ETSI Security Conference 2022

Cybersecurity Research Challenge in a digital and ultra-connected society

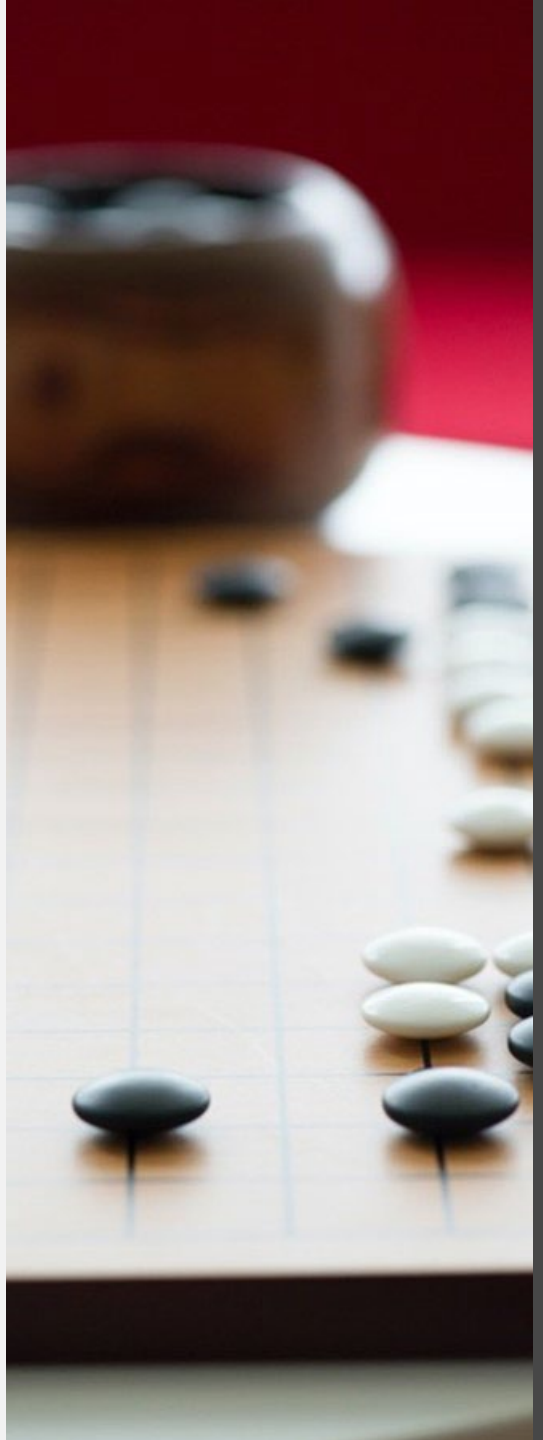
Bruno Charrat
Deputy to the Director
Technological Research Division, CEA

05/10/2022

Active involvement in Research & Innovation agendas

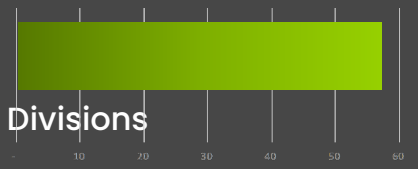
Cybersecurity as a multi-disciplinary program

Cross-cutting expertise



Who we are

Our teams combine combine scientific and operational expertise. Together they form a unique innovation force in cybersecurity.



200+ scientists
3 Operational

15 coordinated teams

Contributions range across

- Cryptology design, techniques and protocols
- Formal methods and theory of security and privacy
- Security services
- Intrusion/anomaly detection and malware mitigation
- Security in hardware
- Systems security
- Network security
- Software and application security
- Forensics

Digitalization is creating great expectations

Smart home

Smart & safe cities

Agriculture

Healthcare

Manufacturing 4.0

Smartgrids

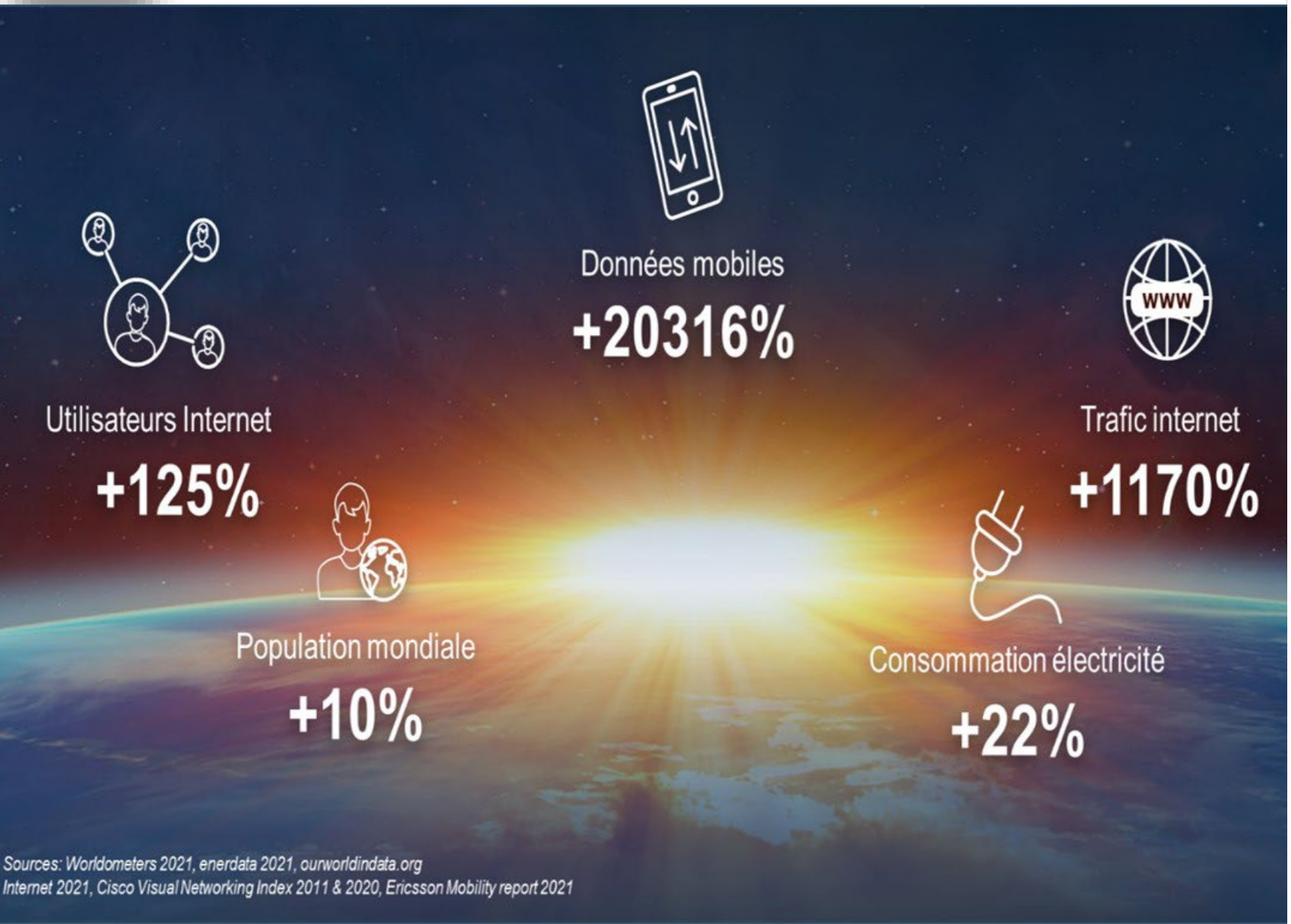
60B

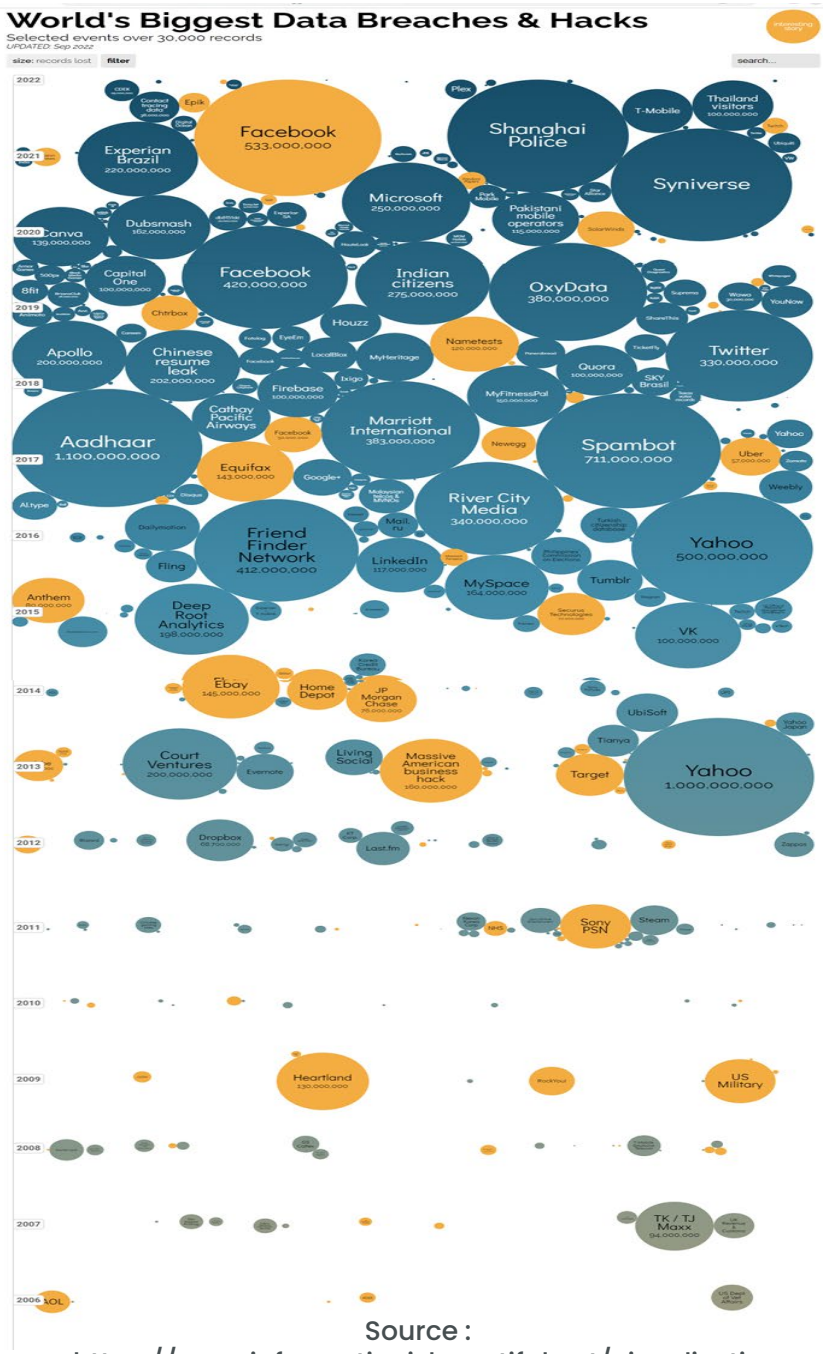
Connected objects in 2030, with strong computation power

IoT, embedded AI and new connectivity could help :

- Run factories and optimize raw materials and energy usage
- Manage decentralized and intermittent energy production
- Design new materials and new medication
- And more

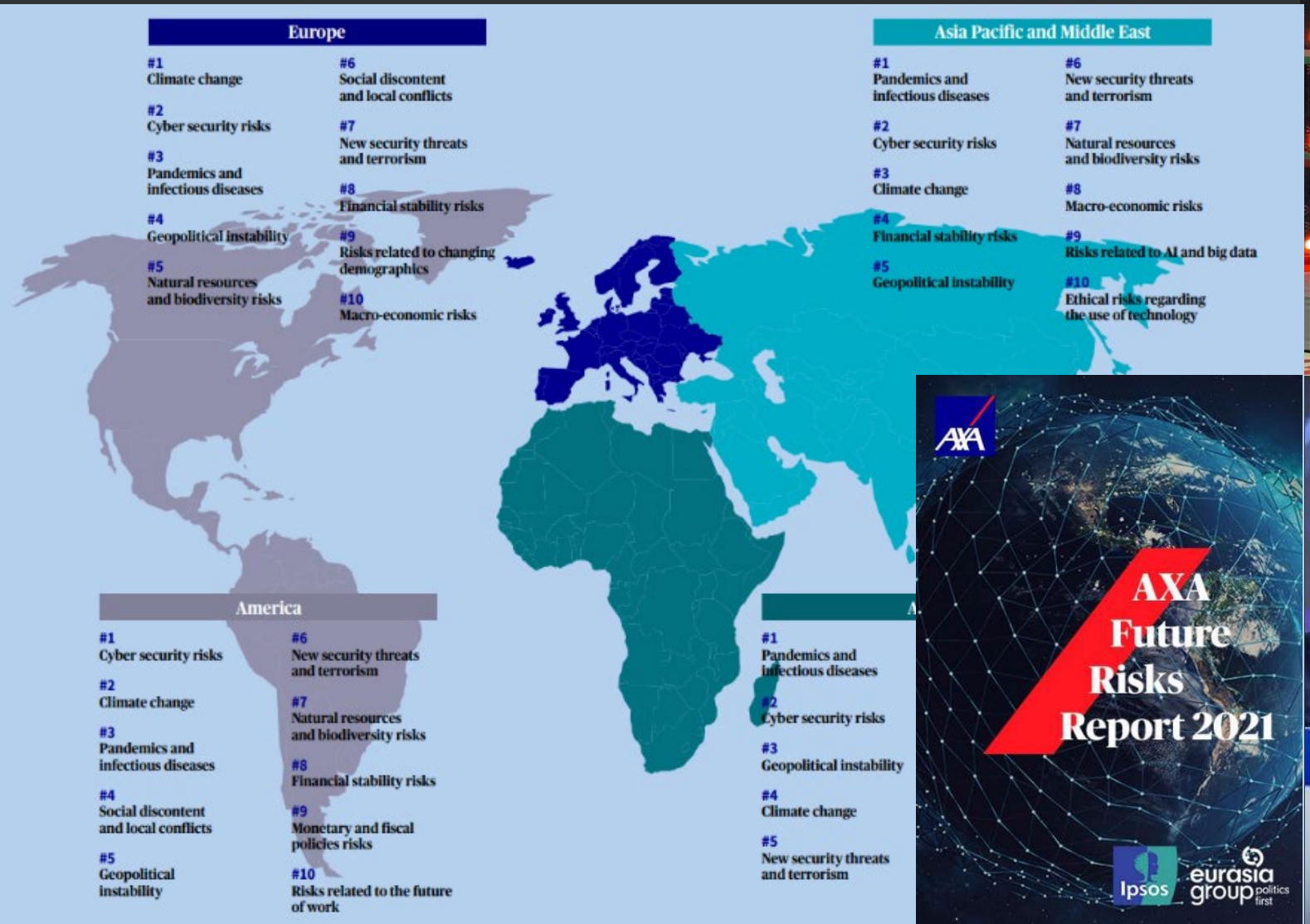
Data are the new uranium





Source : https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

A new era for cybersecurity and privacy with multiple research challenge



France Cybersecurity Acceleration Strategy

- Develop sovereign cybersecurity solutions
- Strengthen the links and synergies between actors
- Raising awareness
- Train more young people and professionals in cybersecurity professions

Priority Projects & Equipment for Research

- Budget 65Meuros (for 6 years)
- 10 first projects funded to :
  - Launch scientific challenges
  - Structure research communities
  - Achieve scientific breakthroughs
  - Develop disruptive technologies
- 7 started from July 2022, 3 under selection

Secure computations

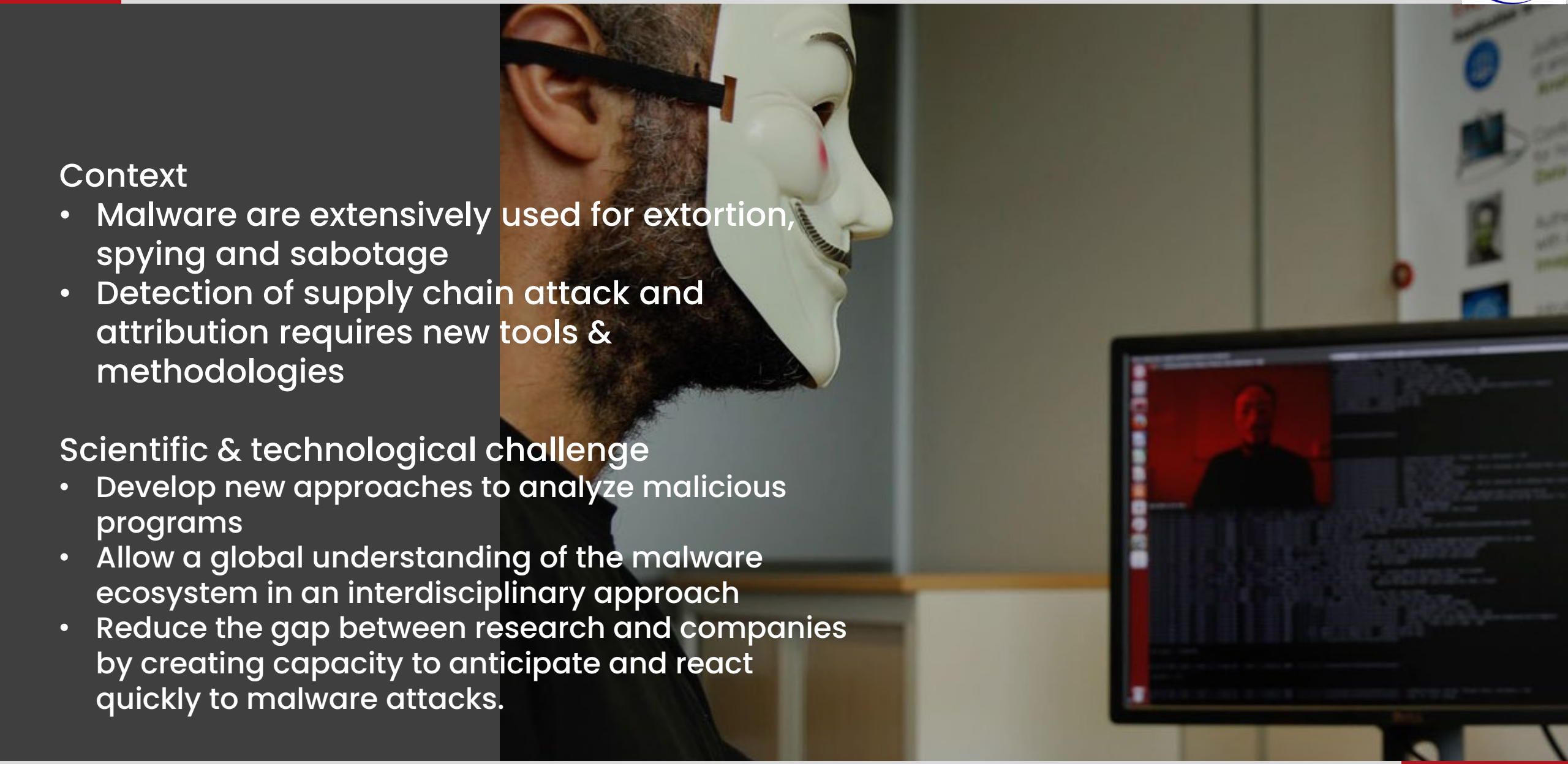
Context

- For cost reasons and the sake of simplification, data storage & processing are massively outsourced
- Leaks are exposing sensitive information, thus creating risks, both to companies and to individuals
- New tools are required

Scientific & technological challenge

- Study cryptographic mechanisms able to ensure the security of data, during their transfer, but also during processing, even in uncontrolled environments (internet, cloud)

New defense against malware



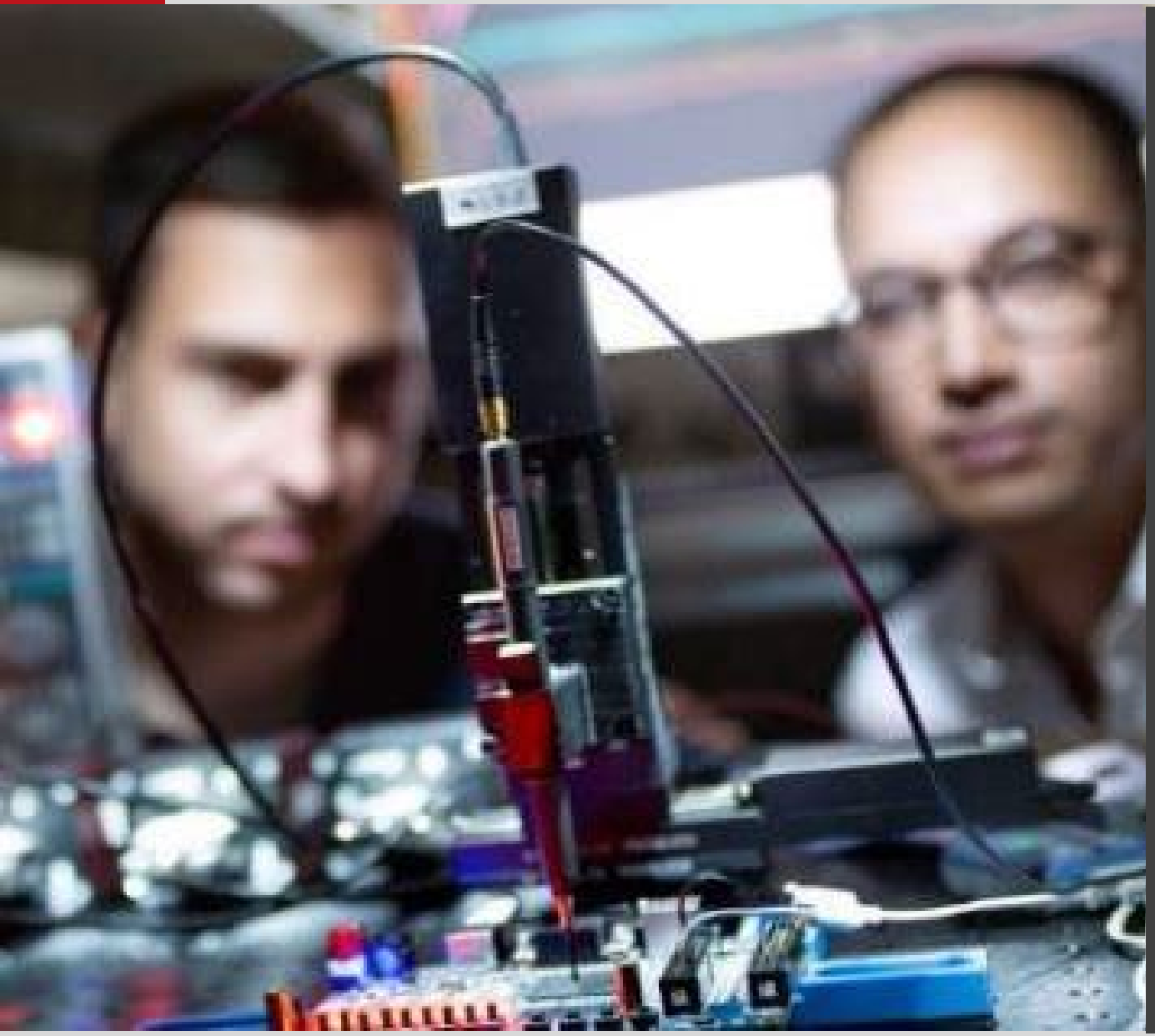
Context

- Malware are extensively used for extortion, spying and sabotage
- Detection of supply chain attack and attribution requires new tools & methodologies

Scientific & technological challenge

- Develop new approaches to analyze malicious programs
- Allow a global understanding of the malware ecosystem in an interdisciplinary approach
- Reduce the gap between research and companies by creating capacity to anticipate and react quickly to malware attacks.

Secure architectures for embedded digital systems



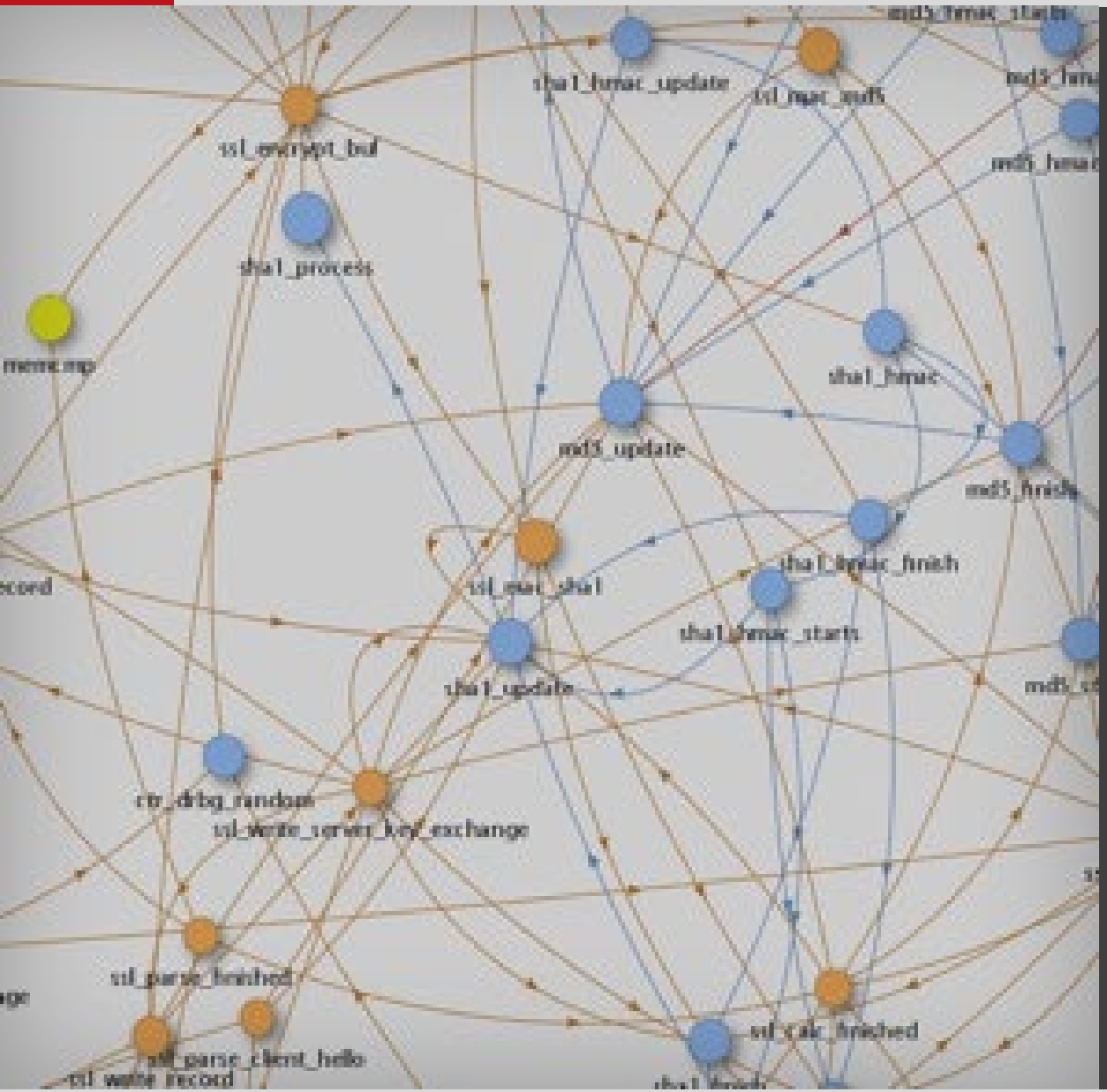
Context

- Security of components and communicating objects is of growing importance

Scientific & technological challenge

- Study and implementation of 32-bit RISC-V for low power secure circuits against physical attacks for IoT applications and 64-bit RISC-V secure circuits against micro-architectural attacks for rich applications
- Research and development of building blocks new RNG, memories, agile hardware accelerators for next generation of cryptography.

Improving Digital Systems Security Evaluation



Context

- Compliance and vulnerability analyses are key to provide recognized cybersecurity assurances
- Drastic increase in the complexity of attacks and systems to be assessed
- Support experts with new tools and techniques

Scientific & technological challenge

- New code analysis techniques to adapt to the objectives of security assessments and to scale up to complex systems
- New research methodologies and tools to provide proof of compliance of software systems, including when they evolve in response to a vulnerability testing campaign

Security Orchestration, Automation and Response

Context

- Supervision of information systems is critical for cyber-resilience
- Increase in the number and capacity of each components makes security supervision more complex.

Scientific & technological challenge

- Significantly improve the efficiency of the detection-reaction chain (response and remediation).
- Scientific work will lead to prototypes and demonstrators that will be deployed on platforms built within the project.

Thanks for your attention

Contact

- mail bruno.charrat@cea.fr
- telephone +33 6 76 48 64 25