



# CyberWal

digital  
wallonia  
.be

June 2022

Axel Legay



# CyberWal: a space open to everyone

- A space where actors in research, innovation and training meet to :
  - Respond to the **needs and challenges** of **socio-economic actors in Wallonia and Belgium**
  - Position **Wallonia in Europe**.
- Throughout the Walloon territory :
  - **Support** the creation of the **focal point** in Galaxia, and also
  - A6K, the digital military district, Tournai, Liège, ...

**More than 100 actors, a true cybersecurity ecosystem.**

# Cybersecurity: Subjective Opinions

Cybersecurity is seen as a cost:

- We will never be attacked,
- It does not increase the market share of the company.

## Facts :

- Any company that has been attacked has lost more money than if it had invested in protections,
- Any company that has computer equipment is susceptible to attack,
- The indirect cost of attacks is substantial,
- New directives will impose it.

Cybersecurity, if perceived as trustworthy, makes money for the business.

# Cybersecurity = topic of the moment in Europe



War in Ukraine, Pandemic (remote working, ...), digitalization and industry 4.0, ...

- Arrival of the NIS (and soon NIS2) and GDPR directives (constraints), and the “European center of expertise in cybersecurity” (coordination of investments in research and infrastructure, community) and “Cyber Act” (certification) regulations
- Reinforcement of ENISA, the European Space Agency’s Cybersecurity Center
- Structuring of research and innovation in Europe through competence centers

# State reaction?

- **France : In 2020:** 1 billion euros in the new cyber strategy, ample room for research and strong commitment from research organizations and universities (65,000,000 in addition to hundreds of millions already invested)
- **Flanders:** 20 million per year (research/innovation/training) (structural)
- **Federal State:** CCB, CERT, digital military districts, ...



How was the situation in Wallonia at the end of 2019?



# Ongoing discussions with the industry

Walloon companies have **major** cybersecurity needs:

- “Help us find new talents!”
- “Help us train our staff!”
- “Help us secure our products and meet standards”!
- ...

# Situation from a talent search/creation perspective

Universities have never hired so many (10 professors at least), but:

- Difficulties in optimizing collaboration
- Lack of positioning in relation to concrete challenges from the socio-economic fabric
- Bad positioning in Europe, “unknown” groups.

## Other observations

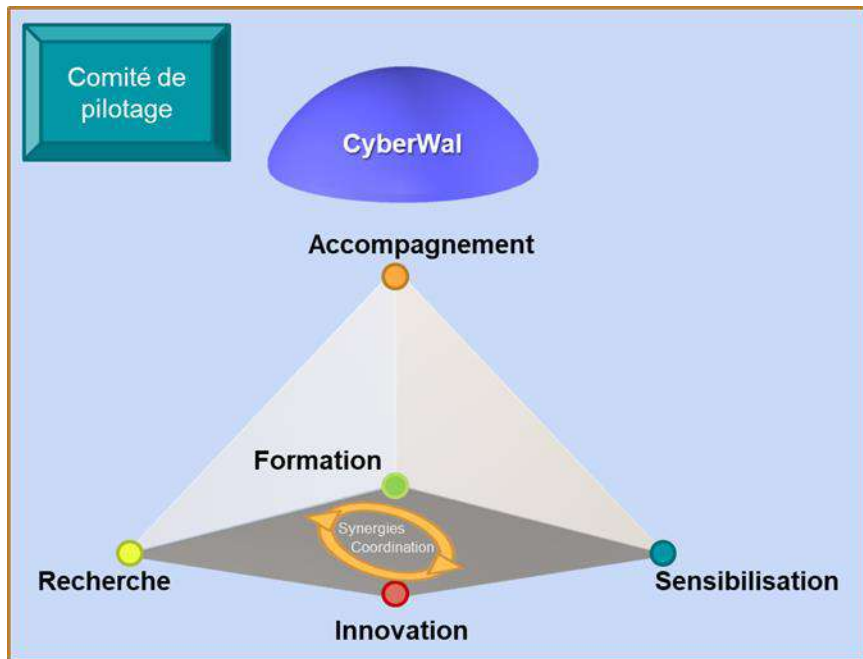
- Some companies do not feel concerned
- Citizens feel neglected
- The authorities and public sectors are little aware of/supported
- It is necessary to link the problems and the people capable of responding to them

Our answer: CyberWal, an “IIS”



# Cyberwal: Unite « cyberwalloon » forces

Regional strategy Digital Wallonia for Cyber



- **Research:** conduct challenge-based, applied research
  - TRL2-4: CyberExcellence
  - TRL3-7: FEDER
- **Innovation:** Creation of startups/values
  - Réseau Lieu,
  - DIANA, cyber defense factory
- **Training:** 4 pillars, Briefcase (PRW)
- **Sensitization:** Virtual/in person Coaching

# Relation DW4Cyber & CyberWal



- CyberWal is the union of research and innovation actors
- CyberWal also includes training because it is inseparable from research and innovation.
- CyberWal raises awareness among public actors
- CyberWal and the « agence du numérique » work hand in hand.

# A huge impact on DIGITAL DIS

DIS	DIS Aire(s) stratégique(s) visée(s)
DIS Innovations for stronger health	<ul style="list-style-type: none"><li>•Connected patient, e-health, “big data”</li><li>•Hospital of the future, prevention and new organization</li></ul>
DIS Innovations for agile and safe production and design methods	<ul style="list-style-type: none"><li>•Digital technologies and innovative solutions in terms of advanced production and design methods, in line with the needs of the productive fabric.</li><li>•Implementation of innovation through the technological and digital transformation of value chains within the productive fabric</li></ul>
DIS Sustainable energy systems and housing	<ul style="list-style-type: none"><li>•Digitization and flow management</li></ul>

# The actors that make up the IIS

- All the actors in the Walloon **academic** world that are active in the field
- All the **training** sector
- **Federations/interco** (Cyber coalition, AGORIA, UWE, IDLUX, A6K, ...)
- Competitiveness **clusters** (Skywin, Mecatech, ...)
- **Societal** actors dans public services (AVIQ, Test achat, ...)
- **Government:** actors (AdN, CCB)

# Companies and CyberWal



- Companies through federations/clusters
- Discussions with at least one to two new companies each week
- Companies play a key role in identifying challenges
- All companies are welcome, but we don't want to bother them with legal matters.

## “In progress”

- Get closer to the General Staff of the armies
- Get closer to state security service (capital for training)
- First success: first training by Mr. Pascal Petry given on March 17
- Second success: rapprochement with the General Staff of the armies and common vision for the district of the future.

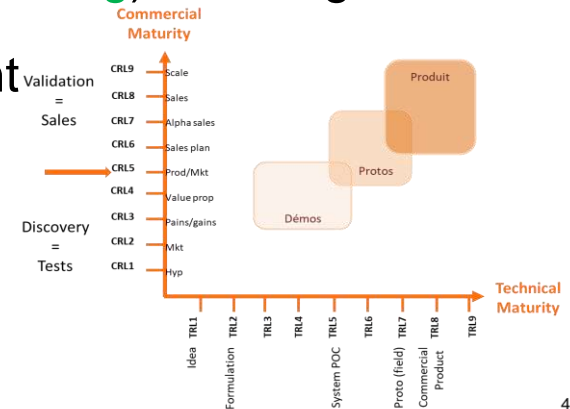
# The role of a transverse IIS in the DIS of the S3

- Cybersecurity is transversal to all DIS
- CyberWal has its own activities (health, industry 4.0, energy communities, 5G, ...), et
- CyberWal will also serve other IIS
- **Example of collaboration:** MEDC are working on a medical demonstrator. CyberWal protects the demonstrator's data.

# A challenge-based approach



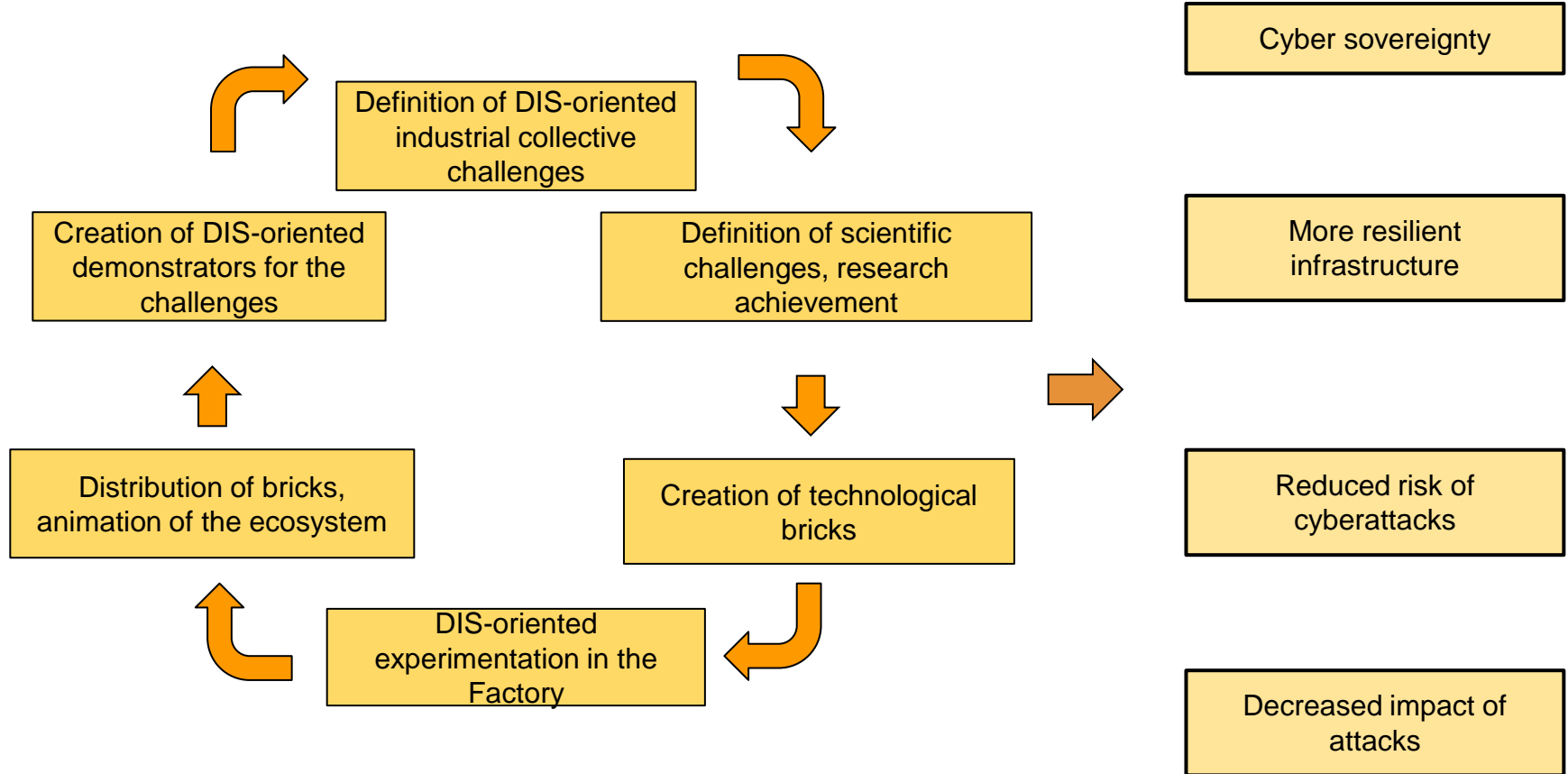
- Consult socio-economic actors to identify challenges
  - In research and innovation
  - In training
- Ensure actors are aligned on these (emerging/existing) challenges
- Make sure the « customer » is taken into account
- Cover the entire value chain.





# Collection of challenges (research/innovation)

Impact



# Examples of scientific challenges (candidates + factory bricks)

CPSET - Cyber Physical System in Energy conversion & Transport



Roadmap CPSET: Generic Tech Brick - Cybersecurity test bench



CyberWal

Collective industrial challenge

CPS (Cyber Physical Systems) cyber verification automation

**Scientific challenges**

**Technology brick**

Automation of cybersecurity functional tests

CyberSecurity Test Builder

Automation of tests

Penetration test generator.

# A firsts success: CYBEREXCELLENCE



- Concretizes the TRL2-4 research component of CyberWal
- Links the 5 French speaking universities and the 2 research centers active in the field
- 52 researchers/year over 6 years, 19 million for the first 4 years

“Striking force equivalent to that of LIST or Brittany’s cyber cluster”

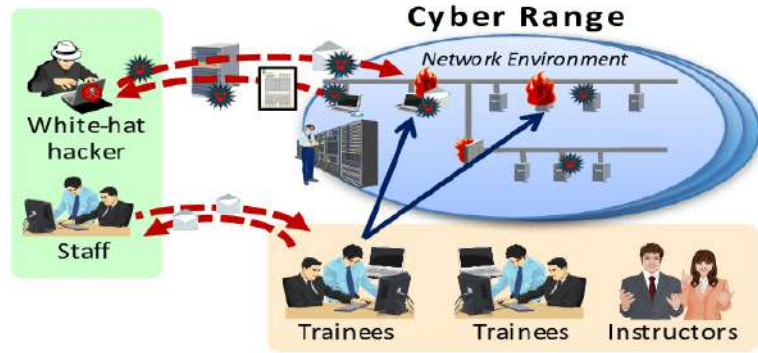
## A second success: Participation in Diana (NATO)

- Powered by WSL
- Software/hardware brick demonstrators
- Dissemination of results beyond Europe
- Sacred union with TRAIL (artificial intelligence)



*For techno-entrepreneurs.*

# Support demonstrators/initiatives (PRW, ...)



# 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.

# The cyber briefcase: a unifying training objective

- A unified training catalog
- Unified media
- Continuous and mobile training
- **Bases = (free):** Available to all and fed by all
- A catalog of advanced training courses **unified by sector (AGORIA, SOWALFIN)**



# Visibility and citizenship action plan



- Discussions with public authorities (cities, municipalities, region, etc.)
- Discussions with public actors (AVIQ, hospitals, energy sector, etc.)
- Discussion with citizens in the form of forums and conference debates
- Available to experts
- Stimulate the actors who should not hesitate to make contact (Thanks to the AdN)



# Operating mode



- General assemblies
- Target groups (research, innovation, etc.) depending on the projects
- Identification of challenges and companies concerned
- Public events (conferences, awareness raising, A6K, Redu, etc.)
- Doctoral schools and information sharing on (set-up of) projects
- A very strong interaction with DW4Cyber, CCB, Cyber coalition, ...
- A necessary interaction with several IIS.

# Coming soon ... “we need to talk”



- CyberWal and UWE to raise awareness/train/innovate
- CyberWal and Agoria using the techniques from CyberExcellence
- CyberWal and the cyber coalition for national outreach (need your answer)
- CyberWal and IA for Belgium for transversality with AI
- CyberWal and les hubs
- CyberWal et l'ESA.
- A monthly technical talk (via CyberExcellence).

# Impact on Research in Europe

- Engagement of a Project Liaison Officer (in conjunction with AWEX, NCP, WBI, etc.)
- Positioning effect: working on clearly identified and numerous needs
- Increased visibility of Wallonia and participation in more prestigious consortia

# Impact on sustainable development

" Sustainable development is development that meets the needs of the present without compromising the ability of future generations to meet theirs. "

Sustainable development is based in particular on 2 pillars: social and environmental

- Social: job creation (including retraining) and ethics
- Environmental : protect critical infrastructure (dams, power plants, etc.)

# Conclusion



- Cybersecurity actors have united
- Cybersecurity actors are aligned with regional/federal/European policy.
- The actors are ready to work together and for all

We are waiting for you!

# Some key figures



2 entreprises sur 3 ont été victimes de la cybercriminalité à plus de deux reprises\*.  
2 out of 3 companies have been victims of cybercriminality more than twice\*

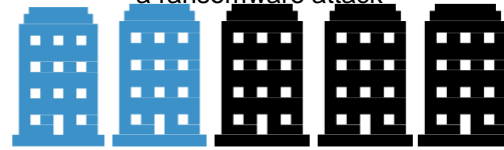


2 PME sur 5 ont été victimes d'une cyber-attaque\*\*\*.  
2 out of 5 SMEs have been victims of a cyber-attack\*\*\*



1 entreprise sur 5 a été victime d'une attaque par ransomware \*\*

1 in 5 companies have been the victim of a ransomware attack \*\*



2 entreprises belges sur 5 ont été victimes d'une cybercriminalité\*.  
2 out of 5 Belgian companies were victims of cybercrime\*

\*Source: Hiscox Cyber Readiness Report 2021

\*\*Source: Mastercard Report

\*\*\*Source: Proximus Cyber Security Survey

# Threats are evolving and intensifying



- 2 out of 3 malware stays under the radar of traditional anti-malware
- + 60 % of attacks are not related to malware
- Increase in the exploitation of critical "0-day" and widespread vulnerabilities : Log4shell, ..
- The geopolitical situation is increasing cyber threat levels globally

## Exorbitant costs

La cybercriminalité se fait plus menaçante et a coûté plus de 6000 milliards de dollars (5.700 milliards d'euros) au monde l'an dernier, a assuré mardi Alessandro Profumo, patron du géant italien de l'aéronautique et de la défense Leonardo. *«Les nouvelles menaces dans le domaine de la cybersécurité au cours des deux dernières années ont été des “dommages collatéraux” de l'épidémie de Covid-19 et de l'accélération de la numérisation que celle-ci a entraînée»*, a déclaré Alessandro Profumo en ouvrant à Rome Cybertech Europe 2022, un congrès d'experts se déroulant sur fond de guerre en Ukraine.

- Les problèmes de cybersécurité ont par ailleurs été exacerbés par la guerre en Ukraine. *«Nous avons noté une pression accrue»* depuis le début de la guerre, a déclaré en avril Alessandro Profumo, dont le groupe possède une branche spécialisée consacrée à la cybersécurité.



# Current status and relationship between partners

- A MoU is signed by all research actors + training and socio-economic actors
- Multiple meetings and contacts (for two years) to collect the challenges of the socio-economic fabric, share common objectives, synchronize.
- Identification of research/training needs that align with these challenges, with the challenges identified in Europe and with S3.
- Huge awareness of industrial and societal actors (principle of perpetual collection).

# Objectives: Reduce the risk and impact of an attack

- **Raise awareness** in order to anticipate threats
- **Train** talents and develop them
- **Create** a structured research/innovation ecosystem
- **Promote** the transfer of skills and support companies
- **Protect** regional and state structures.

For a visible Wallonia on the territory and internationally

# The challenges: An action plan for research and innovation

- CyberWal will impact and strengthen the socio-economic fabric
- CyberWal will work on both:
  - emerging challenges
  - existing challenges on which we can bring added value
- In research/innovation and training..

# The actors to take up the challenges

- The traditional: universities, CRA, ADN.
- The “less traditional” (on a research level): Agoria, info pole, UWE,WBI, A6K, IDLUX, ....
- WSL to accompany us.

# A huge impact on DIGITAL DIS

DIS	DIS Aire(s) stratégique(s) visée(s)
DIS Innovations for stronger health	<ul style="list-style-type: none"><li>•Connected patient, e-health, “big data”</li><li>•Hospital of the future, prevention and new organization</li></ul>
DIS Innovations for agile and safe production and design methods	<ul style="list-style-type: none"><li>•Digital technologies and innovative solutions in terms of advanced production and design methods, in line with the needs of the productive fabric.</li><li>•Implementation of innovation through the technological and digital transformation of value chains within the productive fabric</li></ul>
DIS Sustainable energy systems and housing	<ul style="list-style-type: none"><li>•Digitization and flow management</li></ul>

# Impact of attacks on businesses (2019)

- In 2019, the average Belgian company lost €54,700 (direct costs, median amount) due to cybercrimes.
  - ⇒ This can go up to 13 million and it affects more and more the public world (diversity).
- The median cost is higher than the median cost of Western nations (€54,700 vs €52,000).
  - ⇒ In view of its sensitive infrastructures (NATO Shape and Evere, European Commission, European Council, etc.), Belgium is a target of choice (the indirect impacts are substantial).

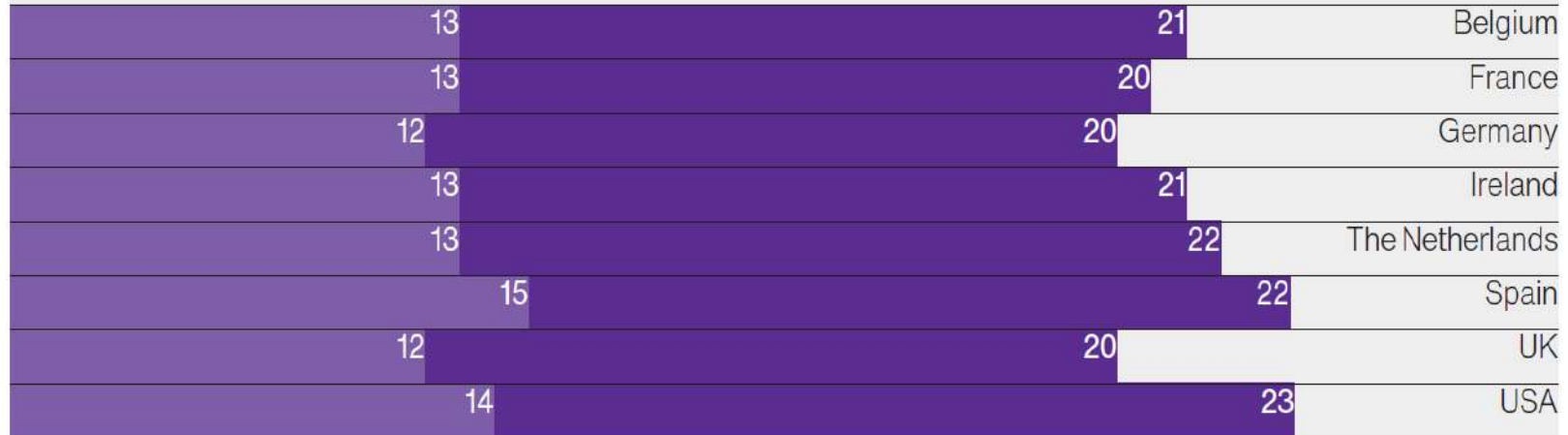
# An impact on small businesses

- Cyber Readiness Report (2019): 12 % 12% of companies targeted more than 500 times
- 20 of the 61 "super targets » are micro-entreprises (1-9 employees)

## Good news: Jobs evolve just as quickly

Cyber security as percentage of IT spend  
(%)

■ 2020 ■ 2021





# Beyond DIS



CyberWal will accompany :

- The Belgian Army and the SGRS
- The State Security Service to give it the visibility it deserves with stakeholders
- The center for cybersecurity in its activities to raise awareness and structure Belgian research
- The Federal level associations : IA for Belgium, Cybersecurity coalition, ...
- ... anyone who asks

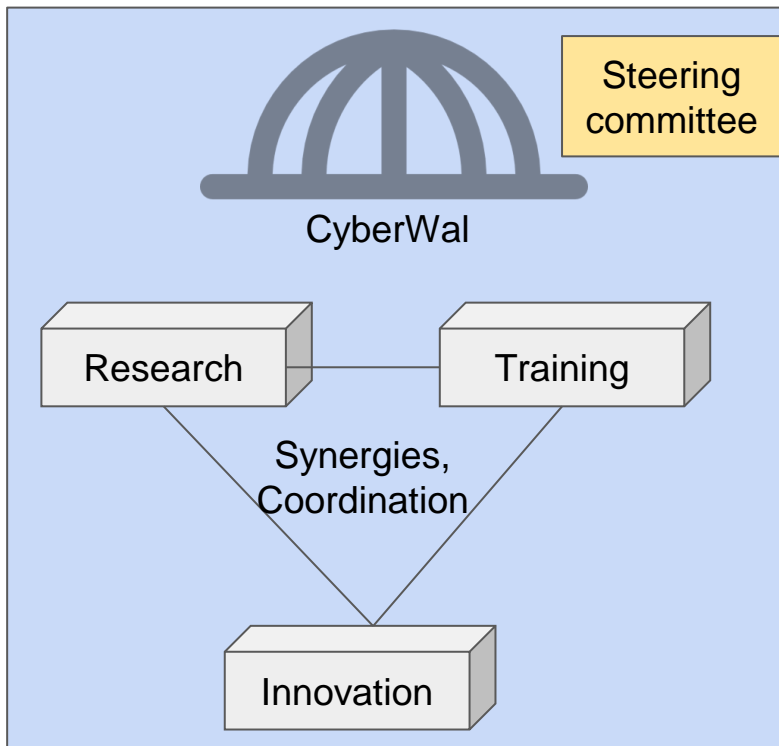
# The cyber briefcase: a unifying training objective

- A catalog of unified **advanced training by sector**
- Unified Media
- Continuous and mobile training
- CTF and Cyber Range scenarios
- **CyberWar support (AGORIA-SIRRIS)**



# Cyberwal: Unite « cyberwalloon » forces

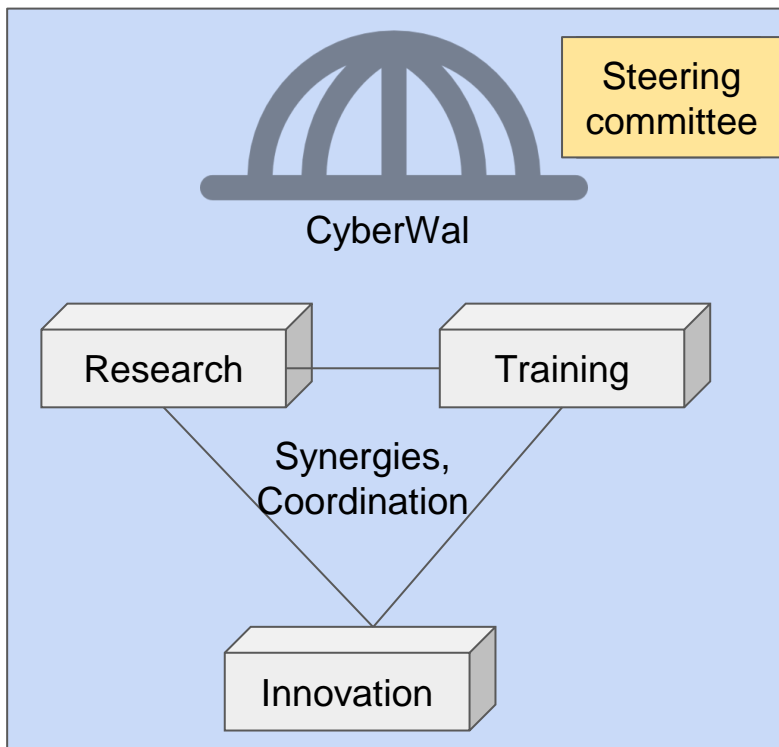
Regional Strategy Digital Wallonia for Cyber



- Identify the needs of our companies and those of Europe
- Conduct applied research whose purpose is to achieve high TRLs (innovation)
- Align with S3 DIS
- First Successes: CyberExcellence, Diana, PRW
- Potential second success: The FEDER

# Cyberwal: Unite « cyberwalloon » forces

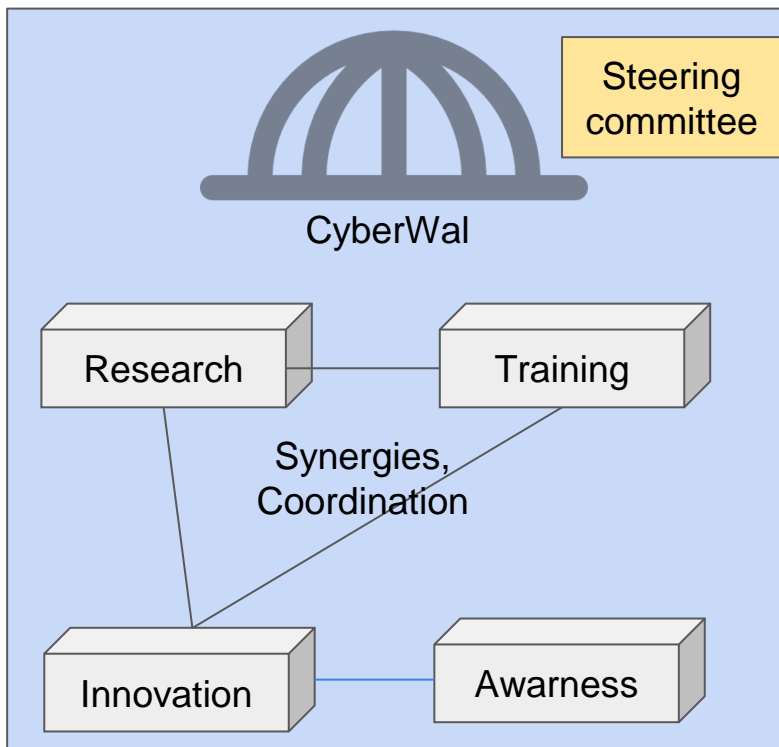
## Regional Strategy Digital Wallonia for Cyber



- Gathers all the actors of the training in 4 pillars
- A briefcase for pooling training needs and materials
- Coordinates with public and societal actors (AVIQ, Test-Achat, ...)
- First success: the PRW of Minister Borsus

# Cyberwal: Unite « cyberwalloon » forces(en cours d'écriture slide à modifier!)

## Regional Strategy Digital Wallonia for Cyber



1. **Motiver et inspirer** : atteindre les entreprises qui sont encore dans des phases « *inconsciente* »
2. **Apprendre des connaissances et des compétences** : chaque action de sensibilisation, chaque courriel, chaque vidéo, ...
3. **Activer : encourager à transformer les compétences acquises en actions concrètes** : considérer la Cybersécurité comme une priorité
4. Offrir des **conseils de première ligne** sous la forme d'une « Foire aux questions »

**CyberWar la nouvelle ambition Fédérale  
d'Agoria/SIRRIS pour l'awarness**

## Competitive objective (regional scale)

- In Brittany, there are 8,000 jobs related to cybersecurity. The Ministry of the Armed Forces aims to create 1,800 additional positions by 2025
- There was almost nothing 7 years ago.....
- And the universities were not in working order.

# Competitive objective (regional scale)

Long-lasting and job-providing structures:

- **Cyber Center of Excellence:** known to the actors of the socio-economic fabric
- **Cyber defense factory:** startups to respond to concrete problems of the army