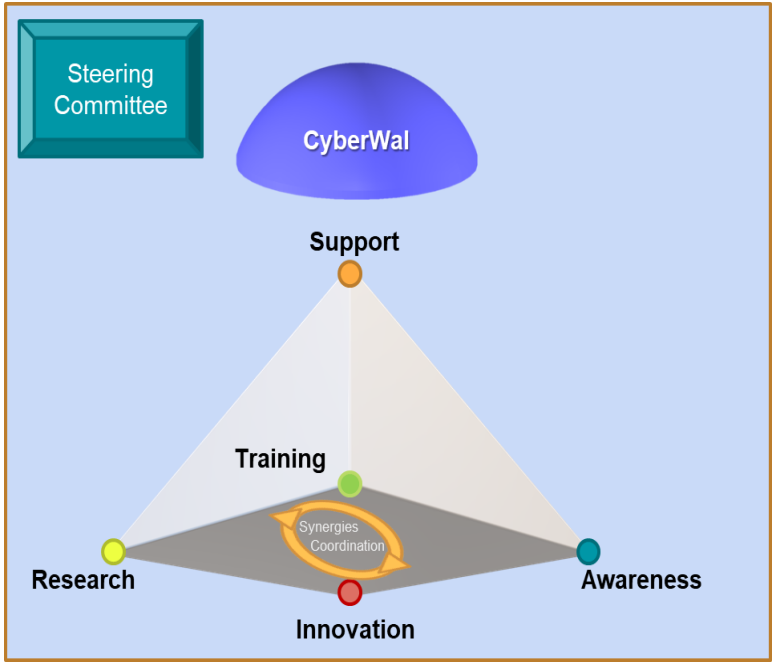
CyberWal as a Nato test center

Axel Legay

Agenda

- The Origins of CyberWal and who we are
- Description of research activities
- CyberWal as a Nato Test Center

CyberWal: The Cybersecurity initiative in Wallonia



- A space where the actors meet to:
  - Respond to challenges of Walloon and Belgian socio-economic actors
  - Position Wallonia in Europe and in the rest of the world.
- More than 100 actors
- Works with Demonstrators and a factory

The actors who make up CyberWal (direct/indirect)

- The “agence du numérique”
- All the actors of the Walloon academic world active in the field
- The entire training sector
- Federations and clusters: More than 50 companies
- Strong collaborations with militaries, secrete services, federal police
- Strong collaborations with societal actors and public services (hospital, ...)

CyberWal is an “initiative d’innovation stratégique” as per defined by the EU

The research before CyberWal

History:

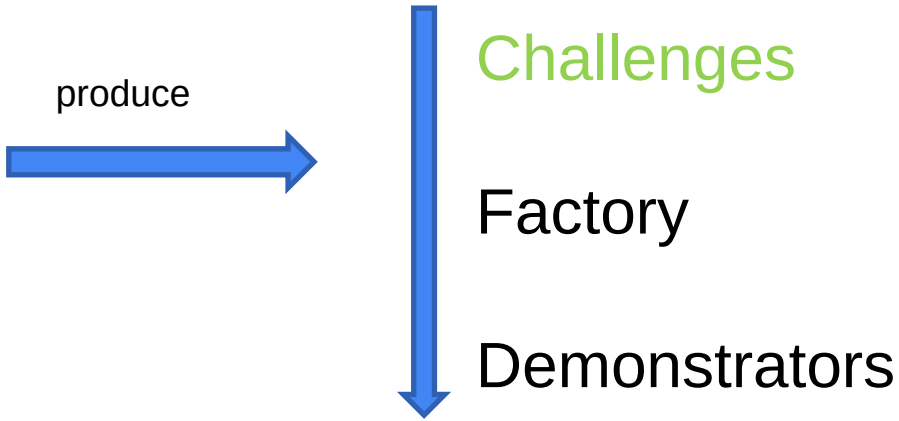
- Cyber security at design
- Cryptography
- Certification scheme and risk analysis processes
- Malware analysis
- Data protection (RGPD) – cloud and access control
- …
- And new hot topics

Examples of disruptive research we are working on

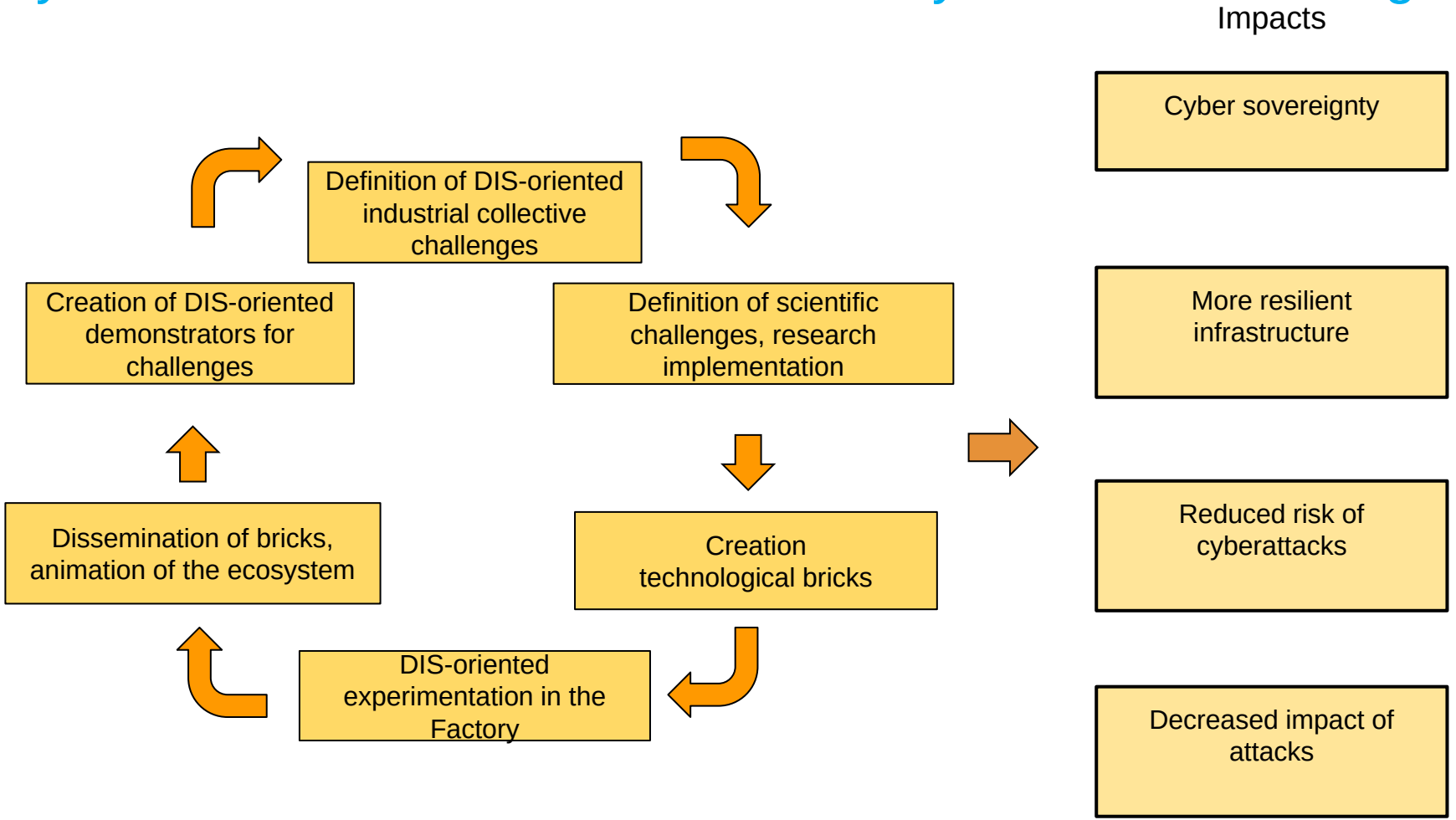
- How to detect malwares and virus with IA techniques (including federated learning)
- How to add IA engine to improve cyber range training and research
- Definition of new quantum computing algorithms (and demonstrators)
- New and automatize access control policies
- Hardware attacks
- …

How does CyberWal work?

- Steering Committee + Committees per topics
- Many networking events
- Research events/projects
- Cross disciplinar events (meet actors in need)



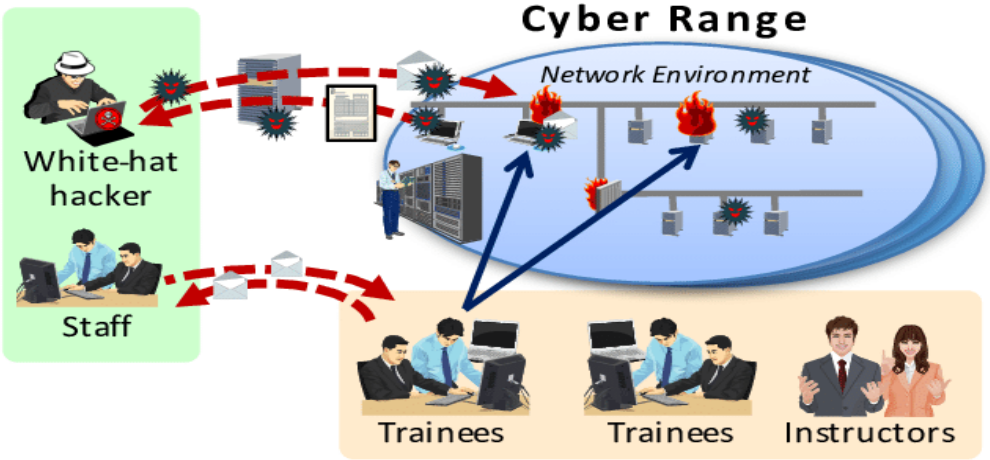
CyberWal: a method based on industry/research challenges



Factory and demonstrators

- A factory is a place where demonstrators and human compences are made available
- With security guarantees and a business model
- Very similar to the french « cyber defense factory »
- Examples (in construction):
  - Data available for training
  - Tools for malware analysis
  - Access to cyber range scenarios
  - Access to quantum demonstrator
  - Access to human ressources (risk analysis, GDPR, …)

(Some) Demonstrators



Pre-selection of Collective Industrial Challenges

2

1, 4, 7

10, 11

Applied R&D Theme	Collective industrial challenge	Sectors
1. Cybersecurity verification of systems	**Automation of cybersecurity vertification of CPS (Cyber Physical Systems)**.	Transport, other sectors
2. Risk management	**Risk management and penetration testing**	Transport
4 Software and hardware security engineering	**Cybersecurity by design for industry 4.0 and space systems**	Industry 4.0, Space
7. Network Security	**Cybersecurity by design configuration for data transmission**	Space, Industry 4.0
10. Intrusion detection	**Anomaly detection in energy networks**	Energy (critical infrastructure)
11. Intrusion detection	**AI based intrusion detection for industrial systems**	Industry 4.0

Conception

1, 2, 4, 7

Operation, maintenance

10, 11

Training: action plan

The training actors have identified challenges/areas

- Area 0 : Encourage vocations
- Area 1 : forgotten talents (graduates or non-graduates)
- Area 2 : Skills development/Upskilling/Reskilling
- Area 3 : State-of-the-art training for and by experts.

CyberWal for Nato

UMONS
Université de Mons

cetic
Your Connection to ICT Research

UCLouvain

RMA
Brussels
Royal Military Academy

sirris
driving industry by technology

UNIVERSITÉ
DE NAMUR

Multitel
INNOVATION CENTRE

Expertise of Universities

- UCLouvain: Risk analysis, Security engineering, Cybersecurity testing and penetration testing, Vulnerability analysis (including hardware simulation), Cyber range (including scenario design), Malware analysis, AI based security solutions, Secure federated learning, Data anonymisation and pseudonymisation techniques, cryptography (pre and post quantum).

- UNamur: Verification and validation, research is conducted on model checking, system analysis using, formal methods (process algebra), and software testing (fuzzing, combinatorial interaction testing), NIS, GDPR.

- UMONS: Design and simulation of network protocols, wireless sensor networks, development and emulation of embedded firmware, Physical layer monitoring Physical layer simulation, Optical fiber technology (telecom and sensing).

- RMA: Cyber ranges, training, cyber situation awareness, testing, certification and accreditation, intrusion detection, social driven vulnerabilities assessments.

Expertise of CRA

- CETIC: Risk analysis, Security engineering, DevSecOps, Cybersecurity testing and penetration testing, Vulnerability analysis, Cyber range, Certification preparation, AI based security solutions, Secure federated learning and privacy preserving IA, Data anonymisation and pseudonymisation techniques.

- SIRRIS: Connectivity of manufacturing systems and digitization of manufacturing, cybersecure digital services and cybersecurity for manufacturing, Universities to SME cybersecurity transfer and animation.

- Multitel: Cybersecurity for the railway system, 5G, Quantum cryptography and infrastructure design, blockchain design and validation.

Contacts

- Axel Legay: axel.legay@uclouvain.be
- Theo Vaessen: theo.vaessen@uclouvain.be


That's all Folks!