security Strategy (2011)

Examples of cybercrime strategies:

- Australia: National Plan to combat cybercrime (2013)
- ?

3

Session 1: Cybercrime vs. Cybersecurity

Cybercrime and cybersecurity: what is the difference?

4

Session 1: Cybercrime vs. Cybersecurity

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

5

Session 1: Cybercrime vs. Cybersecurity

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)

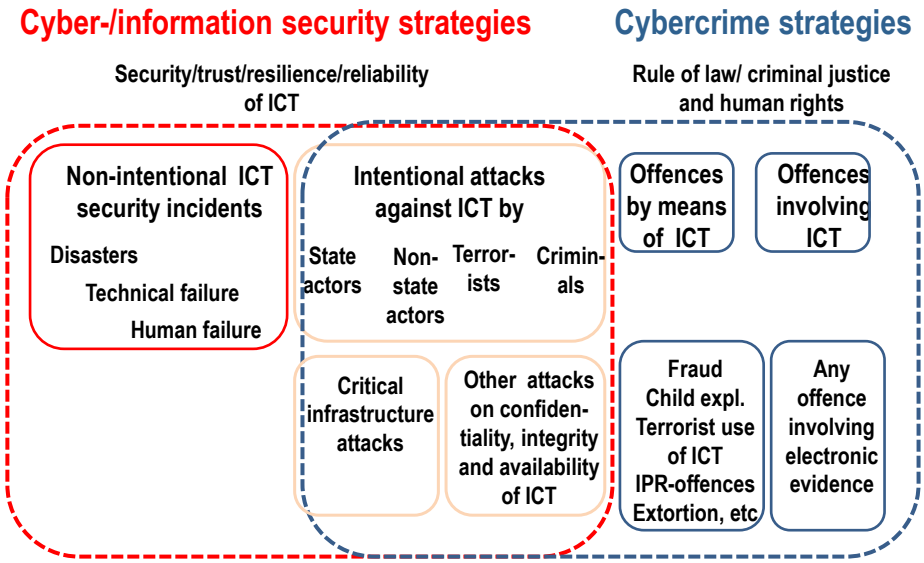
Motivated by:
- Crime prevention and criminal justice

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

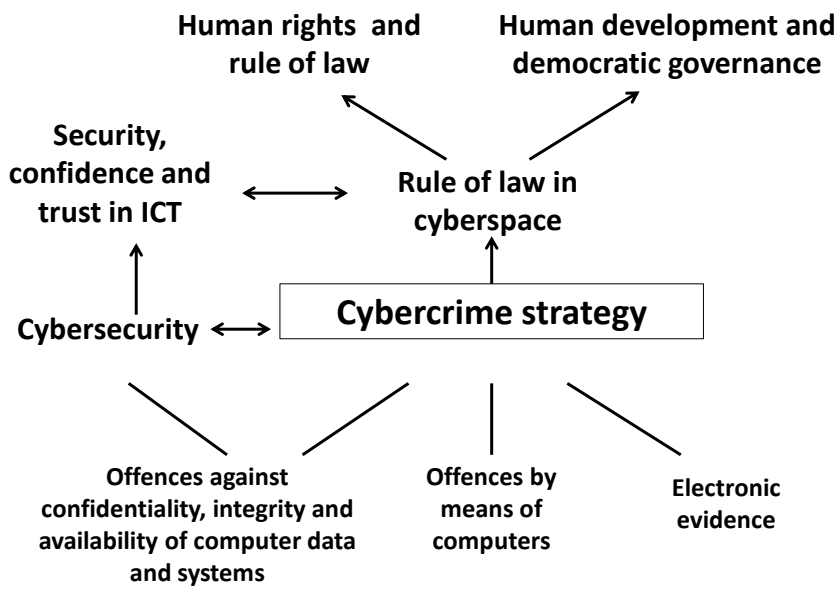
6

Session 1: Cybercrime vs. Cybersecurity



7

Session 1: Cybercrime vs. Cybersecurity



8

Session 1: Cybercrime vs. Cybersecurity

For discussion:

- **Should cybercrime be part of a cybersecurity strategy ?**
- **Or is there a need for a separate cybercrime strategy?**
- **What role for criminal justice in cybersecurity strategies?**
- **Risk: criminal justice sidelined? Powers and resources shifting to national security bodies:**

Pros and cons of uniting, separating, and/or linking the two concepts

- **Approaches, views and experience in participating countries**

9

Project Cybercrime@Octopus

Regional Cybercrime / Cybersecurity Assessment Conference
11-12 November 2015
Manila, Philippines

Session 2

Cybercrime and cybersecurity strategy – Frameworks, challenges, and developments

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

www.coe.int/cybercrime

DEPARTMENT OF JUSTICE
Office of Cybercrime

10

Session 2: Cybercrime / cybersecurity strategies

Session objective: To assess and enhance existing frameworks and strategic approaches on cybercrime and cybersecurity

- **Cybercrime and cybersecurity framework and strategies in participating countries**
- **Existing Framework of Cybercrime/Cybersecurity (Statistics and Reporting mechanisms, Responses, Actions, and Initiatives)**
- **Emerging Challenges and Threats in Cybercrime and Cybersecurity (Issues and Problems)**
- **Developments/Cybercrime Strategies**
- **Developments/Cybersecurity Strategies**

11

Session 2: Cybercrime / cybersecurity strategies

Tour de table will follow:

Cybercrime or cybersecurity strategies in participating countries

If you don't have a strategy yet:

- **What needs/problems should a cybercrime strategy address?**
- **What would be the core objective of a cybercrime strategy?**

12

Session 2: Cybercrime / cybersecurity strategies

Typical objective of a cybercrime strategy (or component of a cybersecurity strategy)

Protection against:

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

13

Session 2: Cybercrime / cybersecurity strategies

Example: Australia: National Plan to combat cybercrime (2013)

Key priorities

- **educating the community to protect themselves**
- **partnering with industry to tackle the shared problem of cybercrime**
- **fostering an intelligence-led approach and information sharing**
- **improving the capacity and capability of government agencies, particularly law enforcement, to address cybercrime**
- **improving international engagement on cybercrime and contributing to global efforts to combat cybercrime and**
- **ensuring an effective criminal justice framework**

14

14

Session 2: Cybercrime / cybersecurity strategies

Example: Belgique – Cybersecurity Strategy 2012

Menaces

- Notre société et économie dépendent de l'ICT
- Notre pays est vulnérable (criminalité, données personelles, cloud servers
- Cybermenace est réelle (criminalité, botnets, hacktivisme, cyberespionnage, cyberwarfare)

Objectifs stratégiques

La Belgique:

1. visera un cyberespace sûr et fiable qui respecte les valeurs et droits fondamentaux de la société moderne
2. visera une protéction et une sécurisation optimales des infrastructures et systèmes publics critiques contra les cybermenaces
3. Désire développer ses propres capacités en cybersecurité

15

Session 2: Cybercrime / cybersecurity strategies

Example: Mauritius – National Cyber Security Strategy 2014 - 2019

Vision:
Enhance the cyber threat preparedness of Mauritius and managing disturbances caused by these threats.

Mission:
To integrate Information Security firmly into the basic structures of the information society

Goals:

1. To secure our cyberspace and establish a front line of defense against cybercrime
2. To enhance our resilience to cyber attacks and be able to defend against the full spectrum of threats
3. To develop an efficient collaborative model between the authorities and the business community for the purpose of advancing national cyber security and cyber defense
4. To improve the cyber expertise and the comprehensive cyber security awareness of the society at all levels

16

Session 2: Cybercrime / cybersecurity strategies

Example: Estonia Cyber Security Strategy 2014 - 2017

Dependence on ICT and e-services ▶ Needs to be addressed:

- **Ensuring vital services**
- **Combating cybercrime**
- **Advancing national defence capabilities**

Vision:
Estonia is able to ensure national security and support the functioning of an open, inclusive and safe society.

General objective:
The four-year goal of the cybersecurity strategy is to increase cybersecurity capabilities and raise the population's awareness of cyber threats, thereby ensuring continued confidence in cyberspace.

17

Session 2: Cybercrime / cybersecurity strategies

Tour de table:

- **Cybercrime or cybersecurity strategies in participating countries, including data/statistics**

If you don't have a strategy yet:

- **What needs/problems should a cybercrime strategy address?**
- **Statistics/data on cybercrime and cybersecurity?**
- **What would be the core objective of a cybercrime strategy?**

18

Session 2: Cybercrime / cybersecurity strategies

Stakeholders

- Who should be involved in a cybercrime strategy or component of a cybersecurity strategy?
- Who should take the lead? Who should coordinate? One institution or committee structure?

19

Session 2: Cybercrime / cybersecurity strategies

Example: Mauritius – National Cyber Security Strategy 2014 - 2019

- Ministry of ICT ("owner" of the strategy)
- National Cyber Security Committee as decision-making body (MICT, CERT-MU, Law enforcement, Regulatory Bodies, Critical Sectors, PMO, Data Protection Office, Vendors & Private Sectors, Adademia)
- CERT-MU
- Law enforcement (police)
- Regulatory bodies (ICTA, IBA, Bank of Mauritius)
- Critical sectors (financial services, tourism, ICT and broadcasting, health, sugar, customs and others
- Prime Minister's Office
- IT Security Unit
- Data Protection Office
- Academia
- Vendors and private sector

20

Session 2: Cybercrime / cybersecurity strategies

Example: Estonia Cyber Security Strategy 2014 - 2017

Ministry of Economic Affairs and Communications directs cyber security policy and coordinates the implementation of the strategy.

The strategy will be implemented by involving all ministries and government agencies, especially the Ministry of Defence, the Information System Authority, the Ministry of Justice, Police and Border Guard Board, the Government Office, the Ministry of Foreign Affairs, the Ministry of the Interior and the Ministry of Education and Research.

NGOs, business organizations, governments, and educational institutions will cooperate in the implementation and assessment of the strategy.

At the request of the Ministry of Economic Affairs and Communications, agencies involved in executing the strategy will submit a written overview of the implementation of the measures and activities each year by 31 January, at the latest.

21

Session 2: Cybercrime / cybersecurity strategies

Discussion/exchange of views with participants:

- **Who should be involved in a cybercrime strategy or component of a cybersecurity strategy?**
- **Who should take the lead? Who should coordinate? One institution or committee structure?**

22

Session 2: Cybercrime / cybersecurity strategies

Elements / priorities of strategies:

- What should be the elements or actions or sub-components of a cybercrime strategy or component of a cybersecurity strategy?
- What should be the priorities for your country regarding cybercrime and cybersecurity?

23

Session 2: Cybercrime / cybersecurity strategies

Example: Estonia Cyber Security Strategy 2014 - 2017

Subgoal 1: Ensuring the protection of information systems underlying important services

Subgoal 2: Enhancing of the fight against cybercrime
- 2.1. Enhancing detection of cybercrime
- 2.2. Raising public awareness of cyber risks
- 2.3. Promoting international cooperation against cybercrime

Subgoal 3: Development of national cyber defence capabilities

24

Session 2: Cybercrime / cybersecurity strategies

Example: Belgique – Cybersecurity Strategy 2012

Approche et domaines d'action

1. **Approche centralisée et intégrée de la cybersécurité**
2. **Création d'un cadre légal (équilibre entre les droits et libertés et interventions nécessairs pour garantir la sécurité)**
3. **Suivi permanent de la cybermenace**
4. **Amélioration de la protection des systèmes informatiques**
5. **Renforcement de la capacité à réagir aux cyberincidents**
6. **Approache spécifique de la cybercriminalité (signalement par la victime, enquête par la police et justice, actions côntre les organisations criminels)**
7. **Contribution à l'élargissement de l'expertise et la connaissance en cybersécurité**
8. **Stimulation du développement technologique**

25

Session 2: Cybercrime / cybersecurity strategies

Example: Mauritius – National Cyber Security Strategy 2014 - 2019

Goals:

1. **To secure our cyberspace and establish a front line of defense against cybercrime**
   Including:
   - **Enhance Law enforcement capability on cybersecurity, in particular training on cybercrime and electronic evidence**
   - **International and regional cooperation on cybercrime**
   - **Legal framework assessment**
2. **To enhance our resilience to cyber attacks and be able to defend against the full spectrum of threats**
3. **To develop an efficient collaborative model between the authorities and the business community for the purpose of advancing national cyber security and cyber defense**
4. **To improve the cyber expertise and the comprehensive cyber security awareness of the society at all levels**

26

Session 2: Cybercrime / cybersecurity strategies

Objective

Protection against:

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

Strategic priorities adopted at EAP conference (Kyiv, October 2014)

ELEMENTS:

- 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

27

Session 2: Cybercrime / cybersecurity strategies

Discussion / exchange of views with participants:

- What are or should be the priorities of a cybercrime or cybersecurity strategy in your country?
- What should be priorities in terms of regional/international cooperation?
- Public/private cooperation?

28

Session 2: Cybercrime / cybersecurity strategies

Tour de table:

Conclusions: what will be the next steps regarding cybercrime or cybersecurity strategies in your country?