

Cybersécurité & Régulation

Tendances - Défis

Genève, 12 octobre 2026

Solange Ghernaouti

Prof. Hon.
Université de Lausanne

Plan



- Contexte
- Régulation
- Tendances & Défis
- Perspectives

Contexte

Infrastructures numériques

- Intelligence artificielle
- Données - Services
- Matériel – Logiciel – Réseau – Cloud

Infrastructures énergétiques

Infrastructures du réel

- Compétences – Acteurs - Institutions
- Ressources naturelles – Territoires géographiques
- Terre Mer Air Espace Cyberespace

Cybersécurité

Dépendances

Interdépendances

Vulnérabilités persistantes

Menaces persistantes



BLACKOUT

```
1001011100111101011
110010101001010101
10110101011011011
111011111111110110
000101010010000101111
10010101010101010100
1111100111111011001000
```

Des facteurs amplificateurs intriqués

- Tensions
 - géopolitiques
 - économiques
- Externalisation généralisée
- Ressources & Compétences
- Intelligence artificielle
- Informatique quantique

Coûts

Sécurité
/
Insécurité

Des risques systémiques complexes

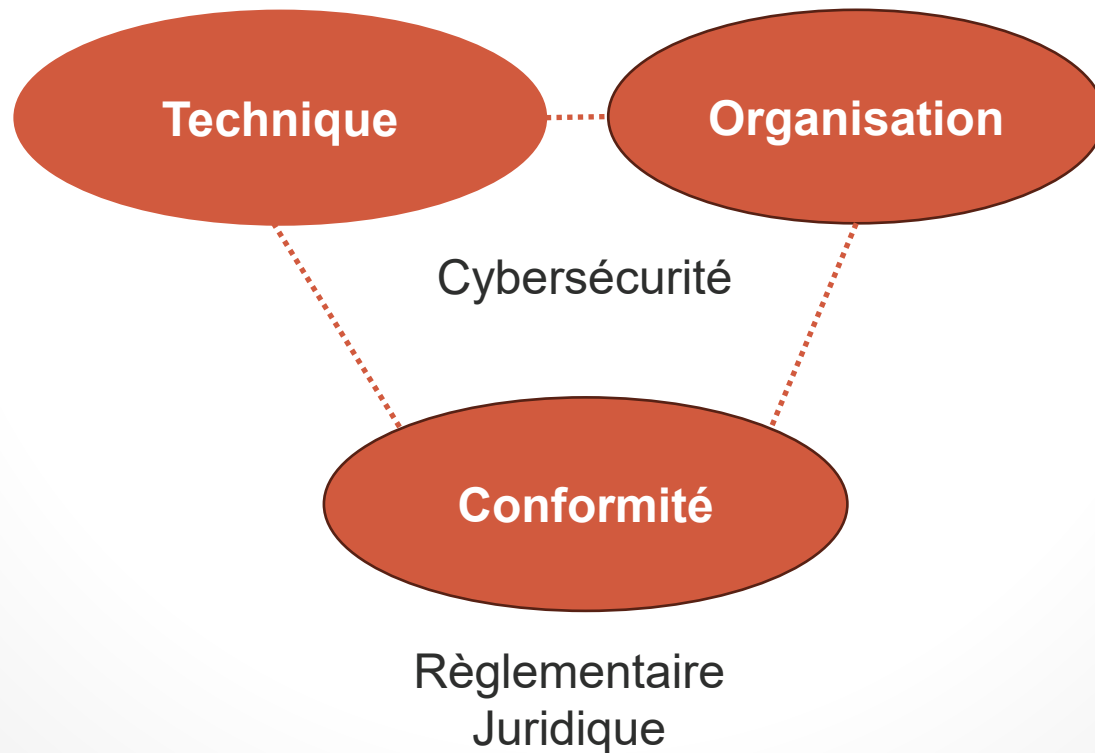
Dette technique

Dette sécuritaire

Chaines d'approvisionnement de la cybersécurité



Chaines de responsabilités ?



Cybersécurité

Qui est responsable ?

Qui paye ?

Qui maîtrise ?

Qui contrôle ?

Quelle confiance ?

Régulation

« *Les tuiles qui protègent de la pluie
ont été posées par beau temps* »

Vision
partagée

- Technique
- Normative

Régulation

Facteur de qualité et de sécurité

- Fabrication des tuiles & leur cycle de vie
- Bonnes pratiques pour les agencer & les utiliser

Importance de la régulation pour répondre à l'interconnexion des risques

Ma cybersécurité dépend de celle de mes voisins directs et indirects

Régulation



Levier de l'innovation responsable

- Expression des besoins de sécurité
 - Socle commun de référence
 - Approche intégrative
 - Autorité partagée
 - Coopération
 - Cohérence
- Diffusion des bonnes pratiques

« Celui qui impose ses règles n'a pas besoin d'user de la force »

Enjeu de la
régulation

Approche
commune et
concertée

- À opposer à des règles imposées par les acteurs les plus forts

Pour quelles finalités?

Tendances Défis

Intelligence artificielle

- Optimise la découverte et l'exploitation des vulnérabilités
- Augmente la rentabilité des attaques
- Modifie la dynamique économique des attaques
- Agent IA capables de contourner les mesures de sécurité

L'intelligence artificielle en cybersécurité

Plus de
Complexité

Gestion des risques

Gestion opérationnelle

Cybersécurité classique

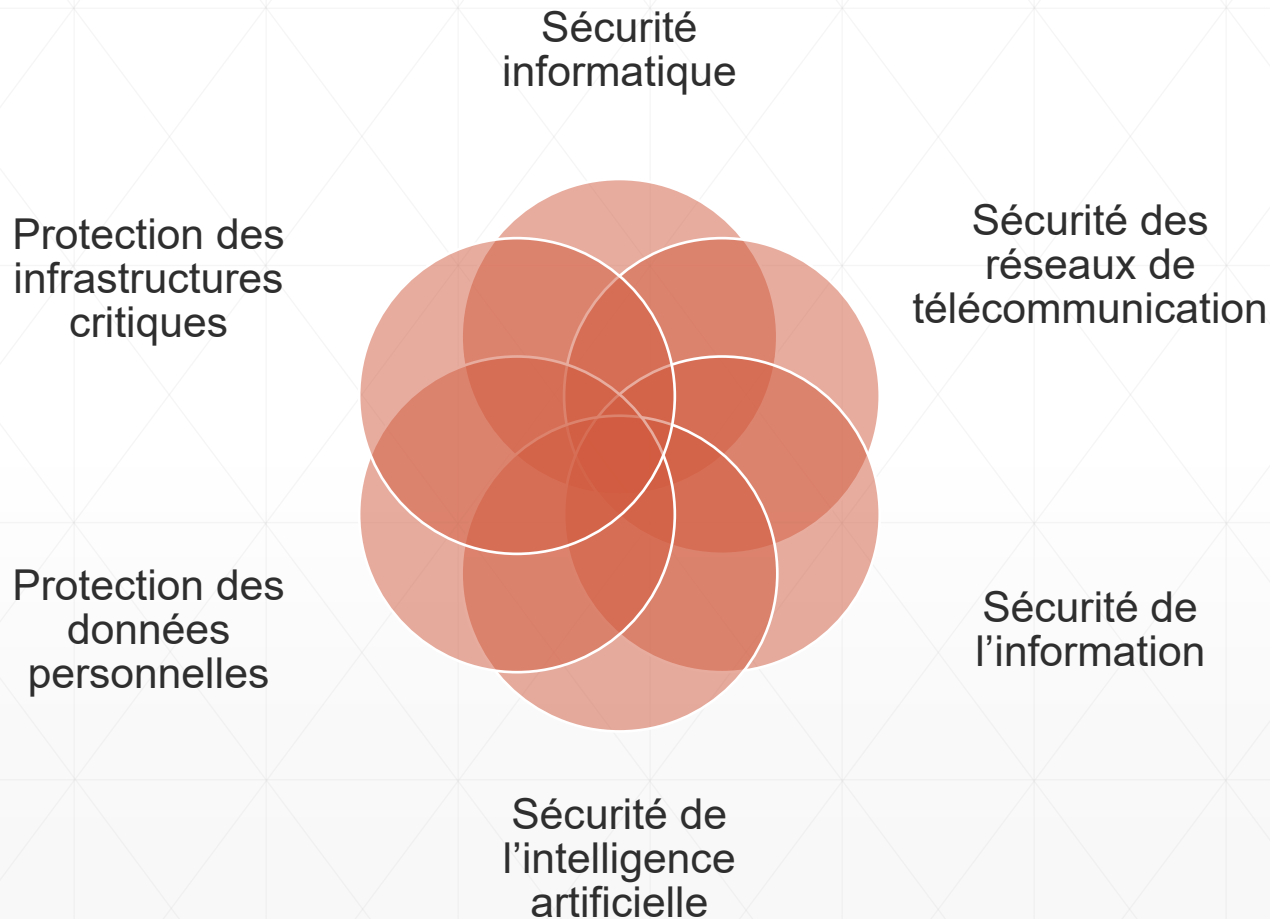
+

Cybersécurité de l'IA

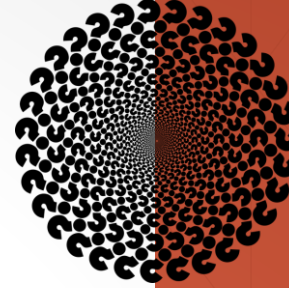
Mettre place des contrôles pour les modèles, les agents, les copilotes, les invites, les données d'entraînement, les données synthétiques, le code généré par l'IA, les identités non humaines

Des approches fragmentées & sectorielles

Des réponses parcellaires



- Pour une assurance raisonnable de cybersécurité



Défis

Volonté partagée

Complexité

Sécurité par
conception

Contrôles de
conformité

Conséquences

Mesures

- Techniques
- Légales
- Organisationnelles & procédurales

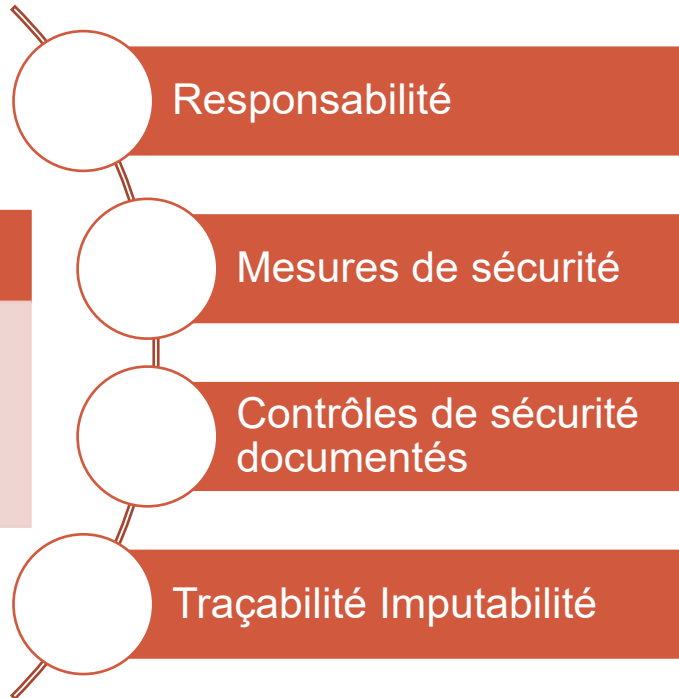
+

Capacités
Coopération internationale

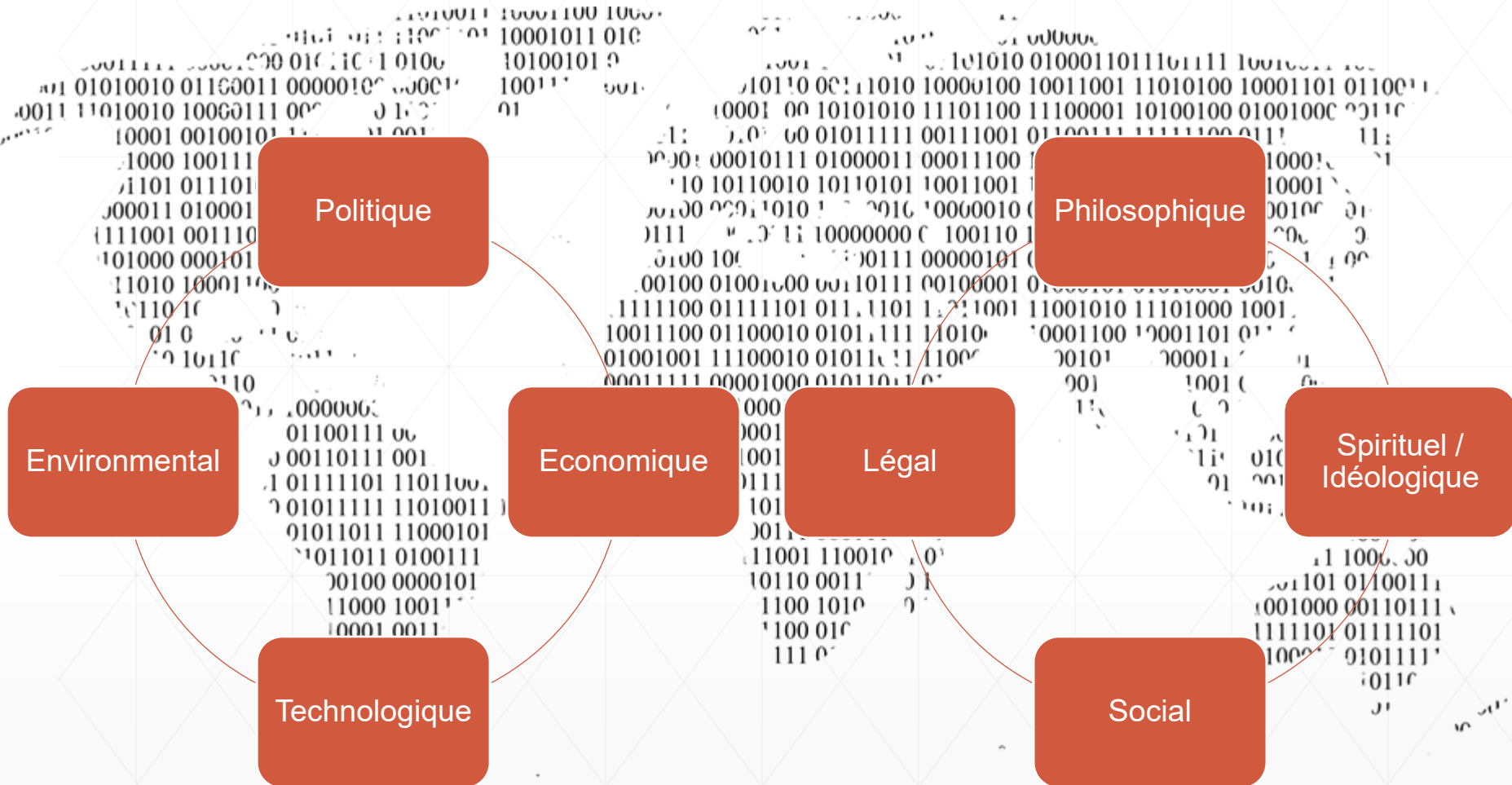
=

Global Cybersecurity Agenda ITU 2008

<https://www.itu.int/en/action/cybersecurity/pages/gca.aspx>



Défis



Perspectives

Günther Anders

L'Obsolescence de l'homme

*Sur l'âme à l'époque de la deuxième
révolution industrielle*

(1956)



PARIS
2002

ÉDITIONS DE L'ENCYCLOPÉDIE DES NUISANCES

ÉDITIONS IVREA

« Il ne suffit pas de changer le monde.
Nous le changeons de toute façon.

Il change même considérablement sans
notre intervention.

Nous devons aussi interpréter ce
changement pour pouvoir le changer à son
tour.

Afin que le monde ne continue pas ainsi à
changer sans nous.

Et que nous ne nous retrouvions pas à la fin
dans un monde sans hommes. »

**Je vous remercie de
votre attention**