Increase cybersecurity maturity while leveraging synergies through coordination, collaboration and information sharing

François Thill, Director cybersecurity and digital technologies,

Ministry of the Economy

LUXEMBOURG
TRADE & INVEST

Introduction - European assessment

LUXEMBOURG
TRADE & INVEST

Introduction – the sad facts

The current situation

- Cybersecurity is increasingly discriminatory in terms of complexity and costs
- Experts in cybersecurity are scarce, and still they are working in silos
- Individual “Threat hunting” is the “new” normal, making scaling difficult
- CTI feeds are proprietary, not interoperable and most probably biased
- The cybersecurity data economy is an oligopoly preventing innovation and research, excluding SME
- 80% of the economy is at risk.

Introduction – market failures

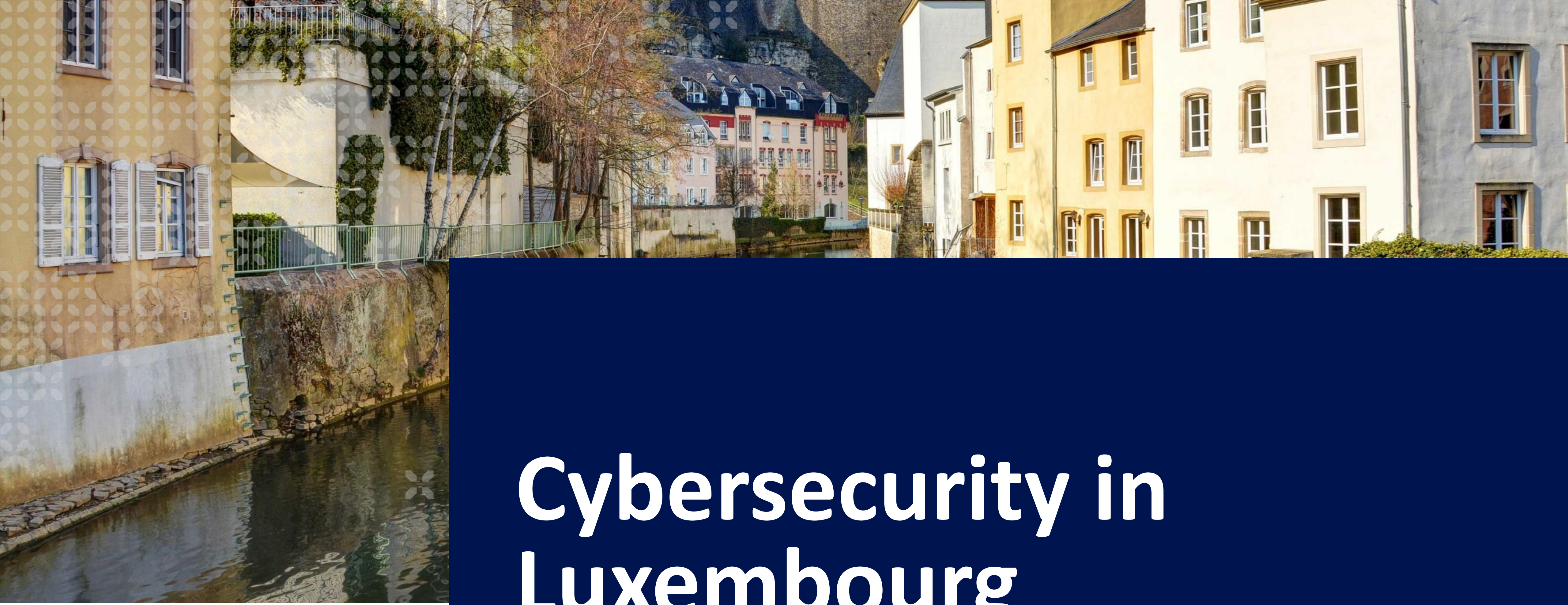
Asymmetry of information

- **Cybersecurity is a data economy** – you need IOC to detect malicious activities. They generally come with expensive and proprietary data feeds running on proprietary software.
- **SMEs are not fully aware of their cybersecurity exposure** given they have no or little information about current cyber threats that can affect them and do not know which security measures should be effectively implemented.
- SME don’t have the information what security measures are effective and efficient.
- Due to a lack of availability, accuracy and real-time threat information, **automatic (unattended) cybersecurity services for data processing activities cannot be designed** – innovation is not happening in this area.
- **Risk management, our main governance tool is mainly based on suppositions** as everybody starts with a blank page

Introduction – market failures

Coordination failure

- **Cybersecurity providers don’t define and adopt common practices to reach interoperability all along the value chains**. There is a strong fragmentation of SOC or CSIRT providers in the different market segments of the cybersecurity market.
- **The same is true for governance**, risk management is **an individual task**. **Governance** decisions rely on the **aggregation of diverging subjective appreciations**.



Cybersecurity in Luxembourg

LUXEMBOURG
TRADE & INVEST

Cybersecurity in Luxembourg

- Since 2017, **the HCPN is heading the «comité interministériel de coordination en matière de cyberprévention et de cybersécurité ».**

- The members contribute, according to their mandates, to the creation and transposition of the national cybersecurity strategy

- The main actors include Ministry of State (HCPN, SREL, ILR, SMCPN), Ministry of Foreign Affairs (Diplomacy, DoD), Ministry of the Economy (DCESI, LHC), Ministry of Digitization (CTIE)

Cybersecurity in Luxembourg

- Since 2014, Luxembourg also has a
  - **Cyber Crisis Plan**
  - **CERC «cellule d’évaluation du Risque Cyber»**

Coordination under NIS2

LUXEMBOURG TRADE & INVEST

Coordination under NIS 2 - international

The **HCPN** assumes the following roles:

- **single point of contact** (liaison function to ensure cross-border cooperation)
- **Member of the Cooperation Group** (It supports and facilitates the strategic cooperation and the exchange of information among EU Member States, provide "harmonized" guidance)
- **Member of CyCLONE** (The European cyber crisis liaison organization network is a cooperation network for Member States national authorities in charge of cyber crisis management.)

Coordination under NIS 2 - national

HCPN: Overall crisis management

GovCERT: CSIRT for public administrations and services, public establishments and critical entities under Directive (EU) 2022/2557

ILR: National authority (the regulator)

CIRCL: CSIRT for all entities not covered by GovCERT and CSIRT for Responsible vulnerability disclosure of ICT products and services

Collaboration under NIS2

LUXEMBOURG
TRADE & INVEST

Collaboration under NIS2

The goal of collaboration

- Inclusive capacity building
- Collaborative Risk management (principles of proportionality and necessity) for effective governance
- Incident detection, management and containment at all levels
- Crisis prevention and management (including cross-border)

Collaboration under NIS2

The collaborations that are needed under NIS2

- EU – HCPN – ILR – CSIRT (crisis and major incident management)
- ILR – CSIRT – OES and OIS
- Chambers and federation – OES and OIS
- CSIRT – Managed IT and cybersecurity service providers
- Managed IT service providers – managed cybersecurity service providers
- Managed IT and cybersecurity service providers – OES and OIS
- CSIRT – ISP (identification of entities)

Information exchange requirements under NIS2

LUXEMBOURG
TRADE & INVEST

Information exchange under NIS2

HCPN

- Manages crisis and coordinates national entities
- Decides whether there is need for public awareness to prevent significant incidents
- Provide national actors with guidance created by the European Coordination Group

Information exchange under NIS2

HCPN - CyCLONE

- Support the coordinated management of large-scale cybersecurity incidents and crises at operational level
- Develop a shared situational awareness for large-scale cybersecurity incidents and crises
- Coordinate the management of large-scale cybersecurity incidents and crises and support decision-making at political level in relation to such incidents and crises

Information exchange under NIS2

ILR – The national authority

- Regulate and guide essential and important entities so that they take appropriate and proportionate technical, operational and organizational measures to manage the risk
- Inform the CSIRT and SPOC about significant and/or cross border incidents

Information exchange under NIS2

CSIRT – (GovCERT and CIRCL)

- CSIRTs share information with IT and cybersecurity service providers as well as with OES and OIS

  a) Situational awareness

  b) Vulnerabilities (external scans)

  c) Alerts on threats, vulnerabilities, IOC, forensic evidence

- CSIRT will provide information exchange platforms (MISP, Open CS data space,…)
- CSIRT can be asked to scan internal networks and give technical guidance

Information exchange under NIS2

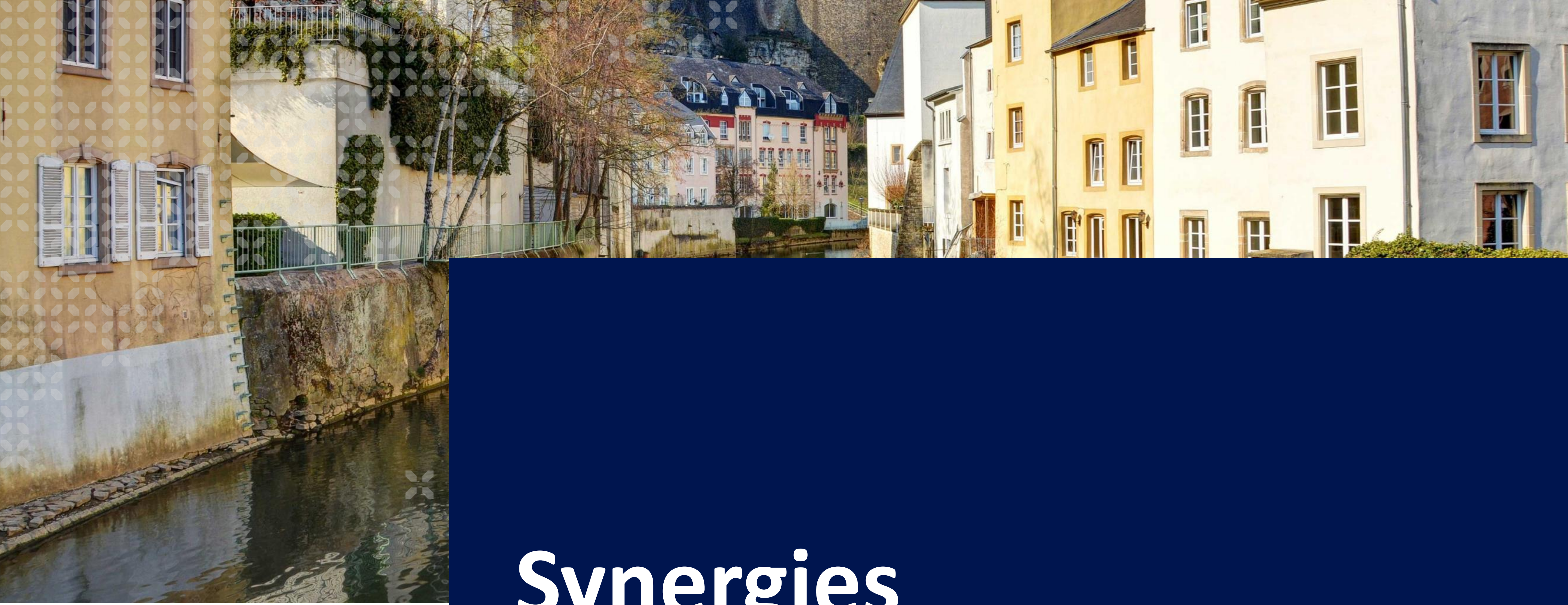
CSIRT – (CIRCL)

- CIRCL implements a responsible vulnerability disclosure program

Information exchange under NIS2

OES – OIS

- notify, without undue delay (early warning within 24 h.) the ILR any incident that has a significant impact on the provision of their services
- Where appropriate, entities concerned shall notify, without undue delay, the recipients of their services



Synergies

LUXEMBOURG
TRADE & INVEST

Synergies

- **The need for effective and efficient collaboration is obvious**, it highlights the necessity of coordination and smart information exchange.
- The CSIRT should **not distort the market**, but enhance it.
- The **collaboration must be as inclusive as possible** (in terms of company size, maturity and roles (technical, managerial)).
- **NIS2 must not lead to more technical and financial discrimination.**

Synergies

Synergies generated by HCPN, ILR, LHC

- Organizational security (policies, procedures, best practices) should by created collaboratively and shared by ILR, HCPN and LHC
- Risk management should be facts based (situational awareness), comparable and as objective as possible

Synergies

Synergies generated by CSIRT, managed service providers, managed security providers

- The synergetic potential through information exchanged is huge **if** a common taxonomy is adopted, **if** mature entities share extensively, **if** a common cybersecurity data space is used **and** cybersecurity tools, policies and behavior are adapted accordingly
- Situational awareness is understandable by technical teams and management

Synergies

Synergies generated by Chambers and federations

- Chambers and federations should consider to open cybersecurity OSPOs as an additional service for their constituency to increase inclusiveness
- Create ISAC (following the example of Fedil IND-ISAC)
- Organize training programs including top management (also in collaboration with the DLH)

Synergies

Yet OES and OIS must

- Implement proportionate and necessary security measures, following the guidance they get
- Chose their managed IT and/or cybersecurity services providers wisely
- Connect with ILR, chambers and federations
- Connect with their CSIRT and prepare for incident response. (Mind, that CSIRT will help, but they will neither perform miracles not reconstruct your data or infrastructure)

Thank you!

tradeandinvest.lu

LuxTradeInvest

www.linkedin.com/company/luxembourg-trade-and-invest/

www.youtube.com/c/LuxembourgTradeandInvest

François Thill

Director cybersecurity and digital technologies

LUXEMBOURG
TRADE & INVEST