International Conference
Assessing the threat of cybercrime
Colombo, Sri Lanka, 26 – 27 March 2015

Workshop 2

Cybercrime strategies

Alexander Seger
Council of Europe

www.coe.int/cybercrime

SRI LANKA CERT|CC

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

ICTA ideas actioned

Purpose and expected outcome of the workshop
Objet et résultats attendus de l'atelier

Purpose: To strengthen policies and strategies on cybercrime

1. **Sharing experience on cybercrime and cybersecurity strategies**

2. **Developing proposals for the strengthening of cybercrime components of cybersecurity strategies or the development of separate cybercrime strategies**

Objectif: renforcer les politiques et stratégies en matière de cybercriminalité

1. **Partage d'expérience sur les stratégies de lutte contre la cybercriminalité et la cybersécurité**

2. **Elaboration de propositions pour le renforcement des composantes de la cybercriminalité de stratégies de cybersécurité ou le développement de stratégies séparées de lutte contre la cybercriminalité**

Topic 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)
- ?

Cybercrime and cybersecurity: what is the difference?

Cybercriminalité et cybersécurité: quelle est la différence?

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

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

Cybercrime vs. Cybersecurity

Cyber-/information security strategies

Security/trust/resilience/reliability of ICT

Non-intentional ICT security incidents

Disasters

Technical failure

Human failure

Intentional attacks against ICT by

State actors

Non-state actors

Terror-ists

Crimin-als

Critical infrastructure attacks

Other attacks on confiden-tiality, integrity and availability of ICT

Cybercrime strategies

Rule of law/ criminal justice and human rights

Offences by means of ICT

Offences involving ICT

Fraud
Child expl.
Terrorist use of ICT
IPR-offences
Extortion, etc

Any offence involving electronic evidence

Cybercriminalité v. cybersecurité

Stratégies de la Cybersecurité

Securité, résilience, confiance, fiabilité de TIC

incidents de sécurité non-intentionnels

Disasters

Défaillance technique

Défaillance humaine

Attaques intentionnelles contre contre TIC par

Acteurs étatiques

Acteurs non-étatiques

Terroristes

Criminels

Attaques contre infrastructure critique

Autres attaques contre la confidentialité, integrité and disponibilité de TIC

Cybercrime stratégies contre la cybercriminalité

Etat de droit/ justice pénale et droit de l'homme

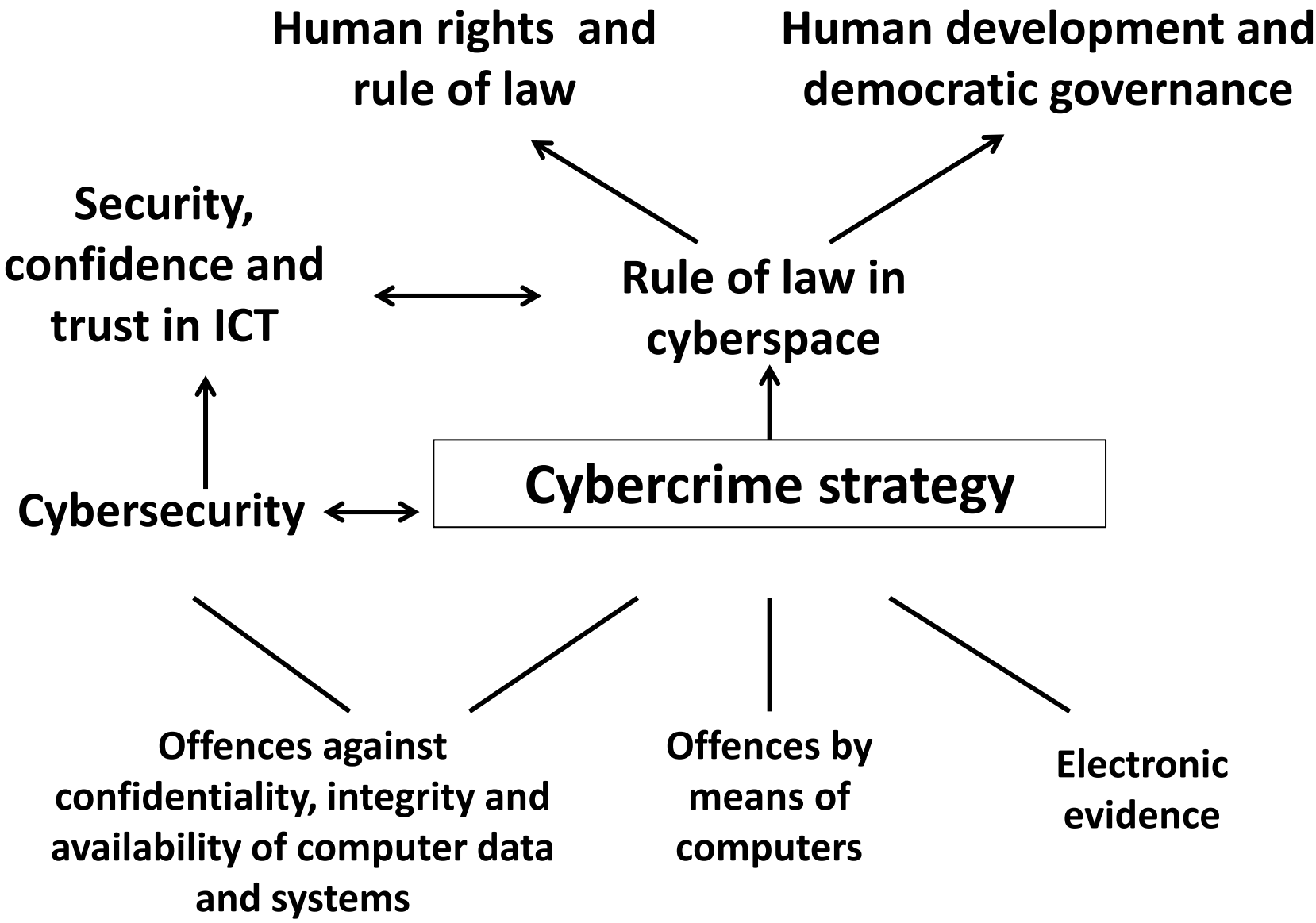
Infractions par TIC

Infractions impliquant TIC

Fraud, Exploit. Enfants, Terrorisme par TIC, IPR Extortion, etc

Toute infraction impliquant preuves électron.

Cybercrime vs. Cybersecurity



Cybercrime vs. Cybersecurity

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?

Example of a cyberCRIME strategy
Example d'une stratégie contre la cyberCRIMINALITÉ

Australia:

National Plan to combat cybercrime

(2013)

Topic 2: Purpose of a cybercrime strategy
Le but d'une stratégie contre la cybercriminalité

What needs/problems should a cybercrime strategy address?

What would be the core objective of a cybercrime strategy?

Quels besoins / problèmes devrait adresser une stratégie de la cybercriminalité ?

Quel serait l'objectif central d'une stratégie de la cybercriminalité ?

Topic 2: Purpose of a cybercrime strategy
Le but d'une stratégie contre la cybercriminalité

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

Topic 2: Purpose of a cybercrime strategy
Le but d'une stratégie contre la cybercriminalité

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

Topic 2: Purpose of a cybercrime strategy
Le but d'une stratégie contre la cybercriminalité

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**

Topic 2: Purpose of a cybercrime strategy
Le but d'une stratégie contre la cybercriminalité

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.

Topic 2: Purpose of a cybercrime strategy
Le but d'une stratégie contre la cybercriminalité

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**

Objectif d'une stratégie de la cybercriminalité (ou d'une composante d'une stratégie de cybersécurité)

Protection contre:

- **Les attaques intentionnelles contre et au moyen d'ordinateurs**
- **Tout crime impliquant la preuve électronique sur un système informatique**

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

Topic 3: Stakeholders – who should be involved?
Les parties prenantes - qui devraient être impliqués

- **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?**

Qui devrait être impliqué dans une stratégie de la cybercriminalité ou d'un composant d'une stratégie de cybersécurité?

Qui devrait prendre l'initiative? Qui devrait coordonner? Une institution ou structure de comité?

Topic 3: Stakeholders – who should be involved?
Les parties prenantes - qui devraient être impliqués

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

Topic 3: Stakeholders – who should be involved?
Les parties prenantes - qui devraient être impliqués

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.

Topic 3: Stakeholders – who should be involved?
Les parties prenantes - qui devraient être impliqués

- **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?**

Qui devrait être impliqué dans une stratégie de la cybercriminalité ou d'un composant d'une stratégie de cybersécurité?

Qui devrait prendre l'initiative? Qui devrait coordonner? Une institution ou structure de comité?

Topic 4: Elements of a strategy
Eléments d'une stratégie

What should be the elements or actions or sub-components of a cybercrime strategy or component of a cybersecurity strategy?

Quels devraient être les éléments ou des actions ou sous-composantes d'une stratégie de la cybercriminalité ou d'un composant d'une stratégie de cybersécurité?

Topic 4: Elements of a strategy
Eléments d'une stratégie

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

Topic 4: Elements of a strategy
Eléments d'une stratégie

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**

Topic 4: Elements of a strategy
Eléments d'une stratégie

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

Topic 4: Elements of a strategy
Eléments d'une stratégie

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)

- 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

Topic 4: Elements of a strategy
Eléments d'une stratégie

Objectif

Protection contre:

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

- **Systèmes de signalement**
- **Prévention**
- **Législation, incl. guaranties et protection des données**
- **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**

Topic 4: Elements of a strategy
Eléments d'une stratégie

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

1. Cybercrime policies and strategies
2. A complete and effective legal basis for criminal justice action
3. Specialised cybercrime units
4. Law enforcement training
5. Judicial training
6. Financial investigations and prevention and control of fraud and money laundering on the Internet
7. Cooperation between law enforcement and Internet service providers
8. More efficient regional and international cooperation

Strategic priority: Cybercrime policies and strategies
Adoption de politiques et de stratégies de lutte contre la cybercriminalité

- **Pursue cybercrime policies or strategies with the objective of ensuring an effective criminal justice response to offences against and by means of computers as well as to any offence involving electronic evidence.**
- ***Poursuivre des politiques ou des stratégies contre la cybercriminalité pour assurer une réponse efficace de la justice pénale aux infractions contre des ordinateurs et au moyen d'ordinateurs ainsi qu'à toute infraction impliquant une preuve électronique.***
- **Ensure that human rights and rule of law requirements are met when taking measures against cybercrime**
- ***Assurer que les conditions des droits de l'homme et de l'État de droit sont remplies au moment de prendre des mesures contre la cybercriminalité***
- **Establish online platforms for public reporting on cybercrime**
- ***Créer des plateformes en ligne de signalement public concernant la cybercriminalité***

Strategic priority: Cybercrime policies and strategies
Adoption de politiques et de stratégies de lutte contre la cybercriminalité

- **Create awareness and promote preventive measures at all levels**
- ***Sensibiliser au sujet et encourager la prise de mesures préventives à tous les niveaux***
- **Engage in public/private cooperation**
- ***Prendre part à la coopération public-privé***
- **Engage in international cooperation to the widest extent possible**
- ***Prendre part à la coopération internationale la plus large possible***
- **Evaluate on a regular basis the effectiveness of the criminal justice response to cybercrime and maintain statistics**
- ***Evaluer régulièrement l'efficacité de la réponse de la justice pénale à la cybercriminalité et produire des statistiques***

Strategic priority: A complete and effective legal basis for criminal justice action / *Etablissement d'une base juridique complète et efficace pour l'action de la justice pénale*

- **Further improve procedural law provisions to secure electronic evidence by law enforcement /** ***améliorer encore les dispositions du droit procédural relatives à la conservation des preuves électroniques par les services répressifs***
- **Evaluate the effectiveness of legislation /** ***évaluer l'efficacité de la législation***
- **Ensure that law enforcement powers are subject to conditions and safeguards in line with Article 15 Budapest Convention /** ***veiller à ce que les pouvoirs des services répressifs soient soumis à des conditions et des garanties conformes à l'article 15 de la Convention de Budapest***
- **Strengthen data protection legislation /** ***renforcer la législation relative à la protection des données***

Strategic priority: A complete and effective legal basis for criminal justice action / *Etablissement d'une base juridique complète et efficace pour l'action de la justice pénale*

- **Complete legislation and take preventive and protective measures on the protection of children against online sexual violence / *compléter la législation et prendre des mesures préventives et protectives pour la protection des enfants contre la violence sexuelle en ligne***

- **Adapt legislation on financial investigation, the confiscation of crime proceeds and on money laundering and the financing of terrorism to the online environment / *adapter la législation relative aux enquêtes financières, à la confiscation des produits du crime, au blanchiment de capitaux et au financement du terrorisme à l'environnement en ligne***

Strategic priority: Specialised cybercrime units
Création de services spécialisés

- **Establish – where this has not yet been done – specialised cybercrime units within the criminal police**
- ***Mettre en place, lorsque cela n'a pas déjà été fait, des unités spécialisées en matière de cybercriminalité au sein de la police judiciaire***
- **Enhance the specialisation of prosecutors**
- ***Spécialiser davantage les procureurs***
- **Review the functions and resourcing of specialised units on a regular basis**
- ***Examiner régulièrement les fonctions et la dotation en ressources des services spécialisés***
- **Improve procedures for cybercrime investigations and the handling of electronic evidence**
- ***Améliorer les procédures pour les enquêtes concernant la cybercriminalité et la gestion des preuves électroniques***

Strategic priority: Law enforcement training
Formation des services policières

- **Implementation of a domestic law enforcement training strategy**
- ***Mettre en œuvre une stratégie nationale de formation des services répressifs***
- **Include rules and protocols on the handling of electronic evidence in all levels of national training**
- ***Inclure des règles et des protocoles sur la gestion des preuves électroniques à tous les niveaux de la formation nationale***
- **Consider the introduction of individual training plans for specialist investigators**
- ***Etudier la possibilité d'établir des plans de formation personnalisés pour les enquêteurs spécialisés***
- **Consider the implementation of procedures to ensure best value for the investment in cybercrime training**
- ***Envisager la mise en œuvre de procédures pour optimiser l'investissement dans la formation sur la cybercriminalité***

Strategic priority: Judicial training / *formation judiciaire*

- **Adapt existing training materials and train trainers**
- ***Adapter les supports de formation existants et former les formateurs***
- **Mainstream judicial training on cybercrime and electronic evidence**
- ***Intégrer la cybercriminalité et les preuves électroniques dans la formation judiciaire***
- **Introduce measures to ensure that judicial training on cybercrime and electronic evidence is compulsory**
- ***Prendre des mesures pour assurer que la formation judiciaire sur la cybercriminalité et les preuves électronique est obligatoire***
- **Introduce training records for individual judges and prosecutors**
- ***Etablir des registres de formation des juges et procureurs à titre individuel***

Strategic priority: Financial investigations and AML
Enquêtes financières et mesures anti-blanchiment

- **Establish an online platform for public reporting on fraud on the Internet and on cybercrime in general**
- ***Créer une plateforme en ligne pour le signalement public de la fraude sur internet et de la cybercriminalité en général***
- **Promote pro-active parallel financial investigations**
- ***Promouvoir la tenue d'enquêtes financières proactives en parallèle***
- **Create trusted fora**
- ***Créer des espaces sécurisés***
- **Establish the legal framework for the seizure and confiscation of crime proceeds**
- ***Etablir le cadre juridique nécessaire à la saisie et à la confiscation des produits du crime***
- **Exploit opportunities for more efficient international cooperation**
- ***Exploiter des possibilités de rendre la coopération internationale plus efficiente***

Strategic priority: Law enforcement / ISP cooperation
Coopération entre les forces de l'ordre et les operateurs

- **Establish clear rules and procedures at the domestic level for law enforcement access to data**
- ***Etablir des règles et procédures claires au niveau national pour l'accès des services répressifs aux données***

- **Foster a culture of cooperation between law enforcement and ISPs**
- ***Favoriser une culture de coopération entre les forces de l'ordre et les fournisseurs d'accès internet***

- **Facilitate private/public information sharing across borders**
- ***Faciliter le partage d'informations privées et publiques à travers les frontières***

Strategic priority: Regional and international cooperation
Coopération régionale et internationale

- **Exploit the possibilities of the Budapest Convention on Cybercrime and other agreements on cooperation in criminal matters**
- ***Exploiter les possibilités de la Convention de Budapest sur la cybercriminalité et d'autres accords relatifs à la coopération dans les affaires pénales***
- **Provide for training and sharing of good practices**
- ***Organiser des formations et partager les bonnes pratiques***
- **Evaluate the effectiveness of international cooperation**
- ***Evaluer l'efficacité de la coopération internationale***
- **Strengthen the effectiveness of 24/7 points of contact**
- ***Renforcer l'efficacité des points de contact 24h/7 j***
- **Compile statistics on and review the effectiveness of 24/7 contact points**
- ***Compiler des statistiques sur les points de contact 24h/24 et 7 j/7 et examiner régulièrement l'efficacité de ces derniers***

Topic 5: 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.*

Topic 6: 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?

Topic 7: Issues

- **The role of CERTS in supporting national strategies**
- ***Le rôle des CERT pour soutenir les stratégies nationales***

- **Government access to private data**
- ***L'accès du gouvernement aux données privées***

- **International dimensions**
- ***Dimensions internationales***

Recommendations

- **Recommendations for enhanced policies and strategies in GLACY and other countries?**

- ***Recommandations pour des politiques et stratégies améliorées dans les pays GLACY et d'autres?***