

Cybersecurity & Regulation

Trends - Challenges

Geneva, 12 October 2026

Solange Ghernaouti

Prof. Hon.
University of Lausanne

Outline



- Background
- Regulation
- Trends & Challenges
- Outlook

Background

Digital infrastructure

- Artificial Intelligence
- Data - Services
- Hardware – Software – Network – Cloud

Energy infrastructure

Real infrastructures

- Competencies – Actors – Institutions
- Natural Resources – Geographic Territories
- Land Sea Air Space Cyberspace

Cybersecurity

Systemic risks



Dependencies

Inter-
dependencies

Persistent
vulnerabilities

Persistent
threats

BLACKOUT



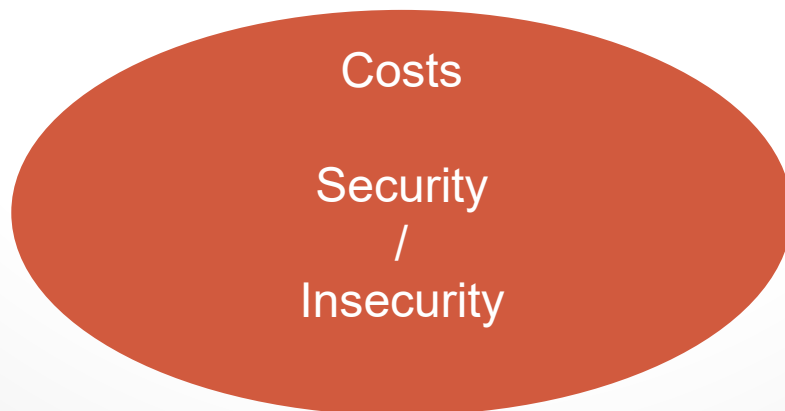
1001011100111101011
110010101001010101
10110101011011011
11101011HACKED11110110
000101010010000101111
10010101010101010100
1111100111111011001000

How should we think about cybersecurity?

How to control systemic risks?

Interconnected amplifying factors

- Tensions
 - geopolitical
 - economical
- Widespread outsourcing
- Resources & Skills
- Artificial Intelligence
- Quantum computing



Complex systemic risks

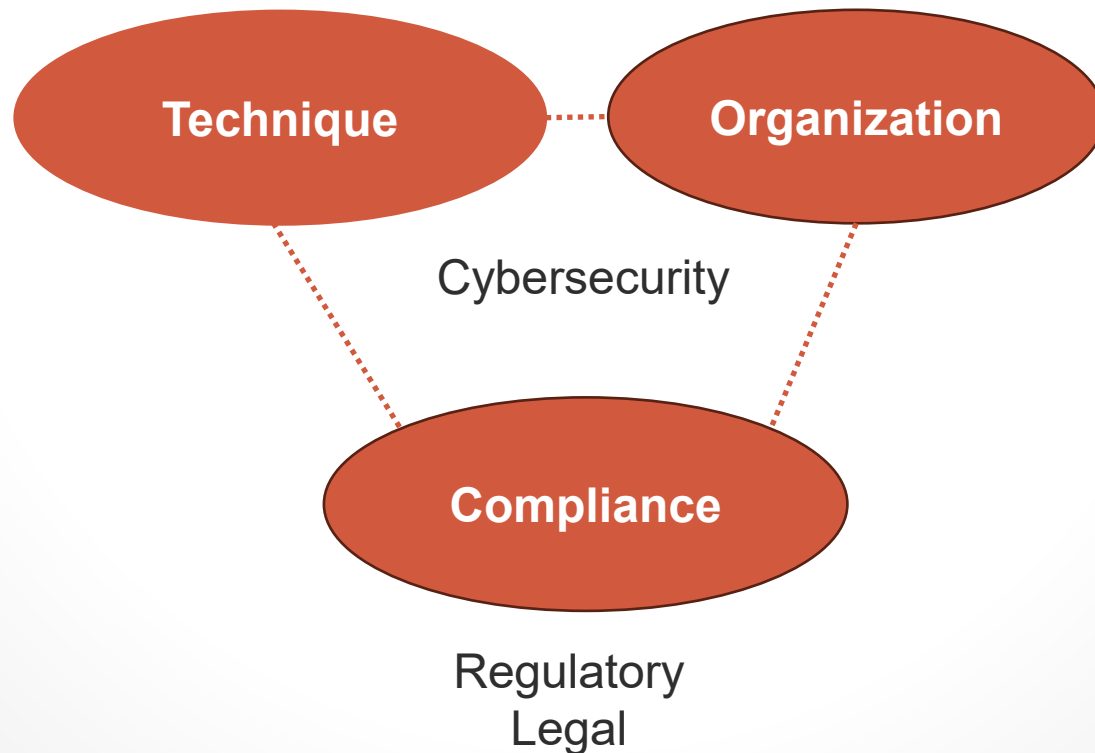
Technical debt

Safe debt

Cybersecurity supply chains



Chains of responsibility?



Cybersecurity

Who is responsible?

Who pays?

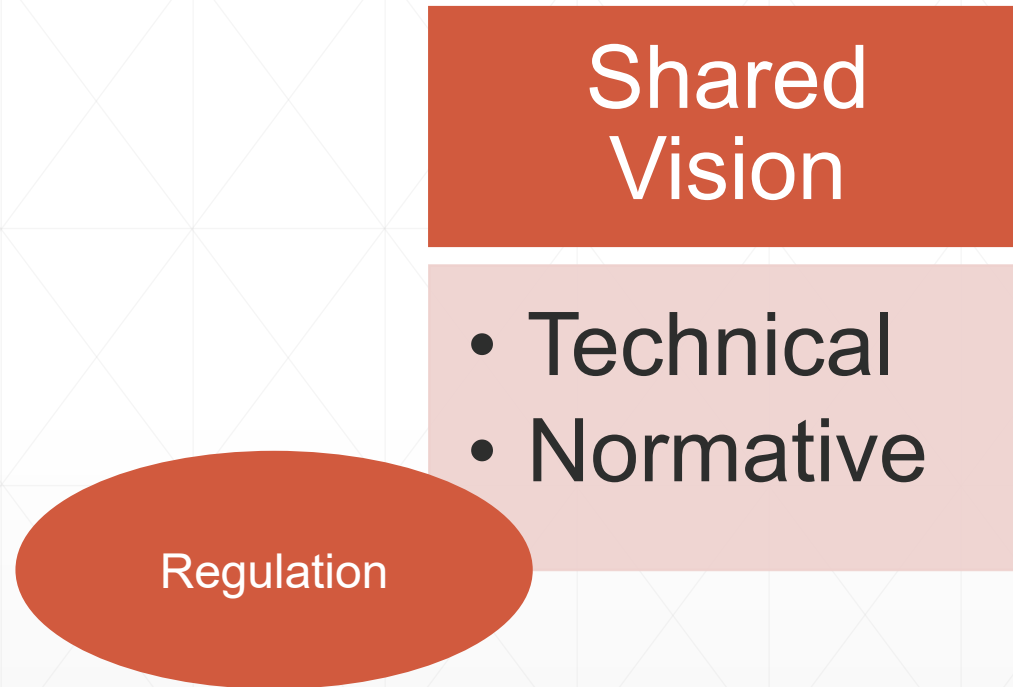
Who is in control?

Who is in control?

What confidence?

Regulation

*"The tiles that protect against the rain
were installed in good weather"*



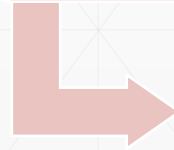
Quality and safety factor

- Tile manufacturing and life cycle
- Best practices for arranging and using them

Importance of regulation to respond to the interconnection of risks

My cybersecurity depends on that of my direct and indirect neighbours

Regulation



Lever for responsible innovation

- Expression of security requirements
 - Common base of reference
 - Integrative approach
 - Shared authority
 - Cooperation
 - Consistency
- Dissemination of best practices

"He who imposes his rules does not need to use force"

The challenge
of regulation

A common and
coordinated
approach

- To be contrasted
with rules
imposed by the
strongest players

For what purposes?

Trends Challenges

Artificial Intelligence

- Optimizes vulnerability discovery and exploitation
- Increases the profitability of attacks
- Changes the economic dynamics of attacks
- AI agent able to bypass security measures

The artificial intelligence in cybersecurity

Risk management

Operational management

More Complexity

Traditional cybersecurity

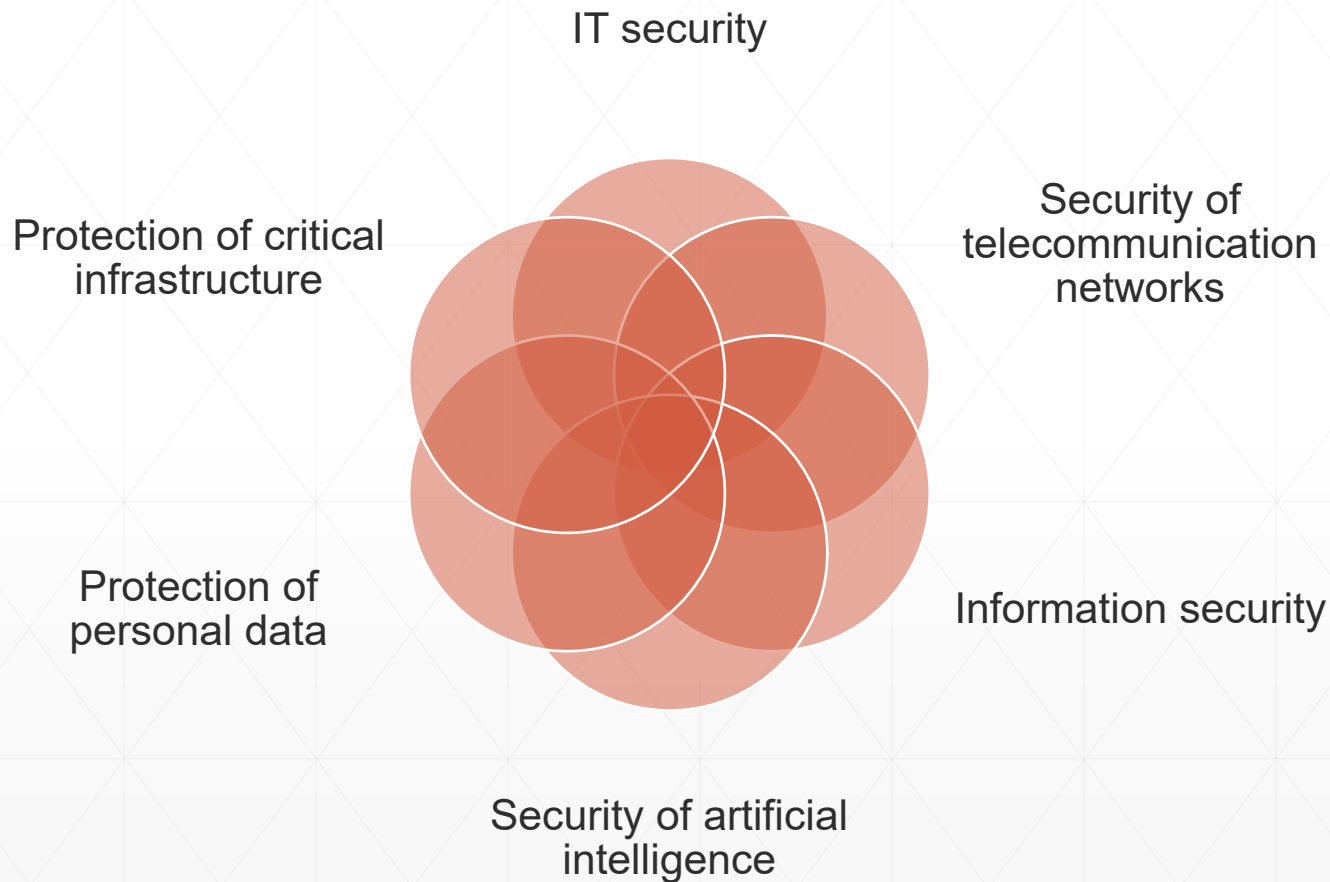
+

AI cybersecurity

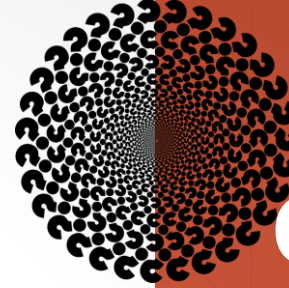
Set controls for models, agents, co-drivers, prompts, training data, synthetic data, AI generated code, non-human identities

Fragmented and sectoral approaches

Fragmented responses



- For reasonable cybersecurity assurance



Challenges

Shared will
Complexity

Security by design

Compliance checks

Consequences

Measurements

- Techniques
- Legal
- Organizational & procedural

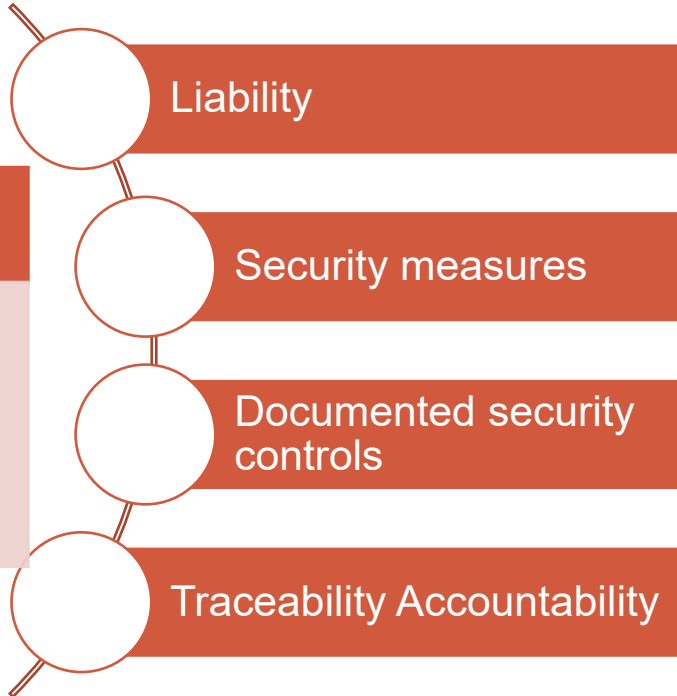
+

Capabilities
International cooperation

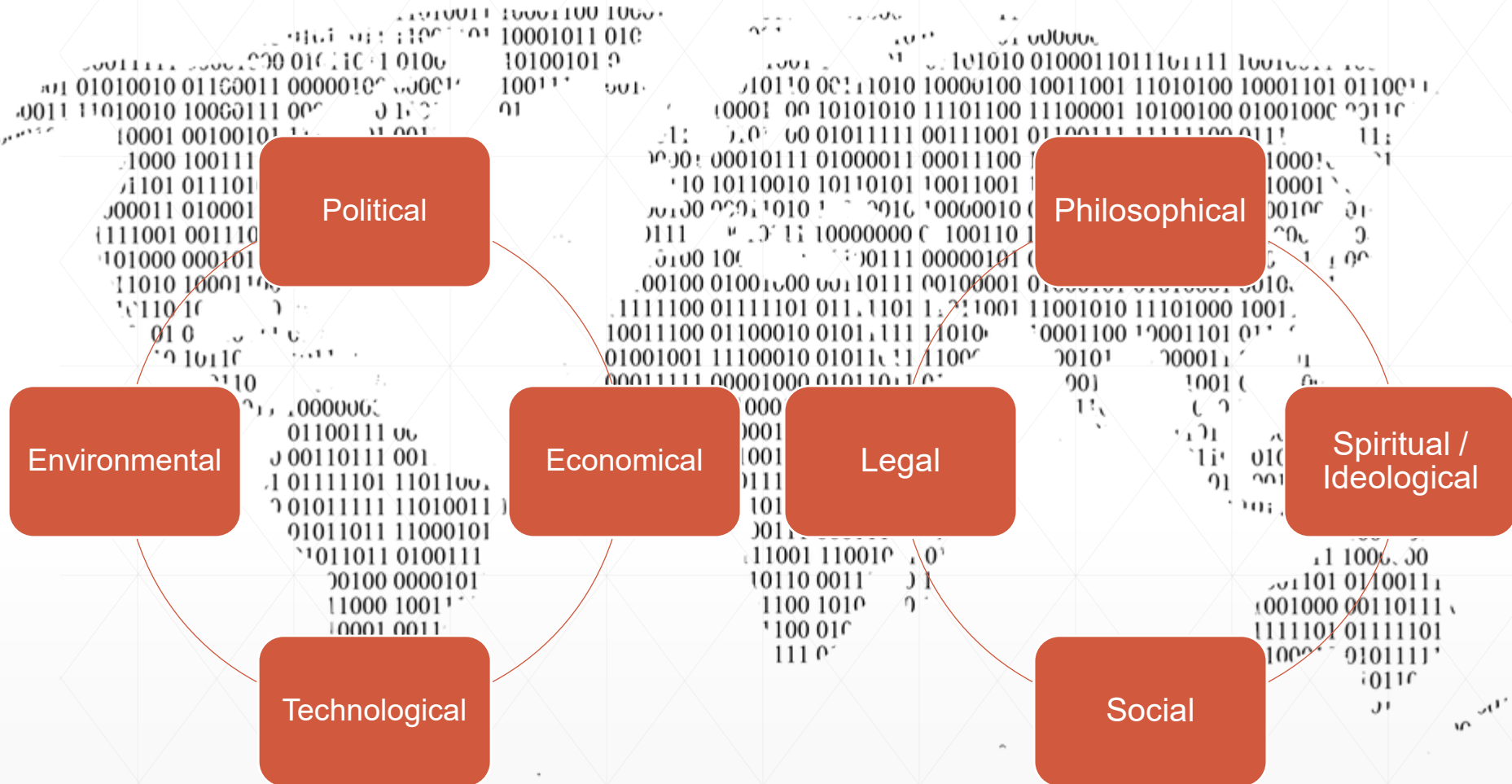
=

Global Cybersecurity Agenda ITU 2008

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



Challenges



Outlook

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

"It is not enough to change the world.
We're changing it anyway.

It even changes considerably without our
intervention.

We must also interpret this change in order
to be able to change it in turn.

So that the world does not continue to
change without us.

And that we do not end up in a world
without men. »

**Thank you for your
attention**