Chaire Cyber-résilience des infrastructures numériques face aux menaces de sécurité

BORDEAUX INP

université de BORDEAUX

FONDATION BORDEAUX UNIVERSITÉ
S'engager pour l'avenir

Advens CYBERSECURITY

BEWARE CYBERLABS

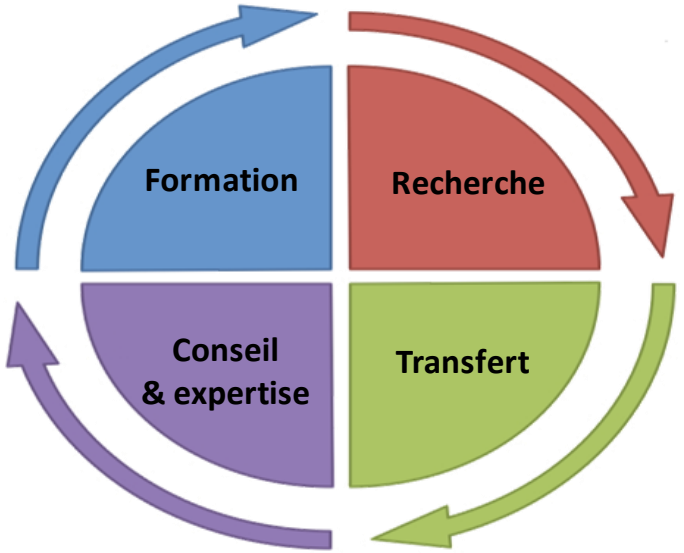
CATIE

SYNACKTIV

TEHTRIS
FACE THE UNPREDICTABLE

Chaire Cyber Résilience

- Construire et structurer
- Regrouper les efforts et les moyens



Développer l'offre de formation

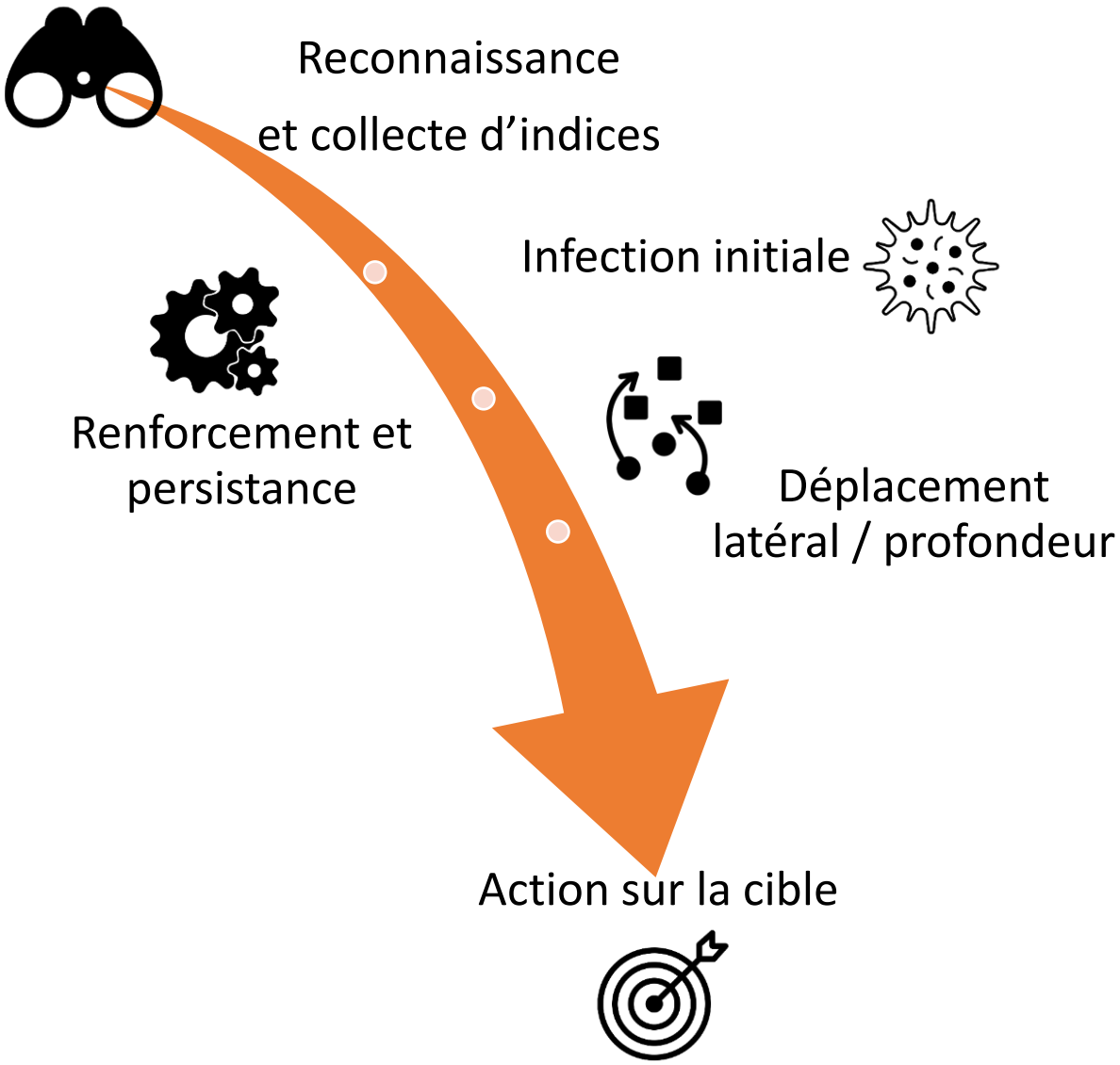
Déficit d'experts cybersécurité :

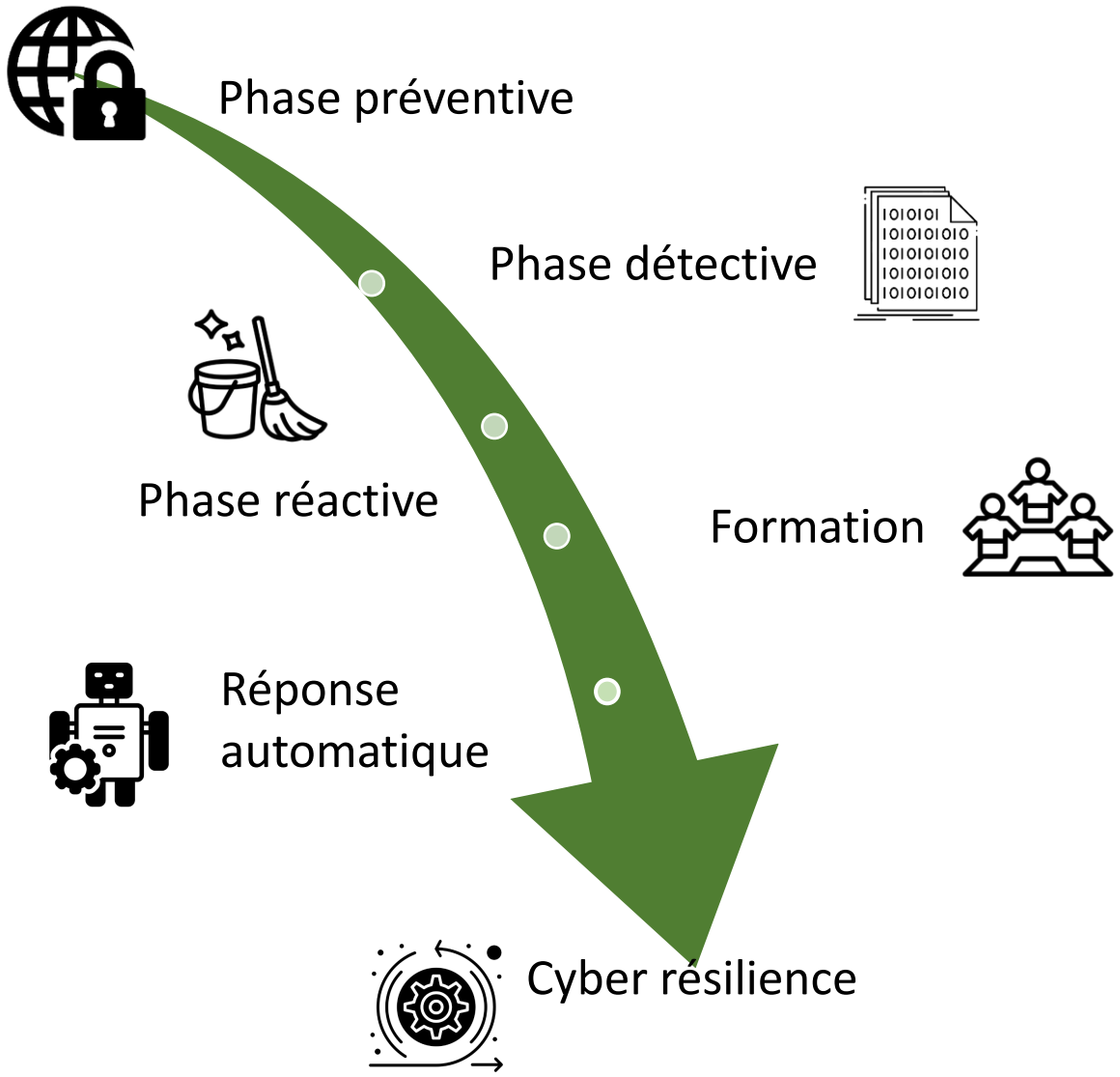
- Domaine très technique
- Cursus de formation trop longs
- Panorama des métiers très riche et varié

ECIN - « Expert Cybersécurité des Infrastructures Numériques »

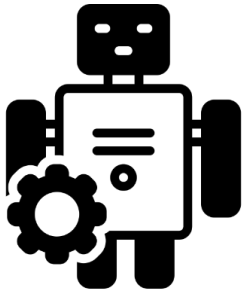
- **UE1 : Gouvernance, gestion des risques et conformité**
  - Module 1 : Ecosystème français et européen de la cybersécurité (3j)
  - Module 2 : Gouvernance, gestion des risques et conformité (3j)
- **UE2 : Audit de sécurité technique**
  - Module 3 : Intrusion sur les applications Web (3j)
  - Module 4 : Intrusion sur les systèmes Linux (3j)
  - Module 5 : Intrusion sur les systèmes Windows (3j)
- **UE3 : Entrainement de cybersécurité**
  - Module 6 : Entrainement technique – CTF (1,5j)
  - Module 7 : Entrainement organisationnel – Gestion de crise (1,5j)

Atteindre la cyber résilience

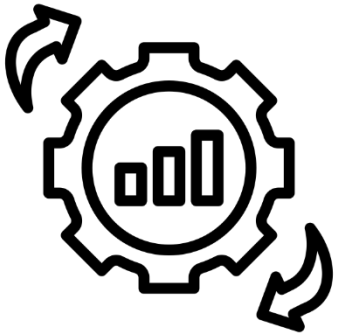




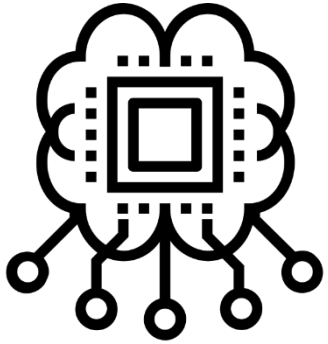
Les dimensions de la cyber résilience



Autonomie

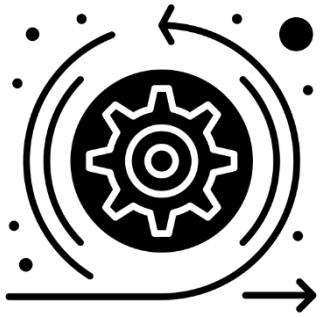


Adaptabilité et Elasticité

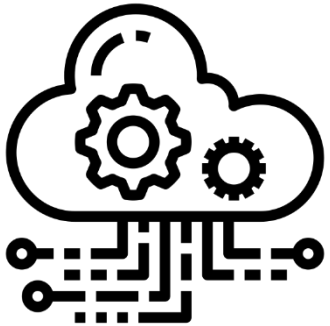


Apprentissage automatique

Les dimensions de la cyber résilience



Agilité

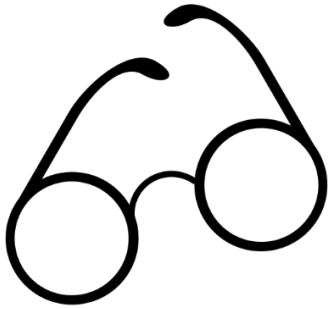


*-as-a-Service (XaaS)

Zero-Trust Ecosystem

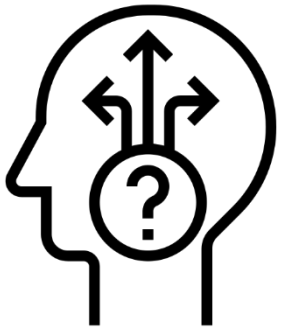
Zero-Touch Network

Conseils pour devenir cyber résilient



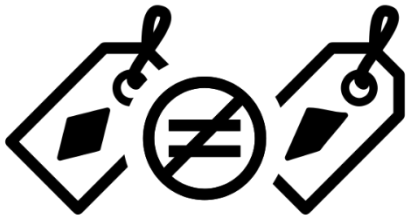
Corriger la myopie

Traiter l’amnésie



Garder une part
d’incertitude et prendre gare
à l’excès d’optimisme

Combattre l’inertie et
la simplification



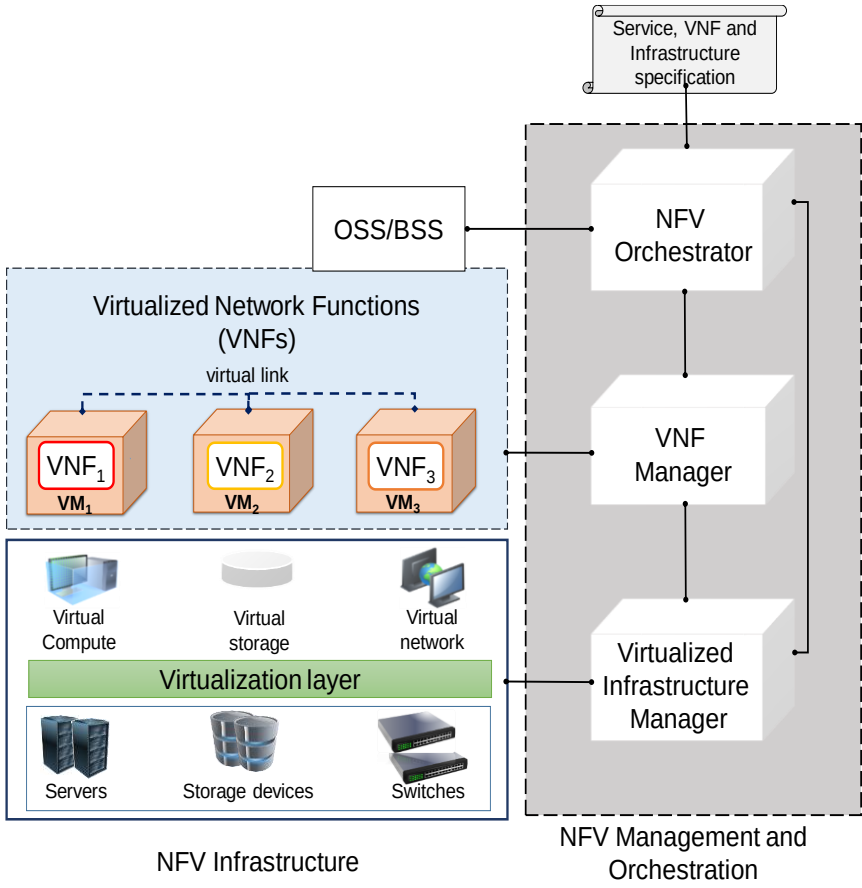
Faire de l’imitation cognitive
un moteur d’innovation

Quelques travaux de recherche en cours

Nouvelles menaces sur les infrastructures virtualisées

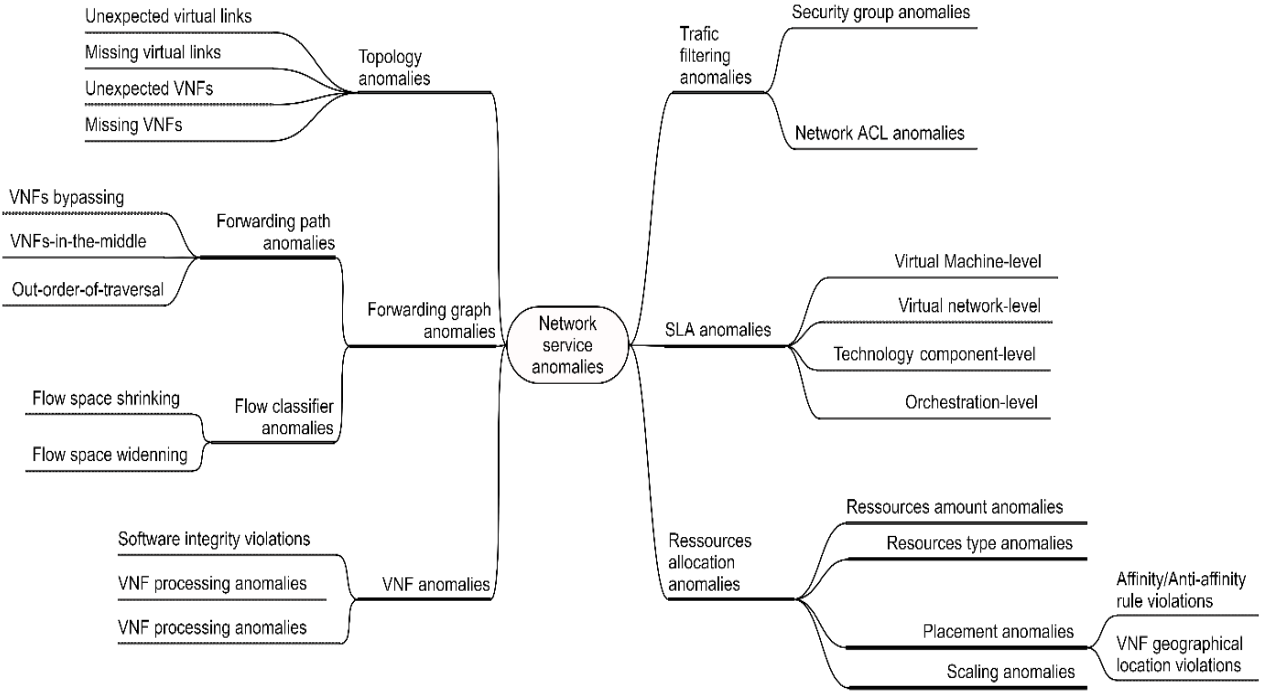
- Menaces sur la couche d'orchestration :
  - Vulnérabilités de l'orchestrateur, de l'API ou de l'interface de configuration (web)
  - Possible reconfiguration de manière malveillante des services déployés
  - Possible incohérence entre les services déployés et leur spécification

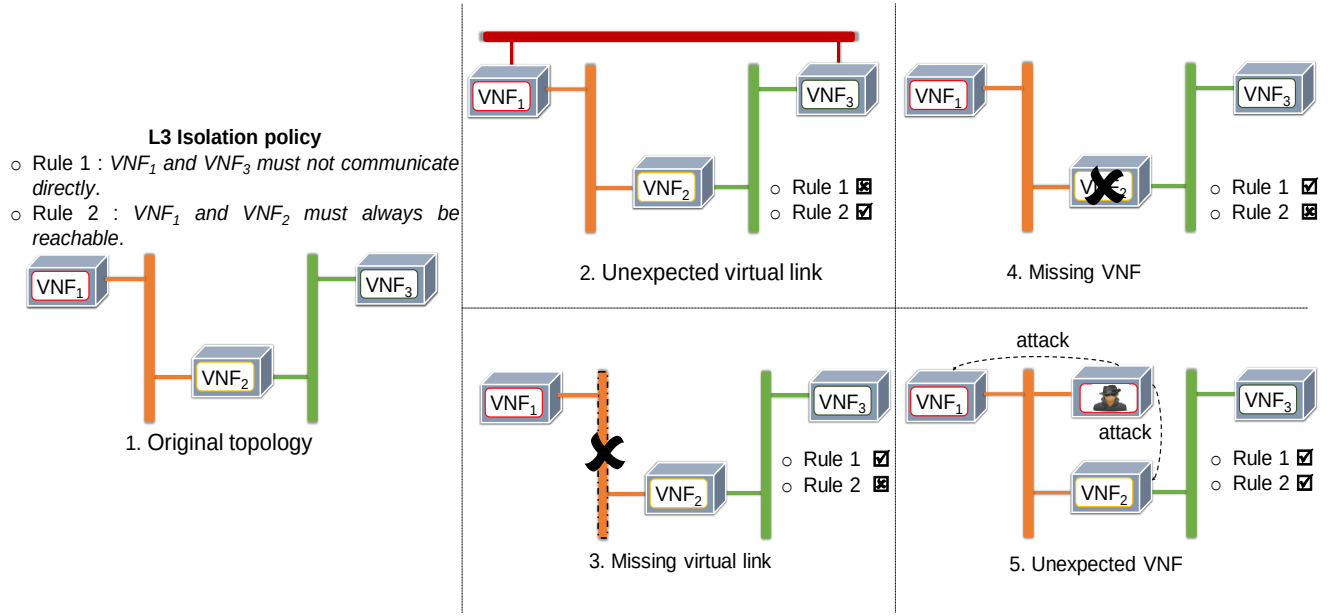
- Menaces sur la couche infrastructure NFV :
  - Problèmes de sécurité sur les VM, les hyperviseurs, les interfaces de gestion, les ressources virtuelles, …
  - Un interne malveillant peut avoir accès aux VNF et exfiltrer des données sensibles

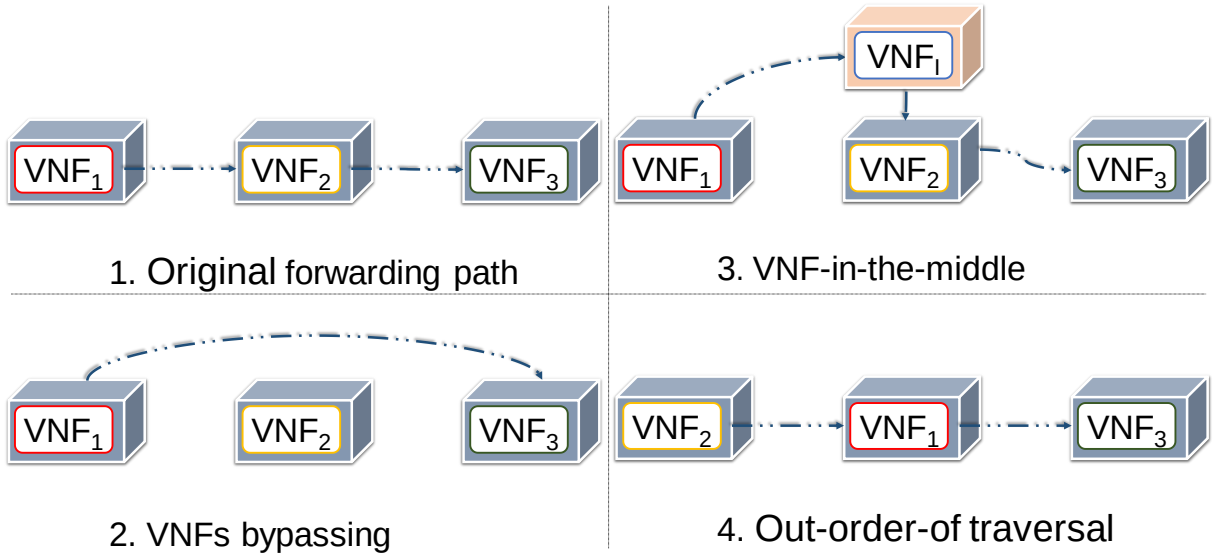


Quelques travaux de recherche en cours

Anomalies de services cloud



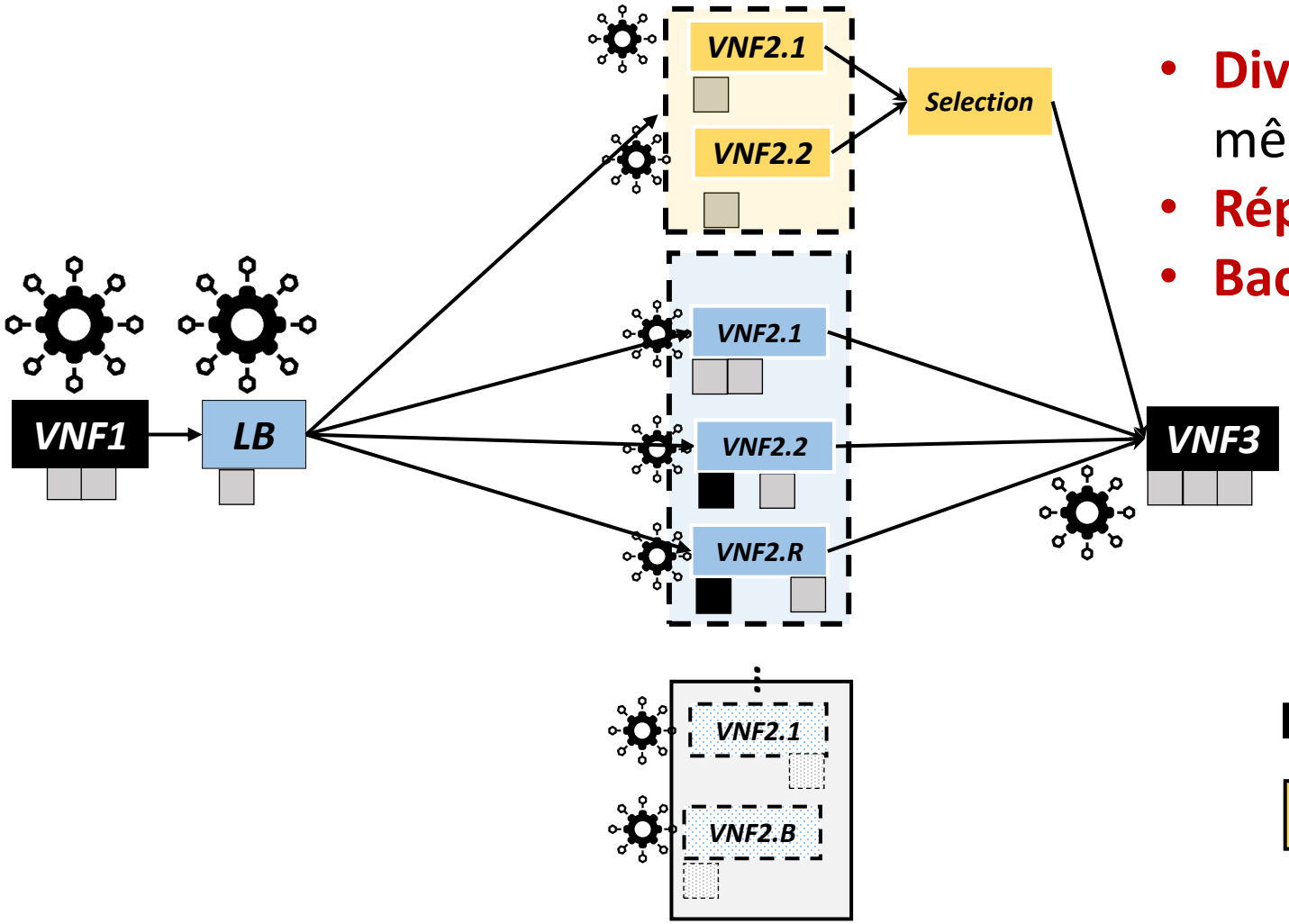




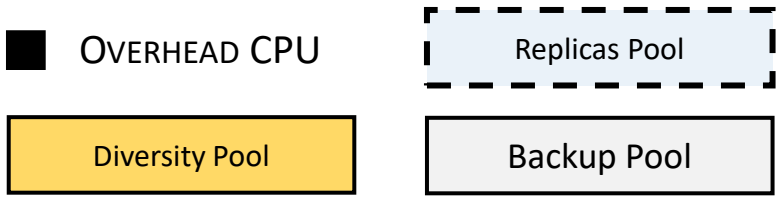
Quelques travaux de recherche en cours

Cyber résilience des infrastructures virtualisées

Personnalisation de la résilience Diversité / Réplicas / Backup : **D+R+B**



- **Diversité** (D) instances fonctionnent en même temps mais une seule sortie utilisée
- **Réplicas** (R) instances actives
- **Backup** (B) instances passives

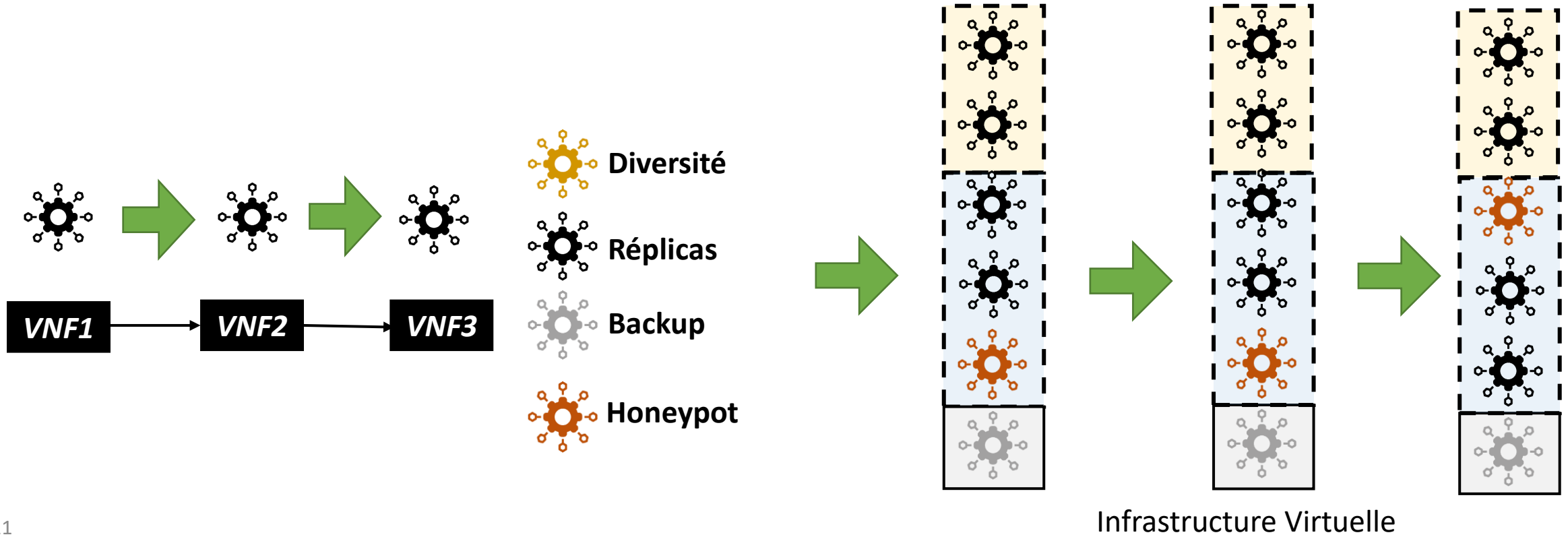


Quelques travaux de recherche en cours

Moving Target Defenses for cyber deception and proactive defense

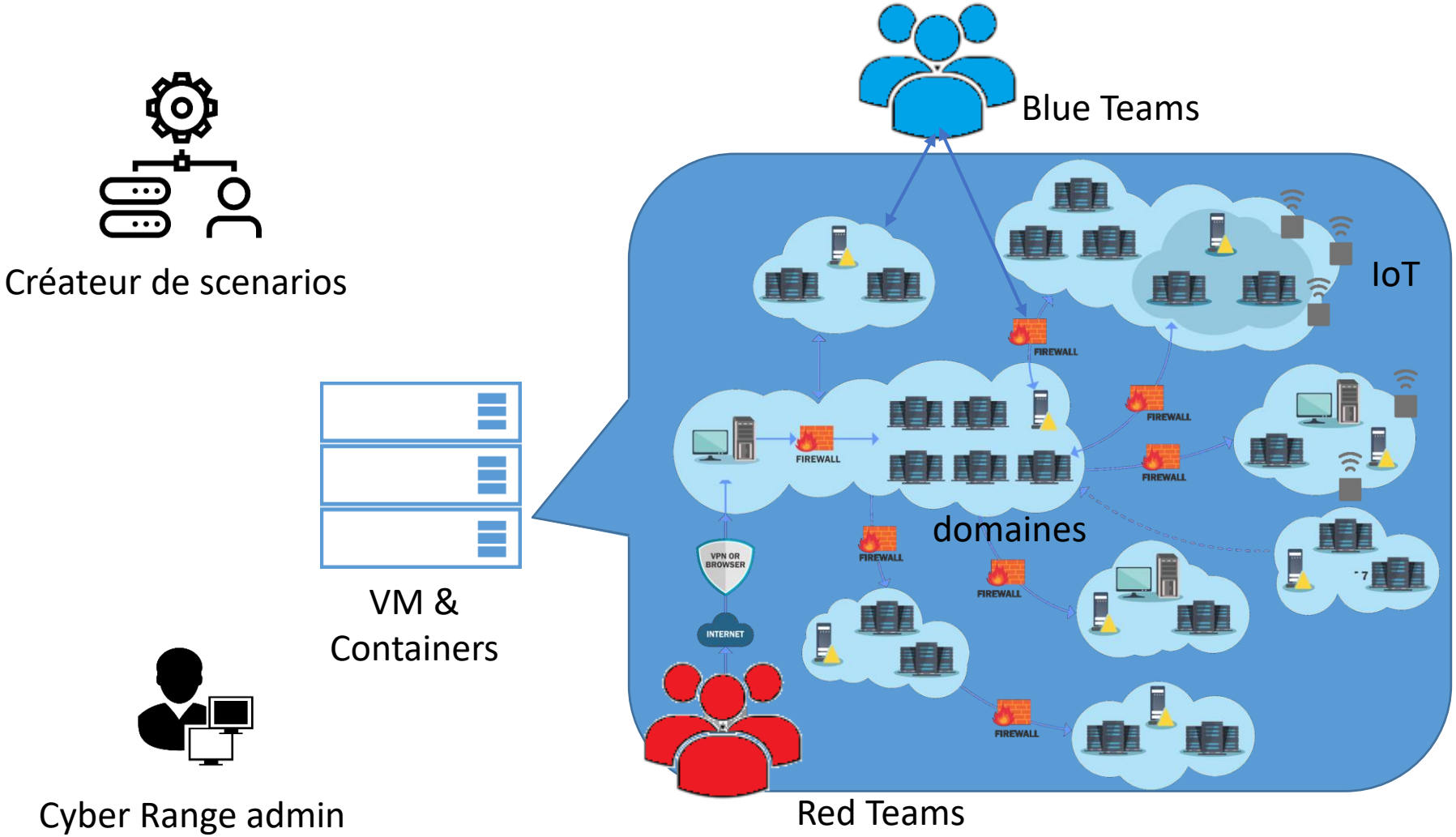
Objectif : augmenter le coût de la reconnaissance

- Orchestration dynamique des services pour cacher la vraie configuration
- Modification de la surface d'attaque par rotation dynamique des instances
- Diversité croissante des chemins et des instances



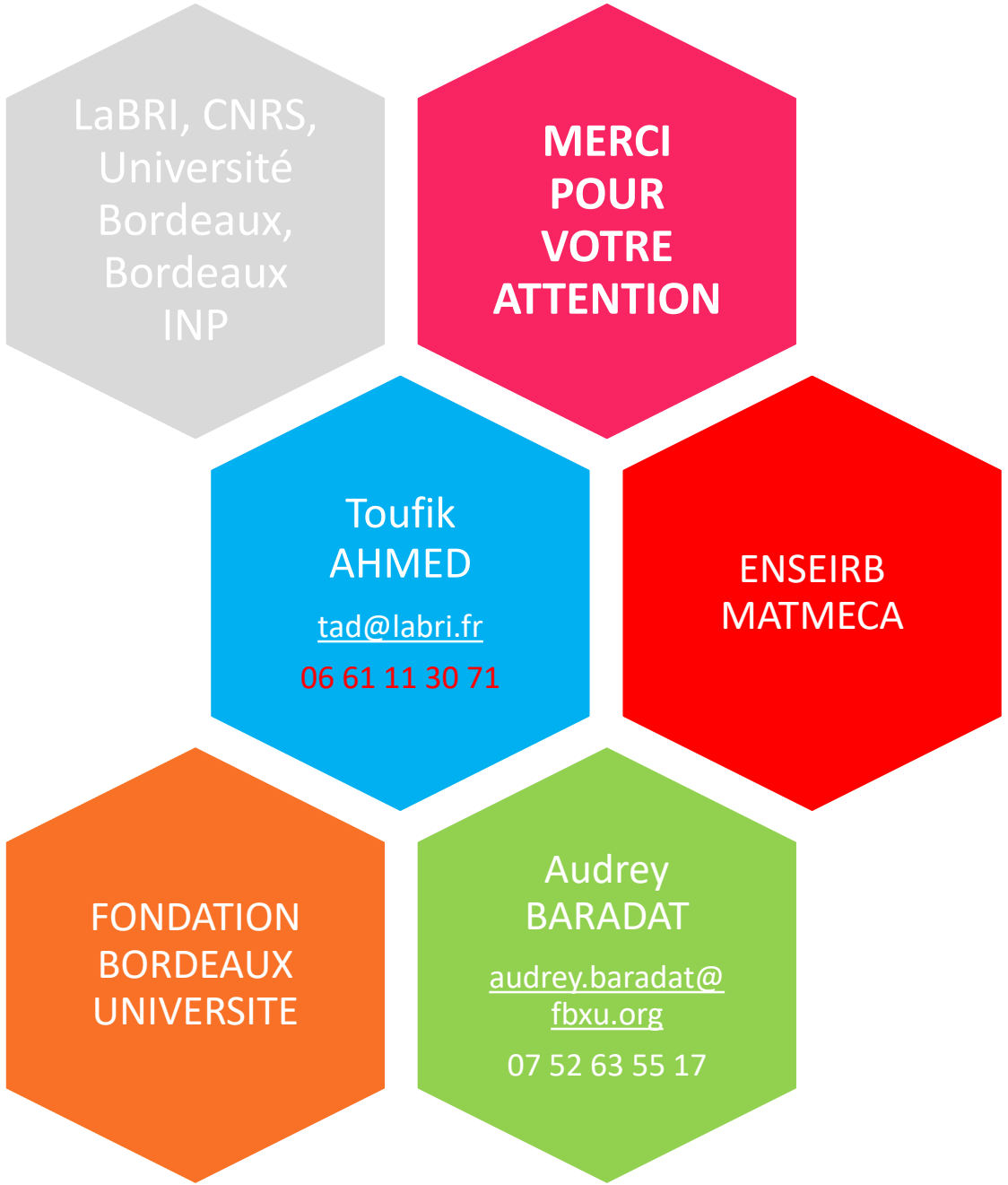
Transfert

Développement de ressources d'entrainement



Transfert

Entrainement à la gestion de crise cyber @ENSEIRB-MATMECA


LaBRI, CNRS, Université Bordeaux, Bordeaux INP
MERCI POUR VOTRE ATTENTION
Toufik AHMED
tad@labri.fr
06 61 11 30 71
ENSEIRB MATMECA
FONDATION BORDEAUX UNIVERSITE
Audrey BARADAT
audrey.baradat@fbxu.org
07 52 63 55 17