CyberSouth
Cooperation on Cybercrime in the Southern Neighbourhood Region

CyberSouth Launching Conference, Tunis, 21-23 March 2018

Session on cybercrime policies and strategies

Strategies on cybercrime: considerations
Stratégies contre la cybercriminalité: considérations

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

Funded by the European Union and the Council of Europe
EUROPEAN UNION
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Implemented by the Council of Europe

www.coe.int/cybercrime

1

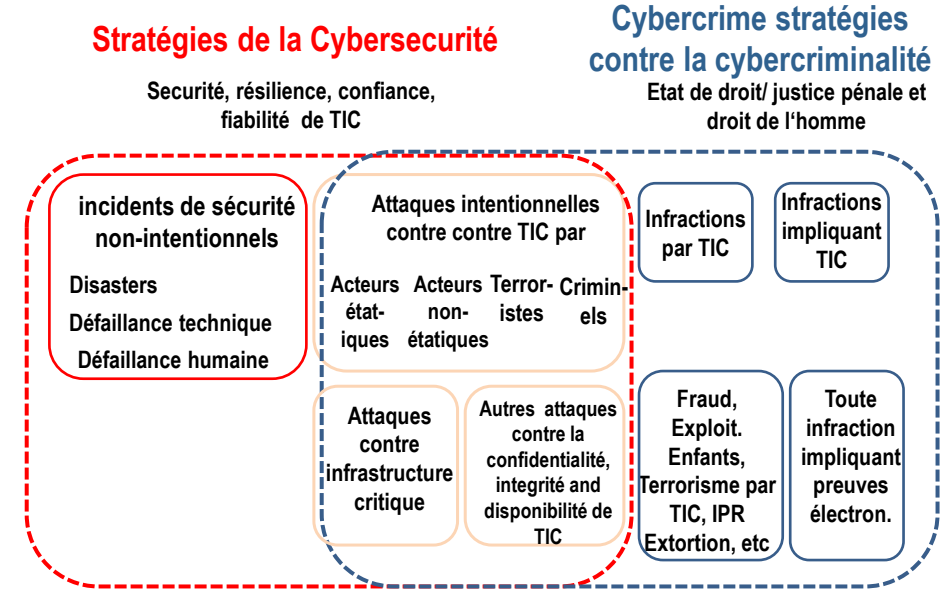
Cybercrime vs. Cybersecurity

Cybercrime and cybersecurity: what is the difference?

Cybercriminalité et cybersécurité: quelle est la différence?

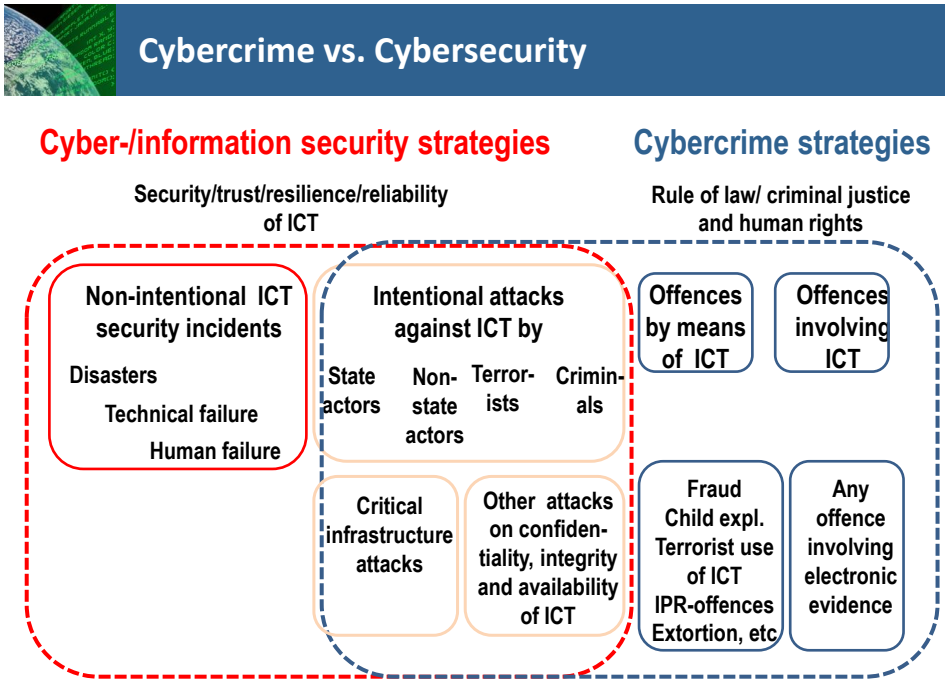
2

Cybercriminalité v. cybersecurité



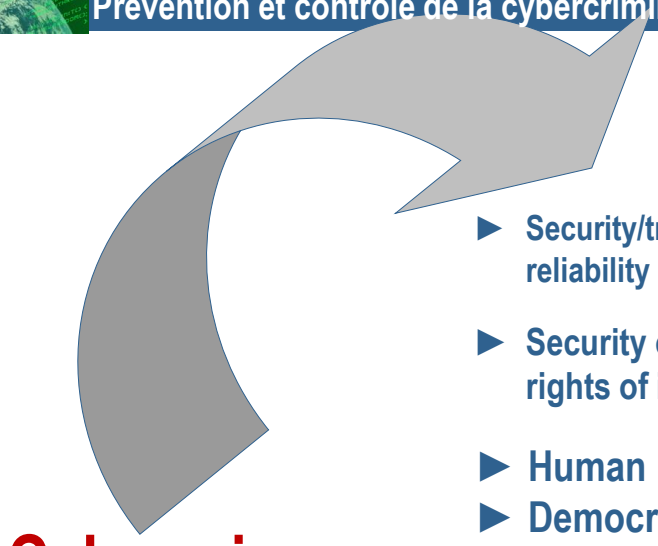
3

Cybercrime vs. Cybersecurity



4

Prevention and control of cybercrime: why?
Prévention et contrôle de la cybercriminalité: pourquoi?



Cybercrime

- Security/trust/resilience/ reliability of ICT
- Security of society and rights of individuals
- Human rights
- Democracy
- Rule of law

5

5

Prevention and control of cybercrime: what?

Cybercrime

- Offences against computer systems and data
- Offences by means of computer systems and data

+

Electronic evidence

- Any crime may involve evidence in electronic form on a computer system
- Needed in criminal proceedings
- No data, no evidence, no justice

Cybercriminalité

- *Infractions contre systèmes et données informatiques*
- *Infractions par systèmes et données informatiques*

+

Preuves électroniques

- *Toute infraction impliquant preuves électroniques*
- *Nécessaire pour procedures criminelles*
- *Pas de données, pas de preuves, pas de justice*

6

Cybercrime and e-evidence: why a strategy?
Cybercriminalité et preuve électronique: pourquoi une stratégie?

- Political commitment
- Define objectives and targets and monitor progress
- Coherence
- Define responsibilities
- Multi-stakeholder cooperation
- Budgets & resources
- Facilitate capacity building

- *Engagement politique*
- *Définir les objectifs et suivre les progrès*
- *La cohérence des actions*
- *Définir les responsabilités*
- *Coopération multipartite*
- *Budgets et ressources*
- *Faciliter le renforcement des capacités*

7

Cybercrime or cybersecurity strategy?

For discussion:

Should cybercrime be part of a cybersecurity strategy ?

or

Is there a need for a separate cybercrime strategy?

Pour discussion:

Devrait la cybercriminalité faire partie d'une stratégie de cybersécurité?

ou

A-t-on besoin d'une stratégie séparée pour la cybercriminalité?

8

Cybercriminalité et prevue-e: Eléments d'une stratégie

Objectif

Protéger la société / les individues et leurs droits dans le cyber espace

Protéction contre:

- Attaques intentionnelles contre et par TIC
- Toute infraction impliquant des preuves électroniques

- Systèmes de signalement
- Prévention
- Législation
  - Droit matériel
  - Pouvoirs procédurales, incl. sauveguardes
- Unités specialisées
- Coopération inter-institutionelle
- Formation policière
- Formation judiciaire
- Coopération publique/privée
- Coopération internationale efficace
- Investigations financières, prévention de fraude and blanchiment d'argent
- Protection des enfants

9

Cybercrime and e-evidence: Elements of a strategy

Objective

Protecting society / individuals and their rights in cyberspace

Protection against:

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

- Cybercrime reporting
- Prevention
- Legislation
  - Criminalising conduct
  - Law enforcement powers (with safeguards)
- 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

10

Structure of a cybercrime strategy / Structure d'une stratégie

1. Introduction
2. Analysis of situation (threats, challenges, trends, opportunities, strenghts, weaknesses) ▶ Justification
3. Overall objective/s
4. Sub-objectives / Sectoral objectives
5. Participants in the strategy
6. Responsibilities / management of the strategy
7. Assessment of progress and reporting
8. Annex: Action plan/s, budgets etc.

1. *Introduction*
2. *Analyse de la situation (menaces, les défis, les tendances, les possibilités, les points forts, les faiblesses) ▶ Justification*
3. *Objectif global / s*
4. *Sous-objectifs / objectifs sectoriels*
5. *Les participants à la stratégie*
6. *Responsabilités / la gestion de la stratégie*
7. *Évaluation des progrès et communication*
8. *Annexe: Plan d'action / s, budgets, etc.*

11

Managing a cybercrime strategy
La gestion d'une stratégie de la cybercriminalité

Who should be responsible for managing, leading, coordinating a cybercrime strategy or component of a cybersecurity strategy?

Accountability:

Reporting on implementation, progress, results: what and to whom?

Qui devrait être responsable de la gestion, de premier plan, la coordination d'une stratégie de la cybercriminalité ou d'un composant d'une stratégie de cybersécurité?

Responsabilité:

Rapport sur la mise en œuvre, les progrès, les résultats: quoi et à qui?

12

Cybercrime / cybersecurity strategies: examples

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

13

Cybercrime / cybersecurity strategies: examples

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

14

Cybercrime / cybersecurity strategies: examples

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.

15

Cybercrime / cybersecurity strategies

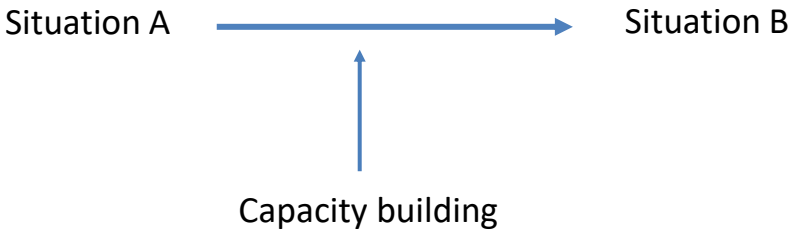
Tour de table:

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

Quelles seront les prochaines étapes concernant les stratégies de cybercriminalité ou de cybersécurité dans votre pays?

16

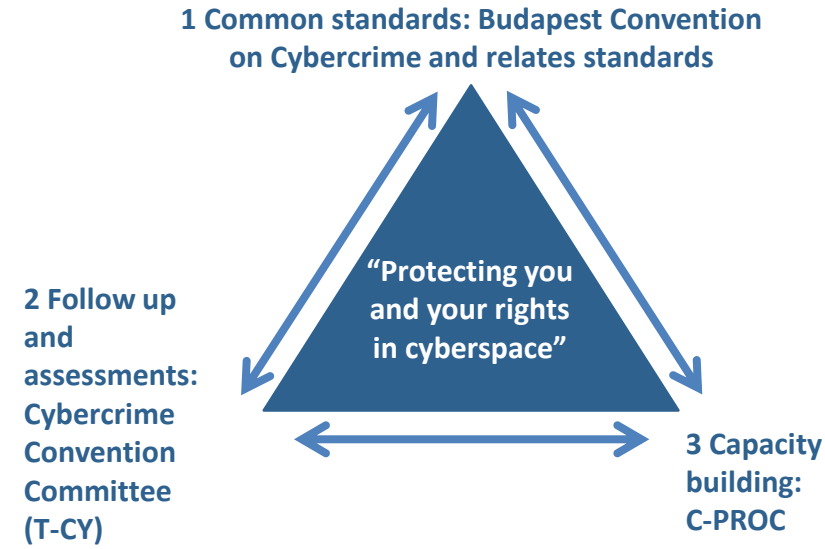
About capacity building / renforcement des capacités



Les politiques et stratégies sur la cybercriminalité et les preuves électronique avec des objectifs et des actions clairs définissent les processus que les programmes de renforcement des capacités devraient soutenir.

17

Strengthening the rule of law in cyberspace: The framework of the Budapest Convention on Cybercrime



18

Capacity building programmes

Capacity building on cybercrime & electronic evidence

Multiple programmes:

- Legislation
- Specialised law enforcement units
- Training of prosecutors and judges
- Public/private cooperation
- Targeting proceeds from crime online
- International cooperation

- Dedicated Cybercrime Programme Office of the Council of Europe (C-PROC) in Bucharest, Romania

- Priority to countries committed to implement Budapest Convention

- Support to any country regarding legislation

19