



# Cybersecurité: Stratégie régionale et coopération internationale

Solange Ghernaouti-Hélie  
Université de Lausanne



# Plan

- Pourquoi la cybersécurité permet de lutter contre la cybercriminalité?
- Qui sont les acteurs de la cybercriminalité?
- Qui sont les acteurs concernés par la cybersécurité?
- Quels sont les dimensions de la cybersécurité?
- Pourquoi une approche globale de la cybersécurité est nécessaire?
- Quelle est l'importance d'une approche nationale?
- Quels sont les enjeux et les limites d'une approche nationale?
- Pourquoi une approche régionale peut être nécessaire?
- Quels sont les besoins, les avantages, les inconvénients et les limites d'une collaboration internationale?
- Quels sont les acteurs potentiels d'une collaboration internationale?
- Questions / Réponses

  
UNIL | Université de Lausanne

# Cybersécurité:

## Répondre aux besoins de maîtrise des risques

### ○ Risques

- Informationnel
- Technologique
- Informatique et télécoms

### ○ Origine des risques

- Naturelle: tremblement de terre, foudre, ...
- Erreur non intentionnelle - Incompétence
  - Au niveau technique
  - Au niveau procédural et de gestion
  - Lors des phases de conception, de déploiement, d'exploitation
- Malveillance d'origine criminelle (intentionnel)
  - Volonté de nuire
  - Profitabilité, enrichissement

# Le risque « Internet » d'origine criminelle

- Internet & le cyberspace
  - « pays » chaotique, complexe, fragile, hostile, non sûre
- Technologies de l'information et de la communication
  - Moyen de réaliser la malveillance
  - Cible de la malveillance
  - Outils de performance au service des organisations et activités illicites
- Les services des technologies de l'information et de la communication exposent l'institution / l'individu au risque d'origine criminelle
- Risque structurel reposant sur une rationalité économique fondée sur la recherche du profits
  - Très peu de risques criminels sont assurables
  - Certains risques criminels ne peuvent être évités du fait de l'usage des TICs



# Cybercriminalité & atteintes à la sécurité intérieure

- Atteintes aux biens immatériels / matériels / infrastructures
- Atteintes aux personnes
  - Usurpation d'identité
- Crime organisé
  - Blanchiment d'argent
  - ...
- Service de renseignement prohibé
  - Espionnage & intelligence économique
  - Investigations informatiques à des fins privées
- Terrorisme
  - Propagande
  - Recrutement
  - Recherche de fonds
  - Planification d'actions
  - ...
- Développement de groupes extrémistes
  - Propagande
  - Communautés virtuelles & réelles
  - ...

# Cybercriminalité: opportunités

- Lacune généralisée d'une certaine culture de l'informatique et de la sécurité
  - Education insuffisante de tous les acteurs
  - Irresponsabilité / Incompétences de certains acteurs
- Vulnérabilités des environnements
  - Fragilité numérique
  - Failles / outils d'exploitation des failles
- Force de justice et de police
  - Insuffisante adaptation au caractère dynamique et novateur du cybercrime
  - Moyens organisationnels, techniques, humains insuffisants
- Caractère international et transfrontalier du cybercrime
- Prise de risque minimale
  - Profits maximum

# La cybercriminalité: les acteurs

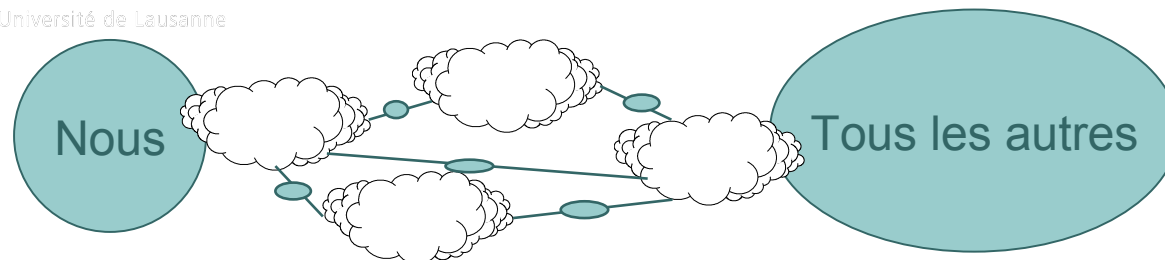
## ○ Personne physique

- De l'amateur au professionnel
- Du criminel à monsieur / madame tout le monde en passant par l'informaticien, ingénieur système à la sensibilité criminelle, le criminel compétent en informatique, ...
- De l'individu isolé à la communauté organisée

## ○ Personne morale

- Intermédiaires techniques
- Fournisseur de service, d'hébergement, de logiciel, ...
- Entreprise utilisatrice des TICs

  
UNIL | Université de Lausanne



# Cybersécurité:

## Répondre aux besoins de performance et de développement économique

- Pour développer des **services de qualité**
  - Disponibilité
  - Intégrité
  - Confidentialité
- Pour développer la **confiance** envers les services et infrastructures informatiques et télécoms
- Pour développer une **société de l'information fiable et durable**
  - Répondant aux besoins locaux de développement économique
  - Tirant partie d'une infrastructure télécoms et d'une économie mondialisées
  - Devenir un acteur incontournable du développement économique
  - Attirer des partenaires étrangers
  - Lutter contre la criminalité
    - Éviter le piège du paradis digital
  - Pour éviter la fracture sécuritaire
  - ...

# Cybersécurité: Pour répondre aux besoins de protection et de sécurité publique

- Protection des **individus**
  - Données personnelles
  - Intimité numérique
- Sécurité des **personnes**
  - Intégrité physique & morale
    - Harcèlement, manipulation, leurre, ...
- Protection du **consommateur**
  - Spam
  - Programmes malveillants (virus, logiciel espion, ...)
- Protection de l'**enfance**
  - Diffusion de contenus illicites
  - Prédateurs
- Protection des **organisations**
  - Valeurs informationnelles, processus de décision, outils de production, ...
  - Compétitivité – pérennité des organisations
- Protection de l'**état**
  - Protections des infrastructures critiques
  - Protection des infrastructures informationnelles critiques
  - e-gouvernement, services aux citoyens, ...
  - Intégrité de la nation, souveraineté de l'Etat, sûreté publique

# Cybersécurité: choisir de ne pas subir!

- Développer / implanter des mesures efficaces de sécurité
  - Mesures aux niveaux:
    - Politique
    - Juridique (justice & police)
    - Economique
    - Technologique
    - Social
- Mettre en place des processus de management et des mesures efficaces de
  - Protection
  - Surveillance
  - Prévention
  - Répression
  - Gestion de crise



# Ne pas subir, c'est:

- Effectuer une sécurité de base
  - Rendre sûr ou plus sûr
  - Mettre à l'abri du danger
  - Assurer
    - Disponibilité
    - Intégrité
    - Confidentialité
    - Imputabilité
    - Authentification
    - Non-répudiation
  - Protéger
    - les valeurs matérielle et immatérielles
    - les personnes, de la sphère privée, des droits fondamentaux (sécurité publique)
    - les institutions publiques et privées
- Faire de la résistance
  - Défense & Anticipation & Dissuasion



# Ne pas subir, c'est: comprendre pour maîtriser

- Nécessité de comprendre pour pouvoir
  - Prévenir et réagir
  - Gérer les risques et la sécurité
  - Dégager les moyens nécessaires pour
    - Eduquer
    - Mettre en place les structures organisationnelles
    - Mettre en place les mesures techniques et procédurales
    - Pour lutter contre la cybercriminalité





# Ne pas subir, c'est: disposer d'une vision stratégique

- Une vision:
  - stratégique, intégrative et globale
  - nationale et transnationale du problème
- Pour:
- Réduire les opportunités criminelles en minimisant:
  - Les vulnérabilités
  - L'exposition des cibles potentielles
  - L'interconnexion des cibles
  - Le gain pour le criminel
- Augmenter:
  - Le niveau de difficulté / d'effort / de compétences requis nécessaire à la réalisation de la malveillance
  - Le coût de réalisation des actions criminelles
  - Le risque pris par le criminel
- Sensibiliser – Eduquer – Responsabiliser
- Etre un acteur proactif et pas uniquement réactif

# De la stratégie à une politique nationale de cybersécurité

## ○ Nécessité d'une politique nationale de cybersécurité pour

- Une appréhension efficace du problème complexe
- Tenir compte de tous les aspects / besoins de sécurité:
- Des besoins de protection
  - du patrimoine numérique culturel des nations
  - du principal outil de production
  - des individus et de leurs droits fondamentaux (dignité numérique)
- Des besoins de détection
  - Centres d'alertes
  - Points de contact pour annoncer des délits
  - Centres de compétence pour investiguer et poursuivre des délits
- Des besoins de coopération
  - Entre les différents acteurs aux niveaux national, régional et international
  - Entre le Secteur privé et le Secteur public

Local

Régional

International

## ○ Mettre en place des structures organisationnelles adaptées



# Stratégie régionale & coopération internationale

- Pour répondre à tous ces besoins et enjeux: une stratégie régionale peut être efficace pour contribuer à:
  - Effectuer des actions de sensibilisation et d'éducation
  - Développer une culture de la cybersécurité
  - Partager des savoirs faire
  - Tirer partie des bonnes pratiques
  - Répondre de manière similaire à des enjeux /problèmes globaux qui caractérisent une région
  - Pallier les limites des approches nationales
  - Dépasser les frontières géographiques
  - Fédérer des ressources et savoir faire
  - Développer des mesures complémentaires, harmonisées et compatibles au niveau national, régional et international
  - Optimiser l'efficacité des réponses
  - Rationaliser les coûts



# Développer des capacités / Optimiser les performances / Réduire les coûts

- Infrastructure matérielle et logicielle
- Compétences et ressources humaines
- Système de justice et police
- Cadre légal
  - applicable au niveau national et compatible au niveau international
- Centre d'alerte et de réponse
  - **CERT (Computer Emergency Response Teams)**
  - FIRST, Forum for Incident Response and Security Teams
  
- Coopération internationale
  
- Modèle économique et volonté politique

# ITU – un programme mondial pour la cybersécurité: collaboration et coc



- Une vision unique - un forum unique pour:
  - la mise en œuvre du Sommet Mondial sur la Société de l'Information – SMSI
  - construire la confiance et la sécurité dans l'usage des technologies de l'information Ligne d'action C5
    - ITU : seul facilitateur!
- Une priorité de première importance
- Un rôle majeur à jouer à travers
  - Résolutions
  - Décisions
  - Programmes
  - Recommandations
  - Une assistance pour construire et développer les capacités à réaliser la cybersécurité
- Un parapluie global: Global Cybersecurity Agenda – GCA
- Programme Mondial Cybersecurité de l'ITU
  - Un cadre de coopération internationale dans le domaine de la cybersécurité

# Global Cybersecurity Agenda



## Policy makers

Legislative, Executive  
Stakeholders, ...

Political  
approach

## Justice and police professionals

Court, Judge, Prosecutor, Attorney,  
Regulator  
Law enforcement, ....

Legal approach

## Organization's owners, shareholders

Auditors, Executive manager  
Production manager, Human resources manager  
CIO, CISO, ...

Economic and managerial  
approach

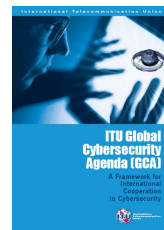
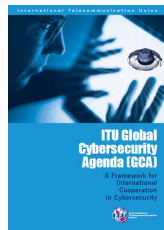
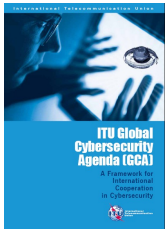
## Information Technologies professionals and providers

System, Network  
engineer  
System administrator  
Software developer  
....

Technical approach

Social approach

End user  
Citizen



Unil  
UNIL | Université de Lausanne

Prof. Solange Ghernaouti – HElie

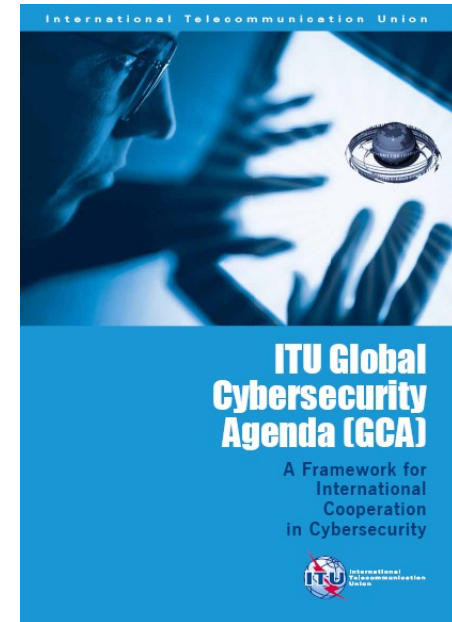


# GCA : Une approche interdisciplinaire

- **Legal Measures**
- **Technical and Procedural Measures**
- **Organizational Structures**
- **Capacity Building**
- **International Cooperation**



Recommandations



Pour une société  
de l'information sûre!

# HLEG - High-Level Experts Group: Des experts au service de l'ITU

- Chairman:
  - Mr. Stein Schjøberg, Chief Judge at the Moss District Court, Norway
- Des représentants
  - Des gouvernements
  - De l'industrie
  - Des organisations internationales et régionales
  - Des centres de recherches et institutions académiques
  - Des experts individuels



# Une grande participation : plus de 120 partenaires du monde entier

## List non exhaustive (avril 08)

- Argentina
- Brazil
- Cameroon
- Canada
- China
- Costa Rica
- Egypt
- Estonia
- France
- Germany
- India
- Indonesia
- Italia
- Japan
- Lithuania
- Malaysia
- Morocco
- Portugal
- Russian Federation
- Saudi Arabia
- South Africa
- Syrian Arab republic
- Switzerland
- United States
- African Telecommunication Union (ATU)
- Asia Pacific Economic Cooperation Telecommunications (APECTEL)
- Commonwealth Telecommunications Organisations (CTO)
- Council of Europe (CoE)
- Department of Economic and Social Affairs (DESA)
- European Information and Network Security Agency (ENISA)
- Forum of Incident Response and Security Teams (FIRST)
- International Criminal Police Organization (Interpol)
- Organisation for Economic Co-operation and Development (OECD)
- Organisation Internationale de la Francophonie (OIF)
- UMTS Forum
- United Nations Institute for Training and Research (UNITAR)
- United Nations Office on Drugs and Crime (UNODC)
- 5 individual experts
  - Authentrus
  - BITEK International Inc.
  - Cisco
  - Intel Corporation
  - Microsoft Corporation
  - Télam S.E.
  - VeriSign, Inc.
  - Etc.
- HEC-University of Lausanne
- Ecole Polytechnique Fédérale de Lausanne (EPFL), Switzerland
- Information Security Institute, Australia
- Moscow Technical University of Communications, Russian Federation
- Carnegie Mellon University

# Plus d'information: International Telecommunication Union

- **Global Cybersecurity Agenda**
  - <http://www.itu.int/cybersecurity/gca/>
- **ITU – Cybersecrité**
  - <http://www.itu.int/cybersecurity/>
- **Sommet mondial** sur la société de l'information – Construire la confiance et la sécurité ...
  - WSIS Action Line C5: Building confidence and security in the use of ICTs  
<http://www.itu.int/wsis/c5/>
- Des questions concernant l'agenda global de la cybersécurité peuvent être adressées à l'ITU : **[gca@itu.int](mailto:gca@itu.int)**





# Merci de votre attention

Professeure Solange Ghernaouti-Hélie

Université de Lausanne – Ecole des HEC

Expert international

Membre du High Level Expert Group de l'ITU

Co-leader des groupes « Organizational structures » et « Capacity building » pour le Global Cybersecurity Agenda – ITU

Auteure de plus d'une quinzaine d'ouvrages dont le « guide de la cybersécurité pour les pays en développement » ITU-D, présenté à la Conférence Mondiale du Développement des Télécommunications CMDT 2006, Doha.

Présidente de la commission sociale de l'Université

Présidente de la commission Egalité des chances de l'Université

[sgh@unil.ch](mailto:sgh@unil.ch)

[www.hec.unil.ch/sgh/](http://www.hec.unil.ch/sgh/)

