RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CORIOLIS SEMINARS

AT ECOLE POLYTECHNIQUE FOR THE ENVIRONNEMENT

HOW DOES CYBERSECURITY CHALLENGE AND RESHAPE THE SECURITY OF THE ENERGY SECTOR ? WILL AI BECOME A GAME CHANGER ?

FRENCH CYBERSECURITY AGENCY

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION – ANSSI

Nicolas Broutin

Head of unit energy, transportation and environment Sectorial coordination

Agenda

ANSSI

Cybersecurity: what are we talking about ?

Threat evolution

Cybersecurity strategy evolution

Relationship between AI and cybersecurity

ANSSI

ANSSI PRESENTATION

ANSSI

PREMIER MINISTRE

SGDSN

Agence nationale de la sécurité des systèmes d'information (French Cybersecurity Agency) created in 2009

National authority for cyber security and cyber defence

Government organisation that reports to the General Secretariat for Defence and National Security (SGDSN)

Defensive mission (not offensive)

Role: to protect the nation from cyber attacks

Primary targets: Operators of critical national infrastructures ("OIV"), operators of essential services ("OES") and administrations

ANSSI’s role in the State’s cyber governance

ANSSI is responsible for implementing and leading the State’s actions in the field of cyber security and cyber defence. They are organised around the following three pillars:

1. “The State responds to attacks”

2. “The State secures its systems”

3. “The State protects the nation”

ORGANISATION

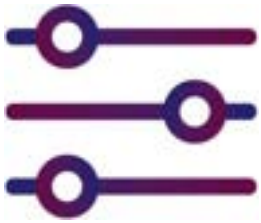
ANSSI’s main missions

Defending

Knowing

Sharing

Supporting



Regulating

4 departments and 1 mission

Expertise Department

Operations Department

Resources Department

Strategy Department

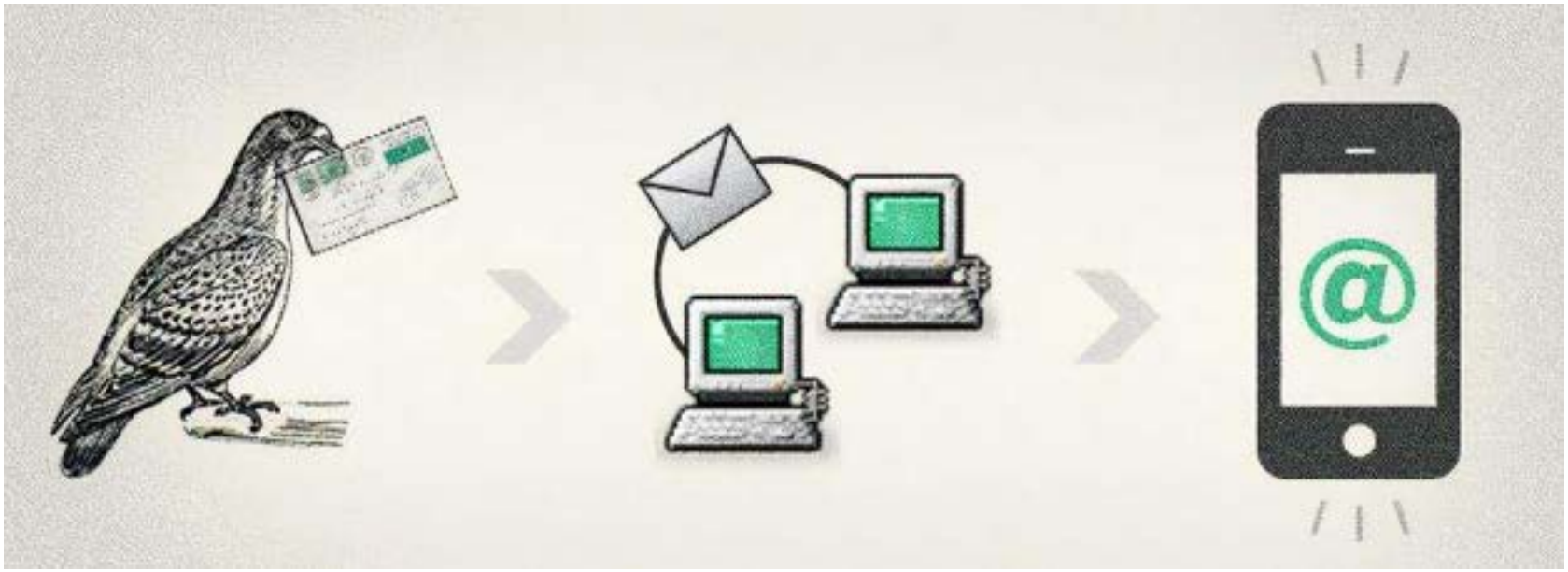
The Control and Supervision Mission

FROM INFORMATION SYSTEM EVOLUTION BY THREAT EVOLUTION TO CYBERSECURITY STRATEGY EVOLUTION

CYBERSECURITY: WHAT ARE WE TALKING ABOUT ?

Cybersecurity: what are we talking about ?

1. Computer science/internet : not for computer scientists



Cybersecurity : From what are we talking about ?

2. Computer science became a big society issues

Cybersecurity : From what are we talking about ?

2. Computer science became a big society issues

Cybersecurity : From what are we talking about ?

2. Computer science became a big society issues

Cybersecurity : From what are we talking about ?

2. Computer science became a big society issues

Cybersecurity : a cross-functionnal, horizontal and pervasive tool

Threat global evolution

- <u>Lesson 1:</u> Cybersecurity is cross-functionnal, horizontal and pervasive tool and depending to the weakest system

- …

THREAT EVOLUTION

The cyber threat

A target

Administrations
OIV
OES

An attacker

Competitors
Hacktivists
Criminals
Governments

An attack

Defacement

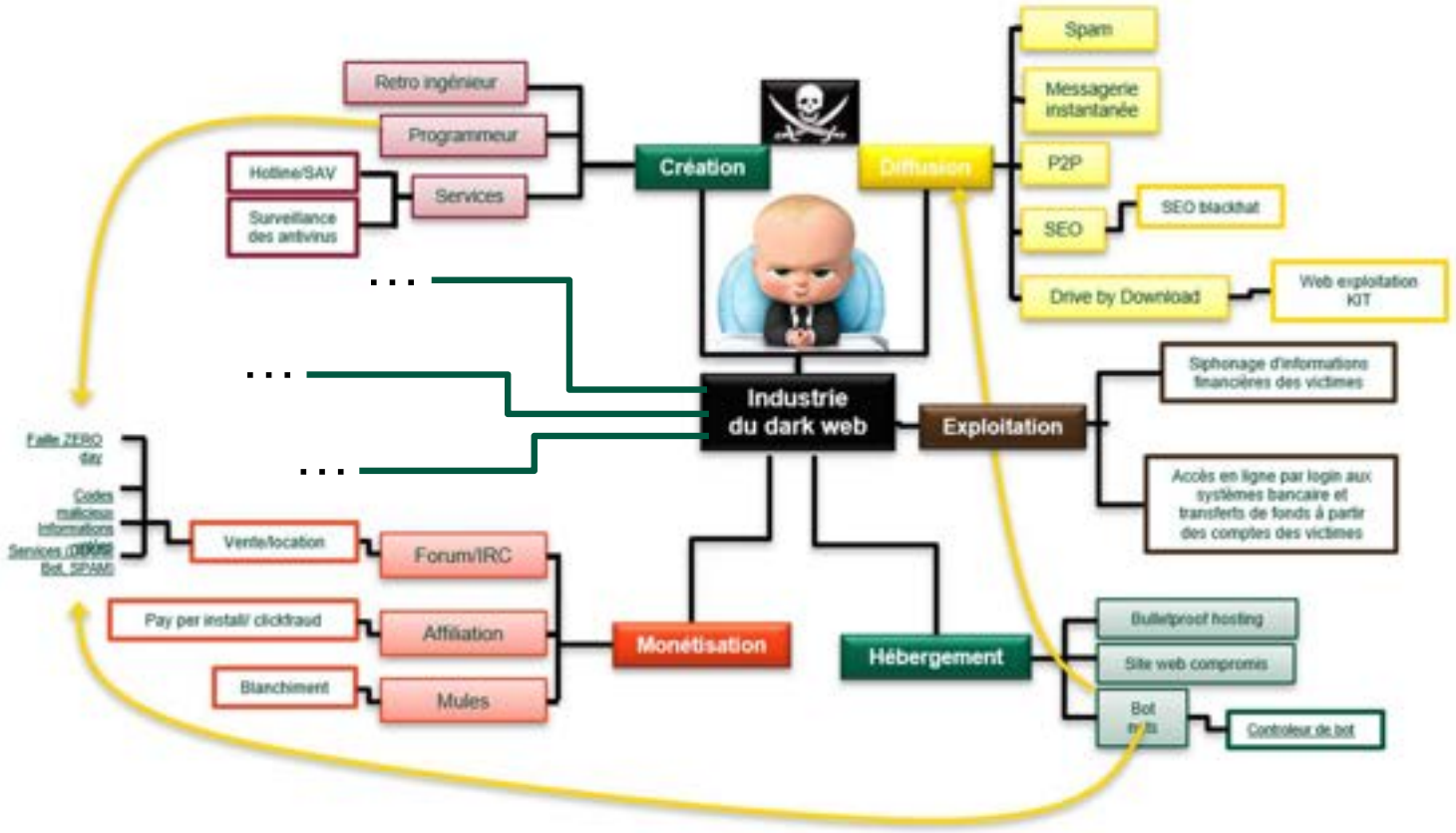
DDoS

Ransomware

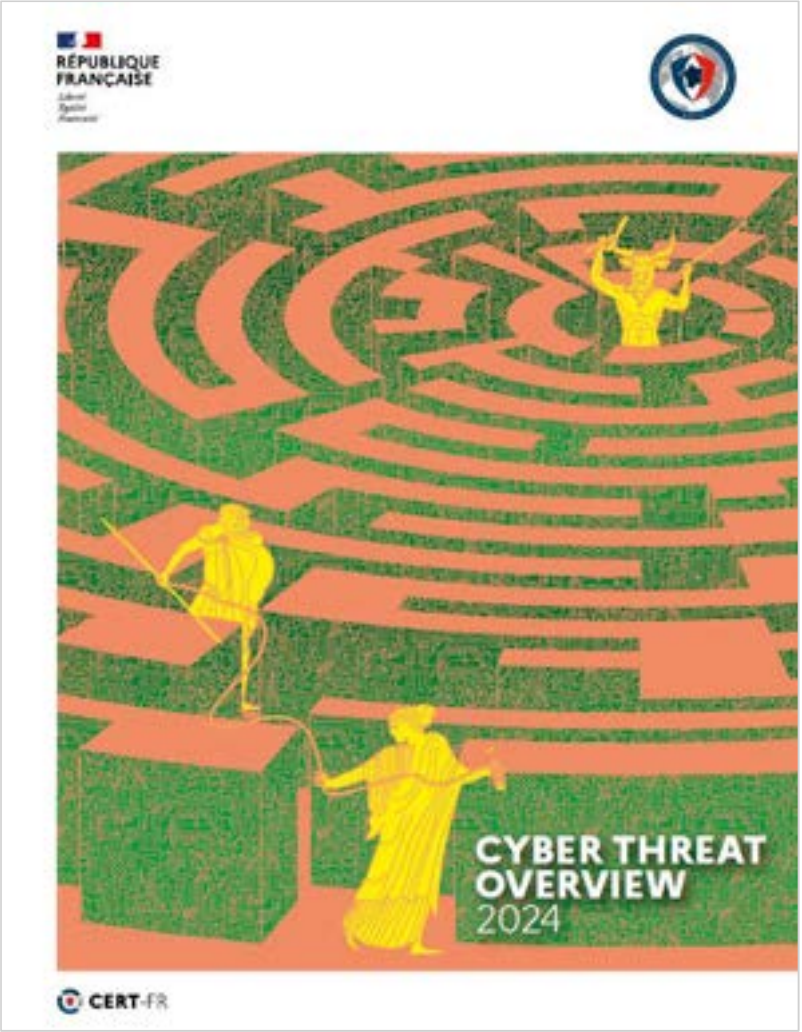
Espionage/
destabilisation

Data leak /
infostealers

Threat evolution



Cyber Threat Overview 2024

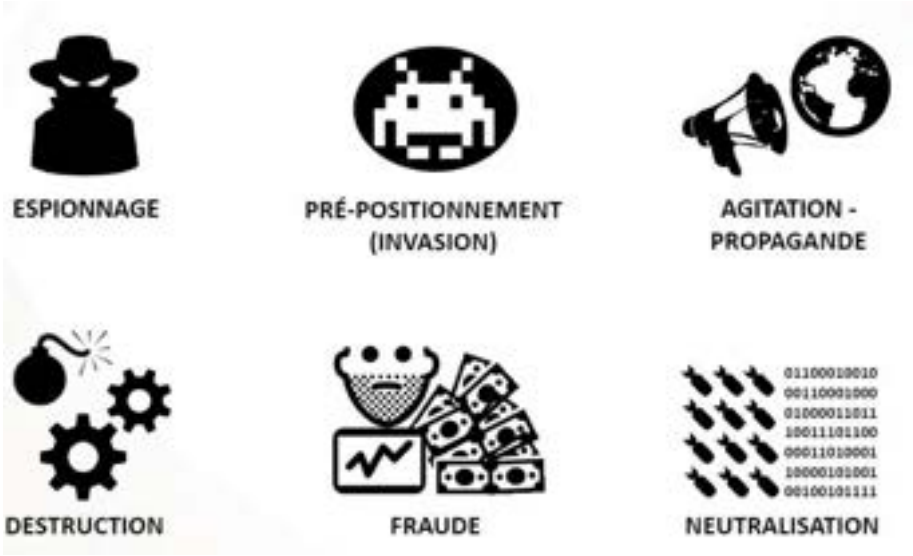


Threat in energy sector

Energy sector specificities

- Major players are highly targeted
- Smaller ones serve as easy entry points

⇒ Sector perceived as having a lot of money



Major trends:

- Follows the general trend: significant increase in ransomware attacks
- Pre-positioning of malicious actors: network mapping / deployment of malicious code

⇒ Sector highly sensitive to geopolitical context: sabotage by state actors

⇒ Main attacks have targeted power grids (e.g., Ukraine)

Recent examples

01net · Actualités · Cybersécurité

Une cyberattaque frappe Schneider Electric, géant français de l'énergie

Publié le 6 novembre 2024 à 11:45

BFM - Tech - Cybersécurité

Cyberattaque: EDF reconnaît des connexions "illicites" mais dément un piratage massif

Publié le 04/02 à 12h51

Stratégie entreprise | Analyse sectorielle

Cyberattaques OT : le secteur énergétique face à 329 milliards de dollars de risques

Un rapport Dragos révèle l'ampleur des vulnérabilités cybernétiques des infrastructures énergétiques mondiales. Les pertes potentielles atteignent des sommets historiques.

L'USINEDIGITALE Intelligence artificielle Cybersécurité Big Tech Robotique Cloud

Une cyberattaque frappe un barrage norvégien, forçant son ouverture pendant quatre heures

Alice Vitard

Publié le 1er juillet 2025 à 10h00

Partager

en energynews | Le 14 août 2025

Example of attack : systemic dimension

Colonial Pipeline (mai 2021)

- 45% of fuel consumption on the East Coast
- Shutdown on May 7, 2021, state of emergency affecting 17 states
- APT attack (long-term observation)
- Targeted IT system: customer billing at the pump (!)
- Approximately 100 GB of data exfiltrated following the DarkSide group's campaign, ransom of 75 BTC (4.4 million USD) paid
- Infection vector via an old VPN access whose password was available in DarkNet databases

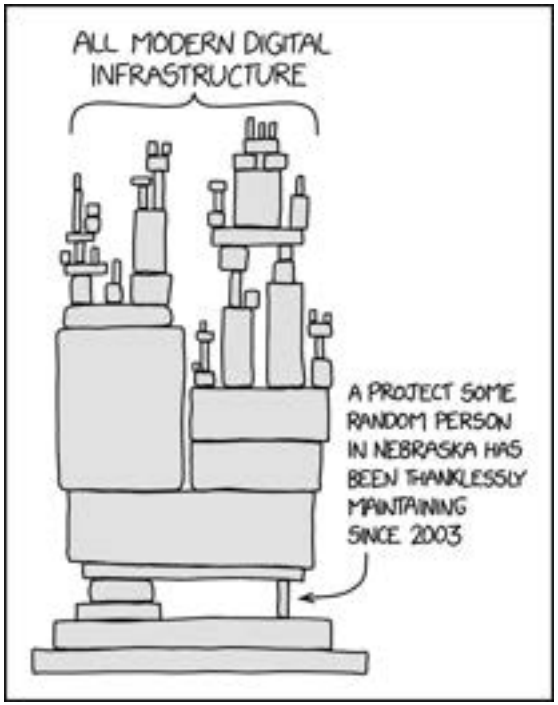
Threat global evolution

Evolution of the threat and its impacts on society:

New targets (SMEs, mid-sized companies, local authorities)

Vulnerability of the supply chain

Severe consequences of ransomware attacks



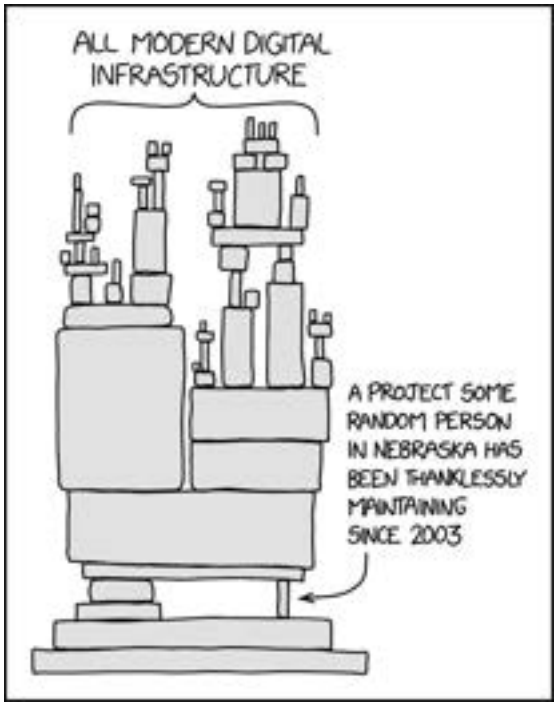
Source : https://xkcd.com/2347/

Threat global evolution

Targeting the supply chain (software… and beyond!)

- **Compromising a software application in order to reach all of its users.**

- **Compromise of a service provider's resources with access to the target's information system:**
  - The attacker can then exploit the privileges and resources that the provider holds on the target's system;
  - In doing so, they take advantage of the provider's weaker security level to reach the final target in a discreet manner.



Source : https://xkcd.com/2347/

Threat global evolution

- Lesson 1: Cybersecurity is cross-functionnal, horizontal and pervasive tool
- “Lesson” 1bis: The whole system is only as strong as its weakest point

- Lesson 2: Shift from a handcrafted threat to an organized threat

- …

STRATEGY EVOLUTION

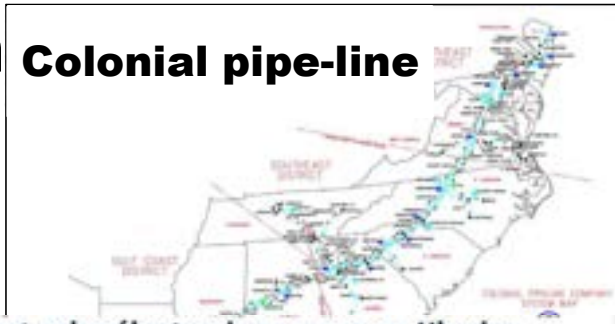
Strengthening the sectoral strategic vision

Crisis situation – A sector disrupted after years of stability

Emergence of a critical situation

- Several events :
  - Reveal the causal links between operators during a cybersecurity incident
  - Reveal an increasing cybersecurity risk because of physical or geopolitical incident

Ex. : NotPetya, Colonial pipe-line, Conflit RU/UA



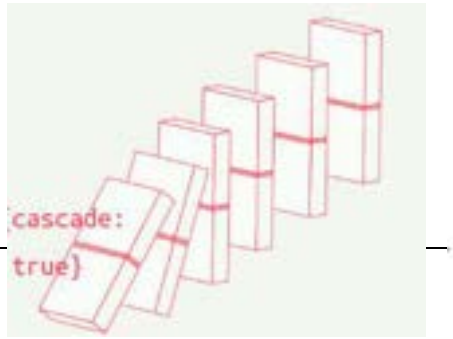
Strengthening the sectoral strategic vision

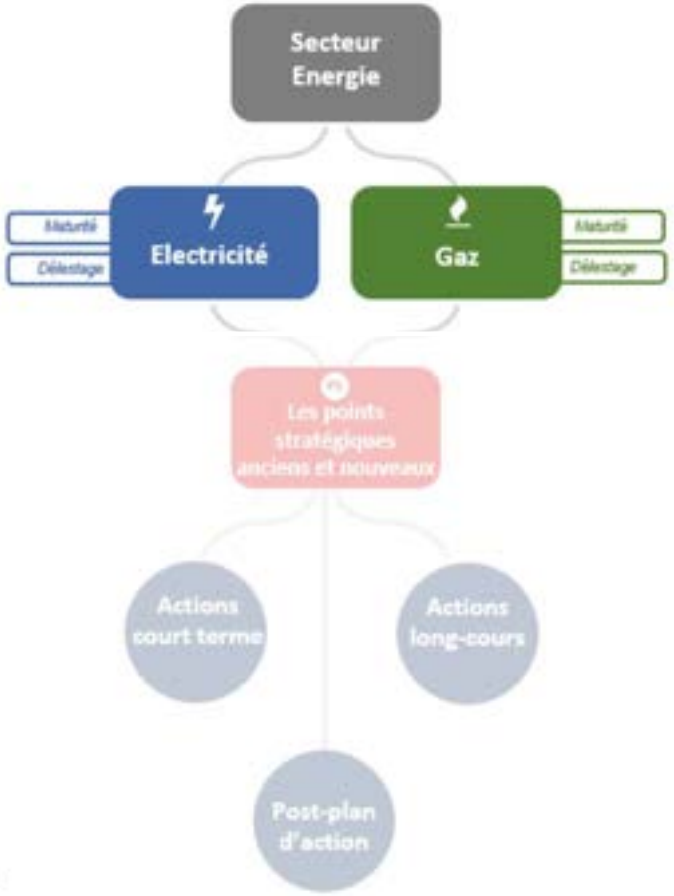
Step 1: A crisis situation – Responding to the emergency

- **Real-time response**
  - Assessment of the situation
  - Securing production
  - Preventing potential concomitant risks

The assessment:

⇒Strengthening our resilience





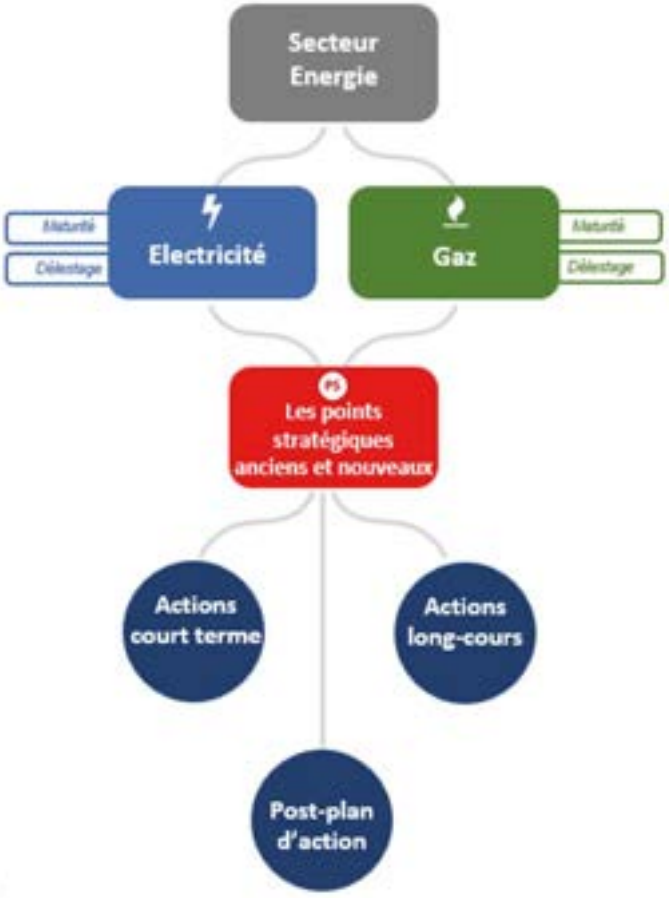
Moving towards hybrid strategies by sector

Step 2: Strengthen and act for resilience – Look further ahead

- **Broaden our knowledge on the risks affecting a sector:**

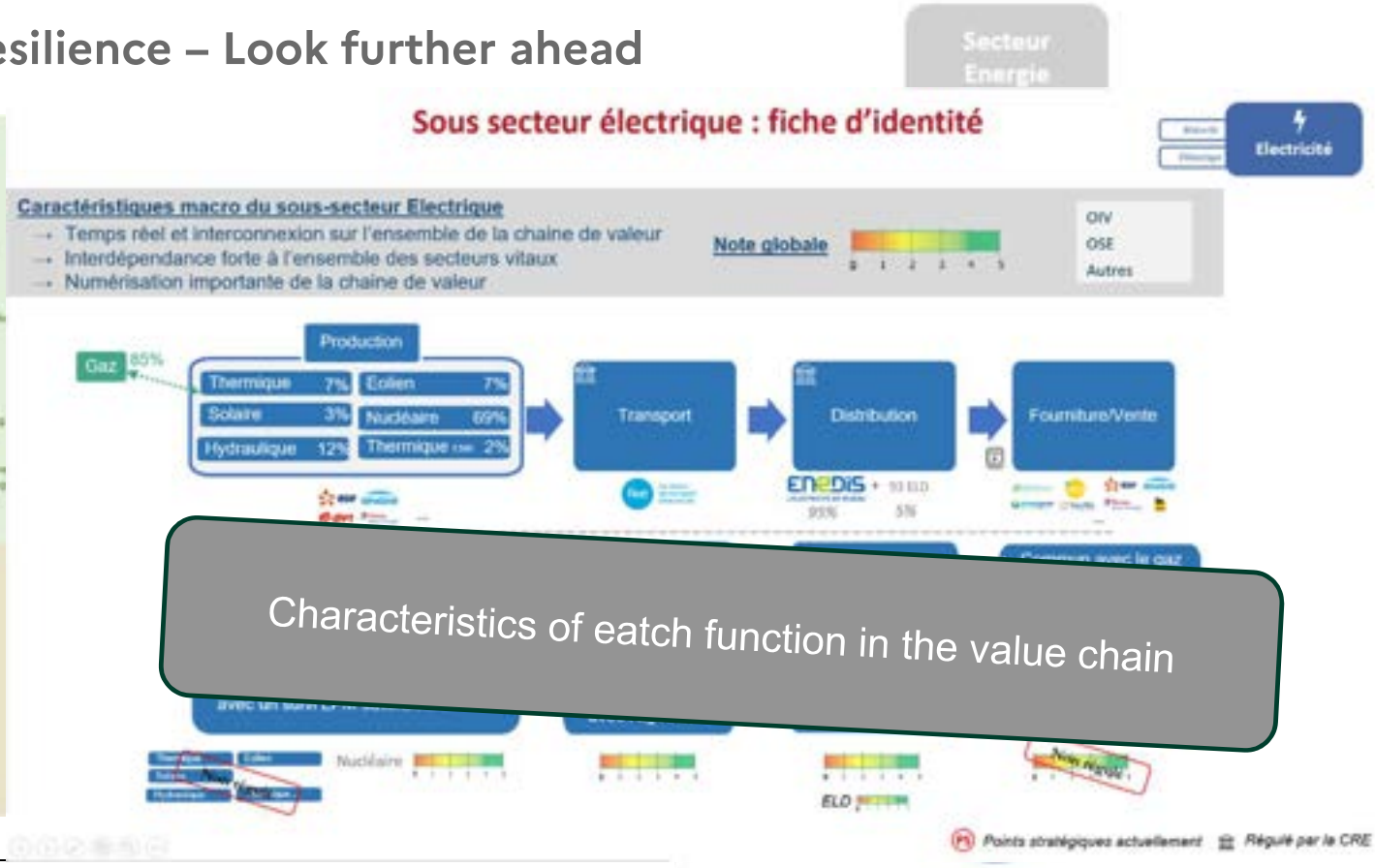
⇒ **Development detailed analysis to build a "reactive" action plan**

⇒ **A new approach to securing our critical sectors: <u>a systemic approach</u>**



Moving towards hybrid strategies by sector

Step 3: Strengthen and act for resilience – Look further ahead



Characteristics of eatch function in the value chain

Moving towards hybrid strategies by sector

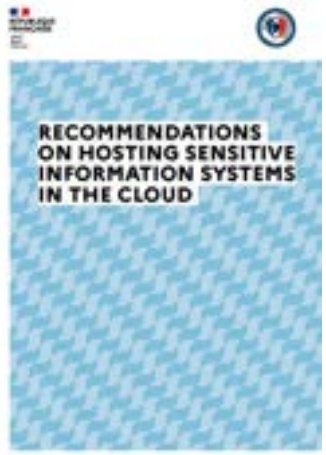
Step 4: Strengthen and act for resilience – Reinforce our capacity to act

- **Even with a good knowledge of the sector, we haded challenges to face with:**
  - Legitimize the analytical work
  - Get stakeholders on board

⇒ **First sectorals risks analysis**

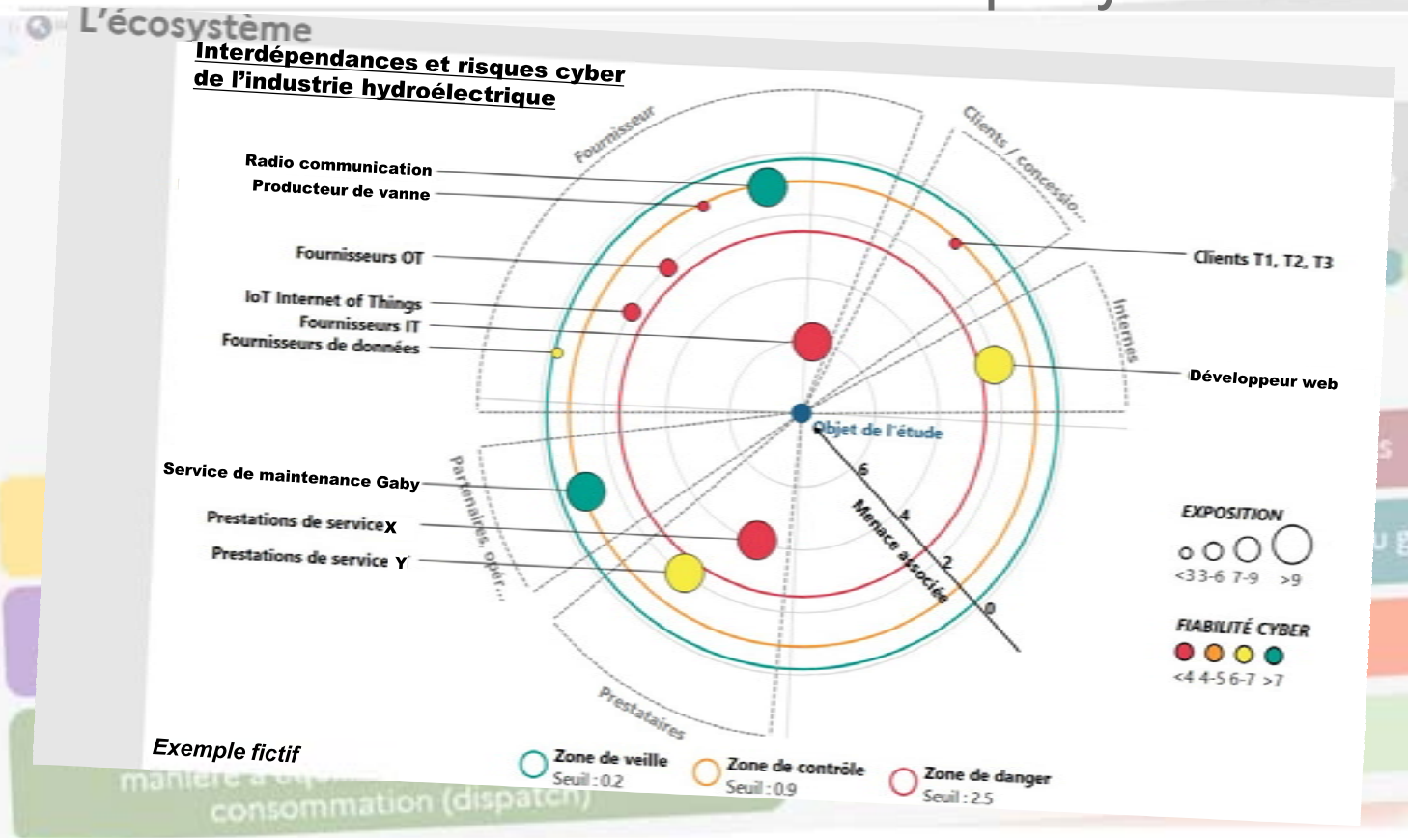
=

First systemic risk analysis



Moving towards hybrid strategies by sector

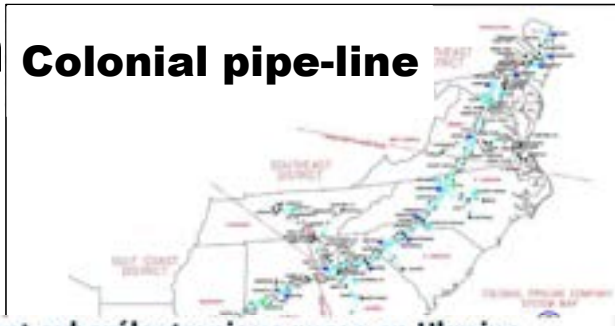
Step 4: Strengthen and act for resilience – Reinforce our capacity to act



Strengthening the sectoral strategic vision

Crisis situation – A sector disrupted after years of stability

- We talked about the fact Cyber was systemic : by the supply et value chain
- We saw that we needed to convince the companies and admin to follow our action plan + we wanted our analysis to be safe
- So we built a new concept of risk analysis



Moving towards hybrid strategies by sector

Step 4: Strengthen and act for resilience – Reinforce our capacity to act

<u>Outputs:</u>

⇒**Specific threat scenarios**

⇒**Action plan highlighting the links with value chains and supply chains**

Strategy evolution

- Lesson 1: Cybersecurity is cross-functionnal, horizontal and pervasive tool
- Lesson 2: Shift from a handcrafted threat to an organized threat
- <u>Lesson 3:</u> We have to reinforce the cybersecurity national strategy
- …

REGULATION EVOLUTION IN THE MEANTIME

Past regulations to…

2009
Creation of ANSSI

2011
ANSSI becomes the national authority for the defence of information systems

2013
Adoption of the "LPM" Critical Information Infrastructure Protection Law imposing measures on OIVs

2015
French national digital security strategy

2016
Adoption of the NIS Directive

2018
Identification of OESs

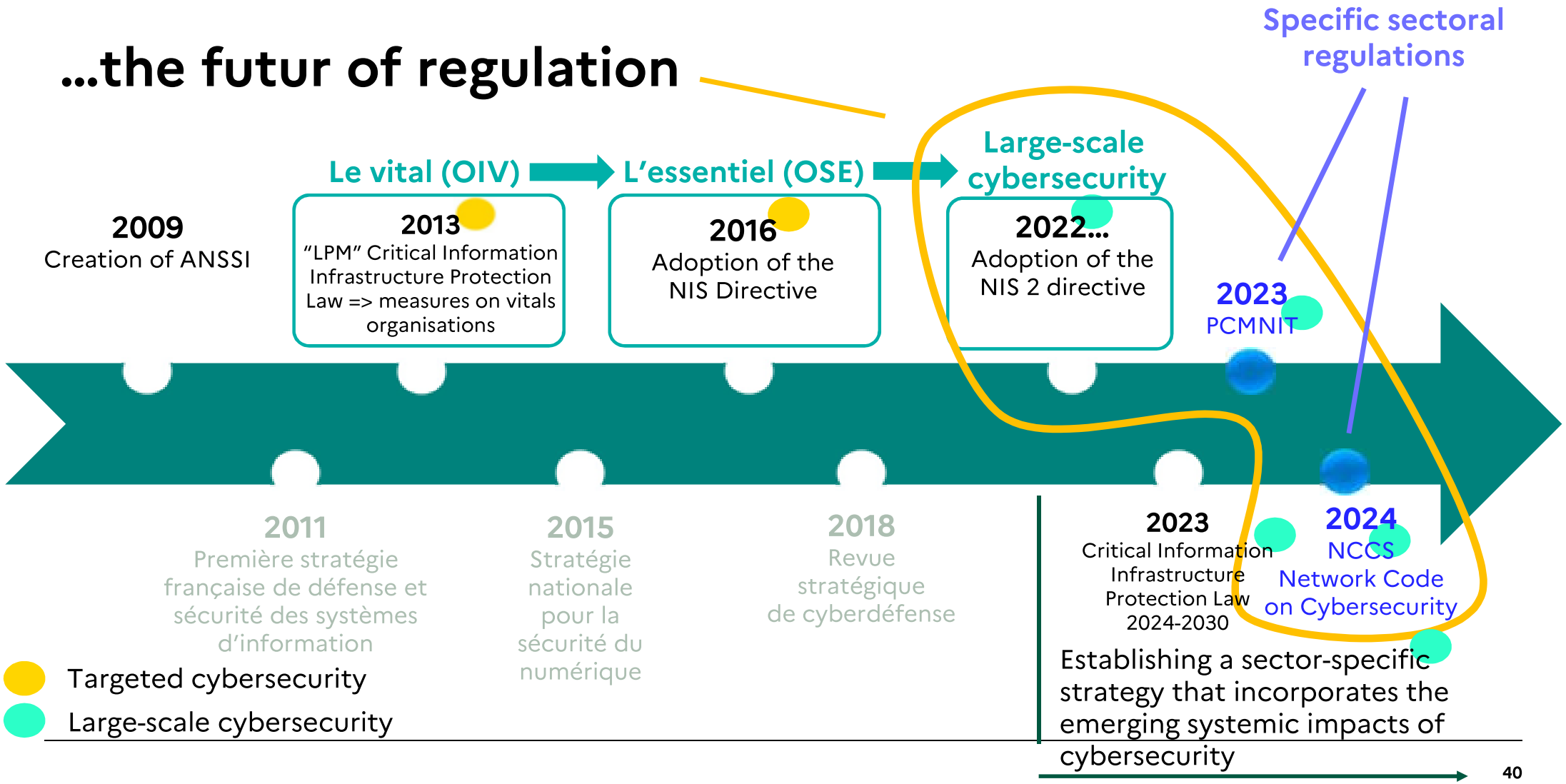
2022
Adoption of the NIS 2 Directive

Establishing a sector-specific strategy that incorporates the emerging systemic impacts of cybersecurity

Targeted cybersecurity

Large-scale cybersecurity

…the futur of regulation



Regulation evolution

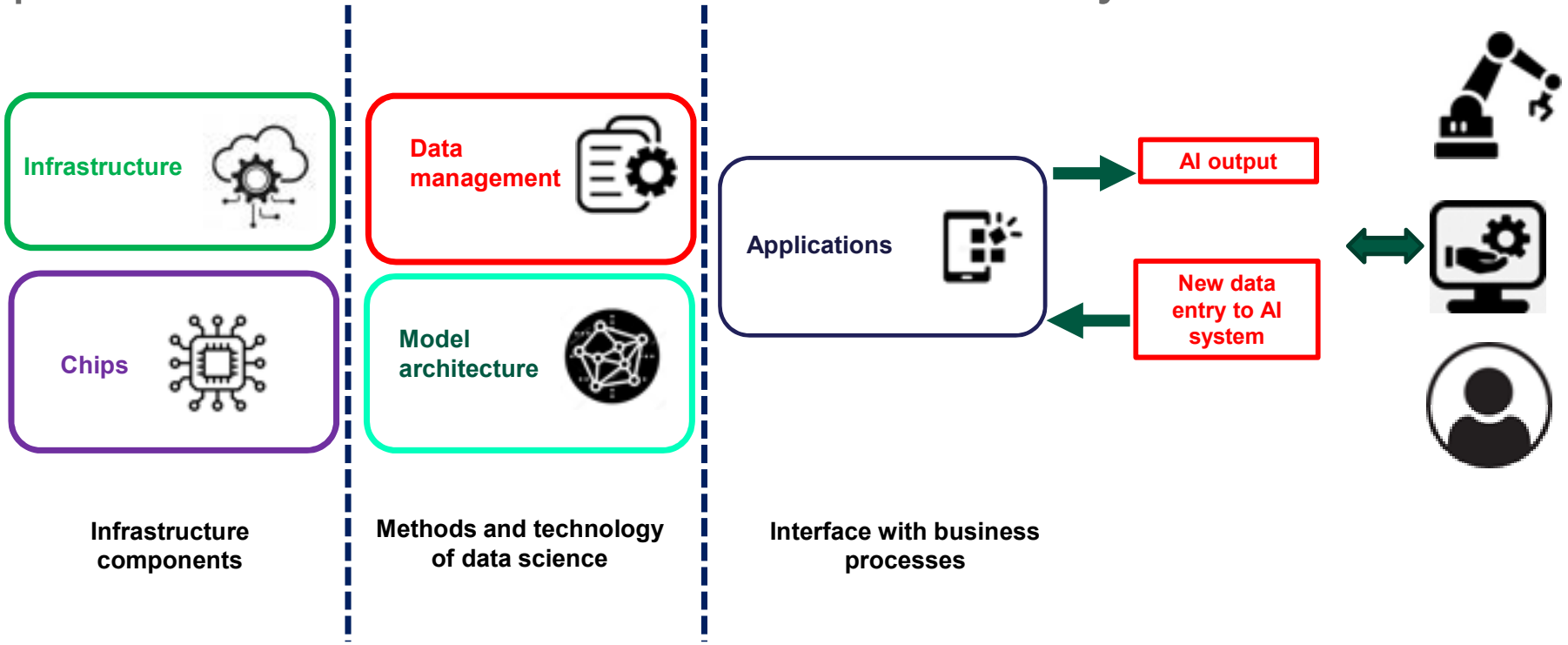
- Lesson 1: Cybersecurity is cross-functionnal, horizontal and pervasive tool
- Lesson 2: Shift from a handcrafted threat to an organized threat
- Lesson 3: Transition to a Systemic National Strategy
- Lesson 4: Reinforcement of the regulatory framework
- …

RELATIONSHIP BETWEEN AI AND CYBERSECURITY IN ENERGY SECTOR

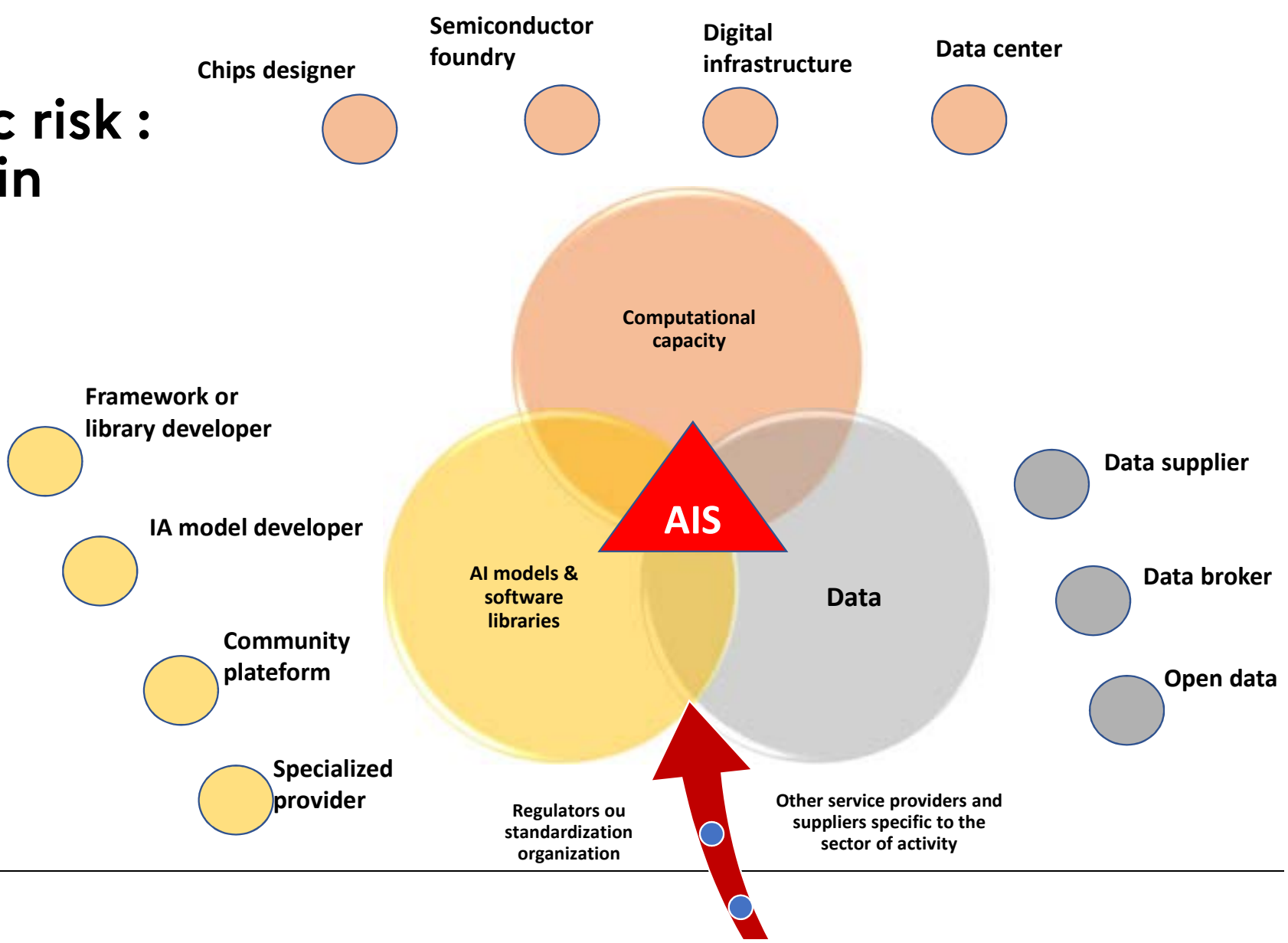
AI AND CYBERSECURITY: SIMILAR PROBLEMATICS

The AI value chain

A specific chain to be taken into consideration in risk analysis…



AI systemic risk : supply chain



Main common risk scenarios

1. Compromise of AI hosting and management infrastructure
2. Supply chain compromise
3. Lateral movement via interconnections between AI systems and other systems
4. Malfunction or malicious behavior in AI system responses
5. Human and organizational weaknesses

AI SYSTEM : FEED BACK FROM ENERGY INDUSTRIAL COMPANIES

The industrial process caracteritics

Limits of AI implementation

- **Industrial production naturals restrictions**
  - Real-time and/or 24/7 production (e.g., electricity production or grid balancing) with very long lifespans
  - No risk tolerance (e.g., nuclear industry)
  - Industrial players and authorities not yet ready

- **AI own limitations**
  - Complex and deep time learning models
  - Libraries transfer between two environments (different applications et standards : bias introduction)
  - Short life of AI models

AI Cybersecurity for industries

Addressing concerns about risks

- AI target only part of the industrial process (e.g., maintenance activity planning)
- Industries need trustworthy tools only
- Trustworthy offer of AI: data confidentiality and trust given to the supplier

AI : one acronym for many use cas

Etape 5 : Capitaliser sur tous ces constats

Lesson 1: AI is also cross-functional (not yet horizontal and pervasive)

Lesson 2: AI is polyform (differents kind ; destinations ; environment and growing way)

Lesson 3: AI is not quite ready for industries and it will need time to

Lesson 4: AI need a lot of human analysis

THANKS


AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI