



# CYBERWEEK

## 2024

### LA RECHERCHE DANS LE DOMAINE DE LA CYBERSÉCURITÉ

17 OCTOBRE 2024



NAMUR



Agence  
du Numérique



Cyberwal  
by digital  
wallonia



Wallonie  
Relance

# Programme

8h30 : Café et bienvenue.

9h00 : Introduction.

9h15 : Présentation du paysage de la recherche en Cybersécurité en Wallonie – Samuël Jude, UCLouvain.

10h15 : Présentation du Belgian Security & Defence Industry (BSDI) - Eric Van Cangh, Agoria.

10h45 : Pause-café.

11h00 : BeQCI: building Belgium's first public quantum communication testbed - Karel Dumon, IMEC.

11h30 : Tour d'horizon des appels à projets européens - Ellen Stassart NCC, CCB.

12h15 : Conclusion.

12h30 : Networking lunch. Animation par Cresco: HackingLab.



**Samuël Jude**

UCLouvain





# La recherche en Wallonie

17 octobre 2024



# Agenda



- État de la recherche dans le domaine de la cybersécurité en Wallonie
  - Les acteurs académiques et centres de recherche
  - Les différentes initiatives existantes
  - Hot topics
- CyberExcellence, une réussite wallonne
  - La philosophie
  - Méthode de travail
  - Résultats
- L'Initiative d'Innovation Stratégique CyberWal
  - « Hub » d'innovation
  - Valorisation de la recherche
  - Internationalisation

# État des lieux

Les acteurs académiques et centres de recherche



# État des lieux

Les acteurs académiques et centres de recherche



Analyse de risque



Analyse de Malware, vérification formelle & sécurisation des clouds



Formation et cybersécurité dans le domaine de l'économie circulaire



Cybersécurité à l'exécution



Laboratoires et créations de démonstrateurs



Aspects juridiques liés à l'IT



Systèmes de certification en cybersécurité



Cybersécurité des systèmes cyber-physique

# État des lieux

Les initiatives wallonnes en cybersécurité



**.AGORIA**



**DIANA**<sup>®</sup>



Calling all **innovators**

# État des lieux

Les initiatives wallonnes en cybersécurité



**.AGORIA**



**DIANA**<sup>®</sup>

Calling all **innovators**



**Cyberwal**



**CyberExcellence**  
By CyberWal



# État des lieux

## Hot topics

- Défense
- Spatial
- Informatique quantique
- Logistique
- Économie circulaire
- Secteur de la santé
- Secteur de l'énergie



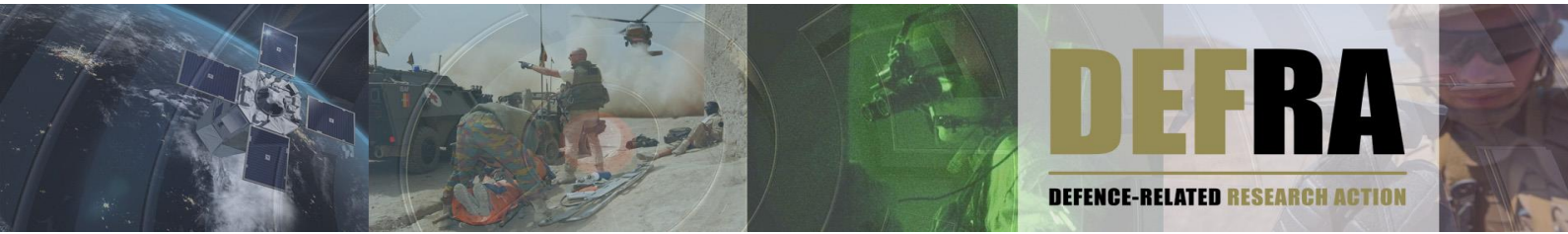


# État des lieux

## Hot topics

- Défense
- Spatial
- Informatique quantique
- Logistique
- Économie circulaire
- Secteur de la santé
- Secteur de l'énergie

Conformité NIS2,  
CRA





# CyberExcellence

## Préambule

### On entendait parfois des opinions assez subjectives:

- La cyber sécurité est perçue comme un coût,
- On ne sera jamais attaqués,
- Ça n'augmente pas les parts de marché de l'entreprise.

### Vérités :

- Toute entreprise qui a été attaquée a perdu plus d'argent que si elle avait investi dans des protections,
- Toute entreprise qui a du matériel informatique est susceptible d'être attaquée,
- La cybersécurité, si elle est perçue comme digne de confiance, rapporte de l'argent à l'entreprise (marché, alignement sur directive, réputation, ...).

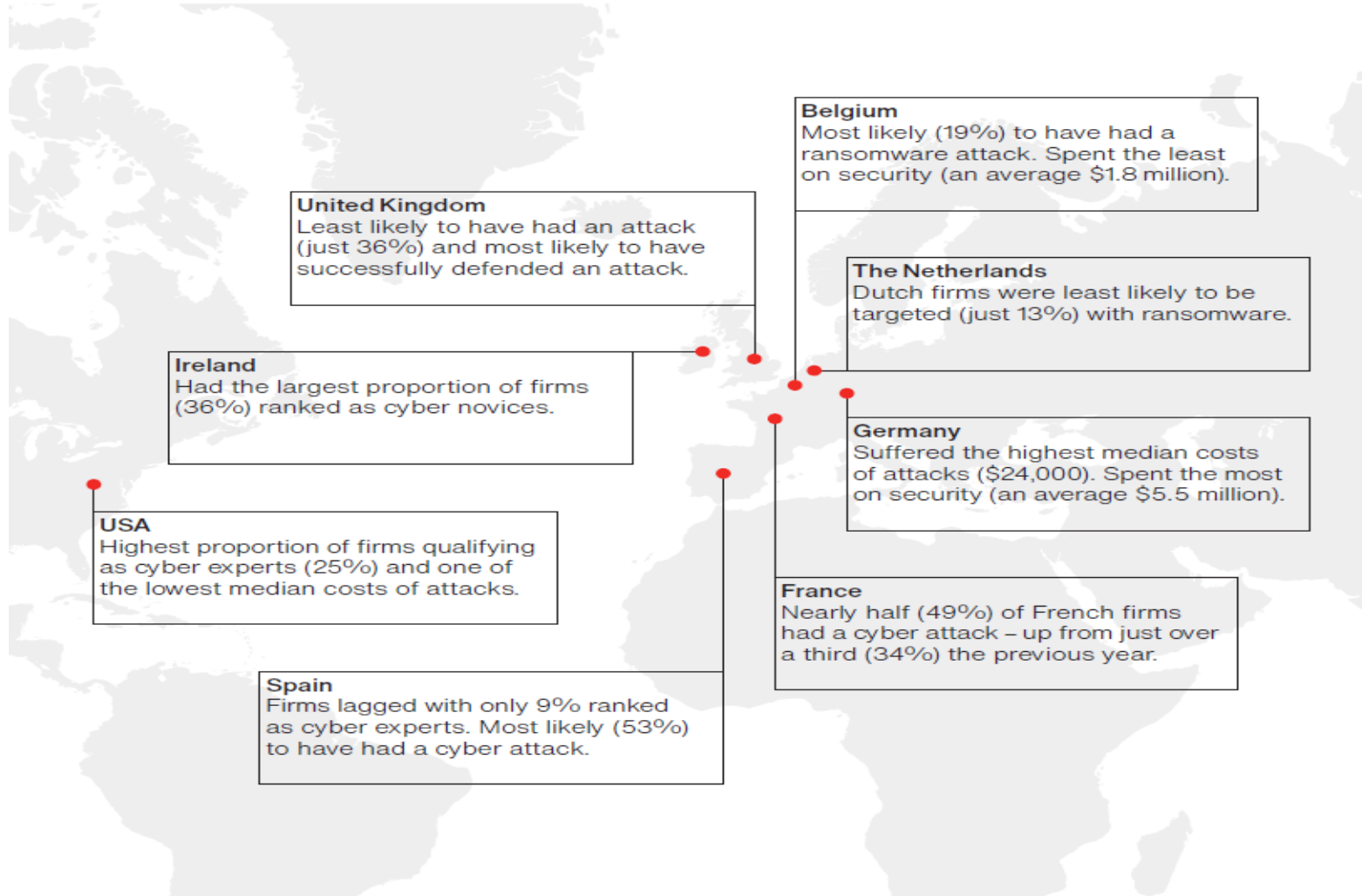
# CyberExcellence

## Préambule

- En 2019, l'entreprise belge moyenne a perdu 54.700 € (montant médian) à cause de cybercrimes.  
=> Cela peut monter jusqu'à 13 millions et ça touche de plus en plus le monde public (diversité).
- Le coût médian en Belgique est supérieur au coût médian des nations occidentales (54.700 € vs 52.000€).  
=> Au vu de ses infrastructures sensibles (OTAN, Europe ...), la Belgique est une cible de choix.
- Le coût a été multiplié par 6, malgré une diminution du nombre d'organisations visées (61 à 39 %).  
=> Les attaques sont de plus en plus pointues.  
=> Une innovation liée à une recherche appliquée doit être menée.

# CyberExcellence

## Préambule



Situation du point de vue du tissu économique (2020)

# CyberExcellence

## Préambule

Nos discussions avec les industriels wallons (2020-2021) montrent que les besoins sont forts :

- Les entreprises sont prêtes à engager massivement dans le domaine.
- Il ne s'agit pas d'une simple hygiène de la sécurité. Les entreprises veulent des profils pour développer des approches pour garantir la sécurité de leurs activités dans des domaines sensibles.
- Exemple: SWDE, ORES, RHEA, IBA, BELFUIS sont tous demandeurs et en recherche de talents.
- **Les entreprises spécialisées dans la production de solution de cybersécurité font venir des travailleurs de l'étranger.**
- Les industriels se sentent déconnectés des universités (besoin en compétences/formations).

# CyberExcellence

## Préambule

### Situation du point de vue de la recherche (2021)

- Les universités n'ont jamais autant engagé (4 profs en 6 ans rien que pour UCLouvain, une chaire ULB et 3 profs, ...)
- Et pourtant ...notre visibilité reste faible.
- Problème de massification, absence de placement par rapport à des défis concrets venus du tissu socio-économique, mauvais positionnement à l'Europe, groupes "inconnus".

=> Il faut une stratégie pour la cyber sécurité en Wallonie

# CyberExcellence

## Notre philosophie

- Consortium de recherche regroupant les acteurs de la recherche en cybersécurité en Wallonie
  - UCLouvain
  - ULB
  - UMons
  - UNamur
  - Uliège
  - CETIC
  - Multitel
- Financement “Win4Excellence” 2022-2027
- Créer de la valeur sur base de la recherche effectuée en cybersécurité en Wallonie

# CyberExcellence

Notre philosophie

## L'exemple breton

2014-2020:

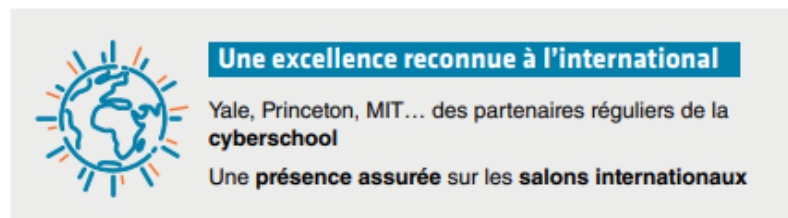
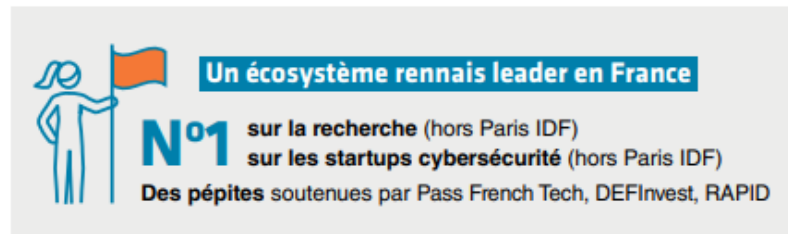
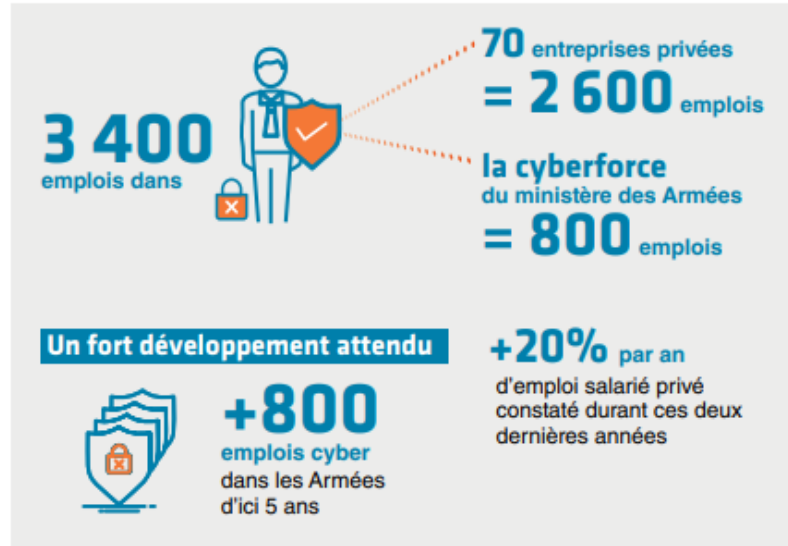
- Rassembler les acteurs de la recherche
- Faire le lien avec l'industrie (innovation) et l'armée
- Massifier la formation
- Tourner

2021 – Présent

- Programme en pleine charge, création d'une école de la cyber sécurité (type université – cursus sur plusieurs années)
- Reçoit une attention MAXIMALE de l'état (capter les financements) et de l'Europe

# Une attractivité forte (illustration pour la population RENNAISE)

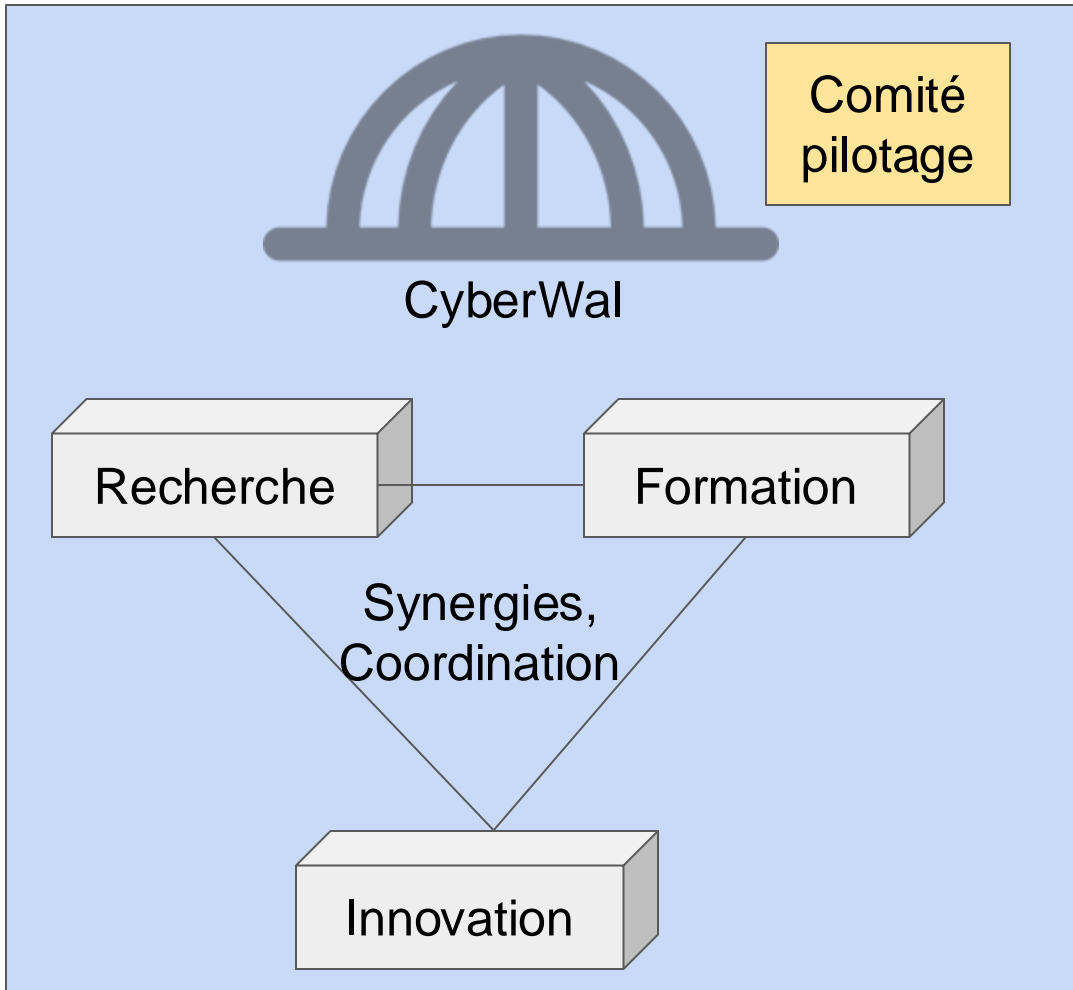
## La cybersécurité dans Rennes Métropole





# Solution: CyberWal (Pôle cyber wallon)

Stratégie de spécialisation intelligente S3 &  
Stratégie régionale Digital Wallonia



Du point de vue de la recherche et de l'innovation

- Identifier les besoins venus de nos entreprises et ceux de l'Europe
- Mener une recherche appliquée dont la finalité est d'atteindre des TRL hauts (innovation)
- S'aligner sur les DIS de la S3
- Garder un lien fort avec la formation

# CyberExcellence

## Notre philosophie

### Pour la recherche : CYBEREXCELLENCE (2022-2027)

- Concrétise le volet recherche TRL2-4 de CyberWal
- Lie les 5 universités francophones et les 2 centres de recherche actifs dans le domaine
- Seuls les acteurs académiques pertinents et la recherche appliquée à haute finalité sont retenus (SPW)
- Se positionne sur de la recherche innovante en lien avec la S3, les défis européens, les défis de notre tissu socio-économique
- **Former 50 chercheurs/an sur 6 ans avec un budget de 27 000 000€**
- Avoir une position équivalente à celle du LIST ou du Pôle cyber Breton à la fin des 6 ans

# CyberExcellence

Notre philosophie

## CYBEREXCELLENCE : une grande envergure

- Suit le modèle TRAIL/ARIAC pour l'intelligence artificielle (2021-2024 et prolongé de 2 ans)
- Il faut des WP, des défis industriels, de la visibilité, ... Et surtout une méthodologie pour tout coordonner
- Il faut créer une communauté et rassembler aussi les projets existants
- CyberExcellence a mené à la création d'une IIS (initiative d'innovation stratégique) qui regroupe l'ensemble des projets de recherche des acteurs wallons en cybersécurité
- **En résumé:** CyberExcellence, ce sont plusieurs projets en un seul.

# CyberExcellence

Notre méthodologie

Les WP du projet CYBEREXCELLENCE (1)

“Une recherche pensée pour une visibilité maximale”

- 5 WP liés à la recherche (de la sécurité à la construction, aux laboratoires d'entraînement en passant par l'éthique et le RGPD)
- Les thématiques sont choisies après une étude avec le tissu socio-économique (2021)
- Les tâches sont évolutives et seront identifiées par rapport à des besoins/défis et une évolution des thématiques possible en fonction des besoins/défis

# CyberExcellence

Notre méthodologie

## Les WP du projet CYBEREXCELLENCE (2)

“Une recherche pensée pour un impact maximal sur le tissu socio-économique”

- Un workpackage type “software factory” pour mettre les réalisations à la disposition des entreprises
  - ... s’adapte au profil de l’entreprise (prestataires, utilisateurs avec/sans compétences internes),
  - ... et lever des projets à TRL plus avancés (FEDER),
  - ... et montrer que ce que l’on fait sert vraiment à quelque chose.
- La factory doit être disponible après 4 ans, les fondations posées après 2 ans

# CyberExcellence

## Notre méthodologie

### Les défis : notre philosophie pour s'aligner sur la S3

- On cherche à impacter le tissu socio-économique
- Nous sommes convaincus qu'une recherche cyber n'a de sens que si on peut l'appliquer (métrique de publication)
- On travaillera à la fois sur:
  - des défis émergents (après 2 ans)
  - des défis existants sur lesquels nous pouvons apporter une plus-value (au départ du projet)
- Les défis type "prof d'unif déconnecté de la réalité" ou "défis à finalité non impactante" sont exclus

# CyberExcellence

Notre méthodologie

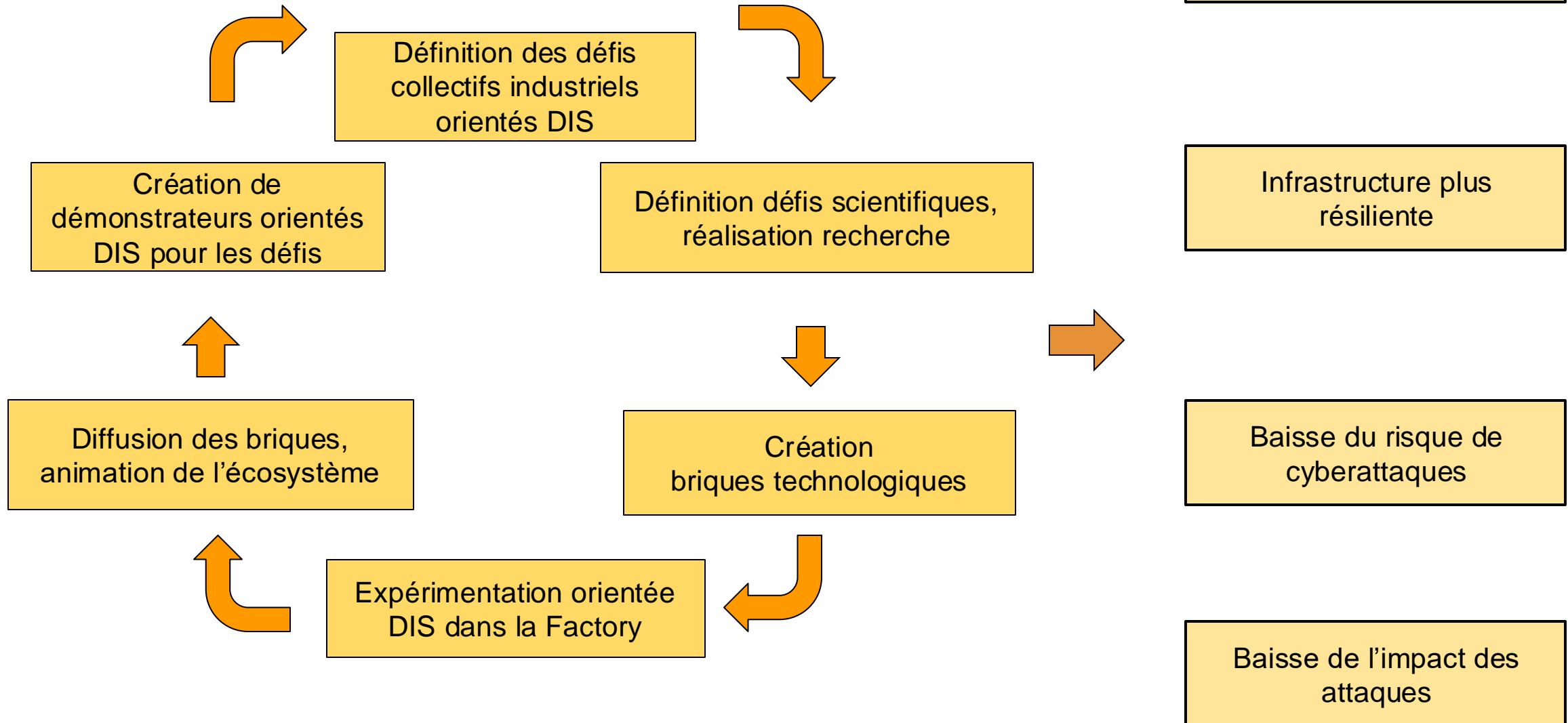
## Les acteurs pour remonter les défis

- Les grands classiques : universités, CRA, ADN, réseau Lieu
- Chaque étudiant travaillera au moins 15% de son temps avec un CRA
- Les “moins classiques” (niveau recherche) : Agoria, info pole, WBI, A6K, IDLUX, ....

# CyberExcellence

Notre méthodologie

Collecte des défis au cours du projet (WP6)





# CyberExcellence

## Notre méthodologie

### Quels WPs recherche pour CyberExcellence (à la création)?

WP1 - Rendre les systèmes résilients aux cyberattaques: phase de conception

WP2 - Détection, Réponse, Réaction: Phase Dynamique

WP3 - RGPD et Open data: sécurité à la conception

WP4 - La protection et le partage des données au cœur des préoccupations

WP5 - Laboratoires d'expérimentation, de validation, et d'entraînement

- Les WP1,2, et 3 sont alignés sur les DIS
- Les WP4 et 5 sont transversaux
  
- Tous les WP sont alignés sur des défis wallons et européens (un an de travail)
  
- **Tâches reconfigurables en fonctions des défis.**
  
- **Création d'une IIS pour rayonner sur la DIS de la S3 (aide Wallonie post COVID)**

# WP - DIS innovations pour des modes de conception et de production agiles et sûrs (PRODUCTION)

WP1 - Rendre les systèmes résilients aux cyberattaques: phase de conception

WP2 - Détection, Réponse, Réaction: Phase Dynamique

WP3 - RGPD et Open data: sécurité à la conception

WP4 - La protection et le partage des données au cœur des préoccupations

WP5 - Laboratoires d'expérimentation, de validation, et d'entraînement

Industrie du futur

Technologies de fabrication avancée

Matériaux avancés

Matériaux fonctionnels intelligents

Matériaux bio-inspirés

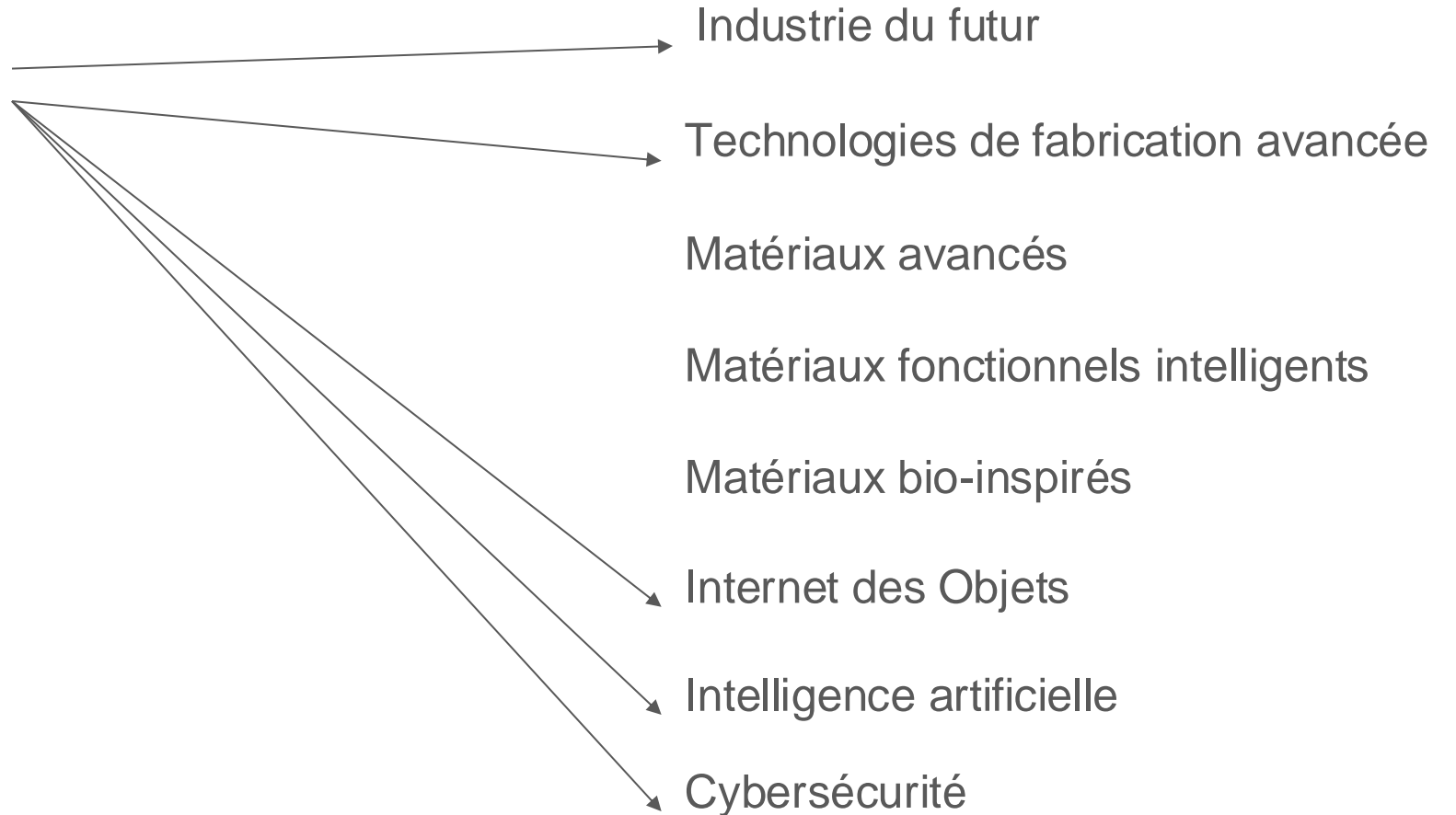
Internet des Objets

Intelligence artificielle

Cybersécurité

Simulation numérique

Conception et outils de simulation



# WP - DIS systèmes énergétiques et habitat durables (ENERGIE)

WP1 - Rendre les systèmes résilients aux cyberattaques: phase de conception

WP2 - Détection, Réponse, Réaction: Phase Dynamique

WP3 - RGPD et Open data: sécurité à la conception

WP4 - La protection et le partage des données au cœur des préoccupations

WP5 - Laboratoires d'expérimentation, de validation, et d'entraînement

Efficacité énergétique des bâtiments

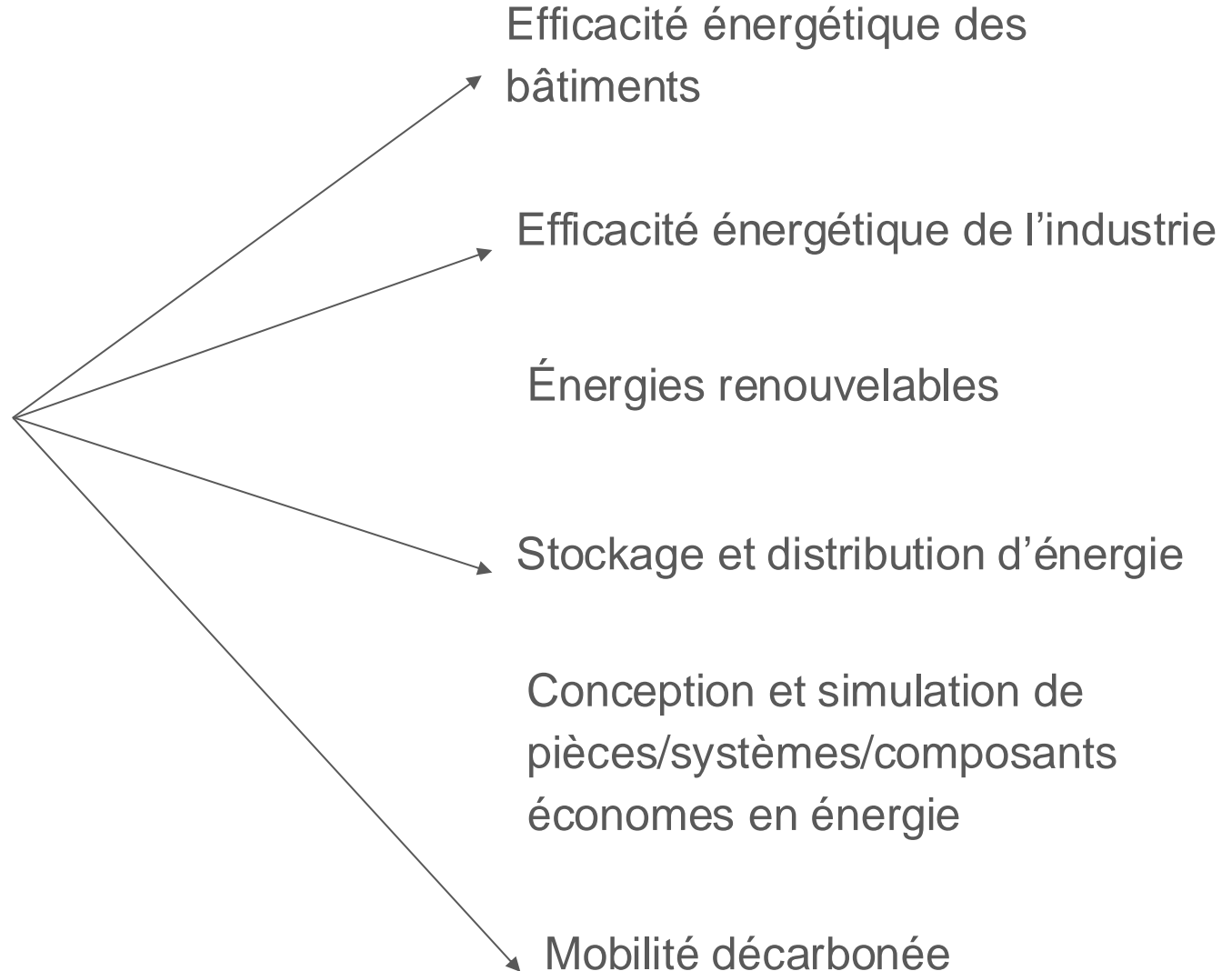
Efficacité énergétique de l'industrie

Énergies renouvelables

Stockage et distribution d'énergie

Conception et simulation de pièces/systèmes/composants économes en énergie

Mobilité décarbonée



# WP - DIS innovations pour une santé renforcée (SANTE)

WP1 - Rendre les systèmes résilients aux cyberattaques: phase de conception

WP2 - Détection, Réponse, Réaction: Phase Dynamique

WP3 - RGPD et Open data: sécurité à la conception

WP4 - La protection et le partage des données au cœur des préoccupations

WP5 - Laboratoires d'expérimentation, de validation, et d'entraînement

Biotechnologies

Technologies médicales

Radiothérapie

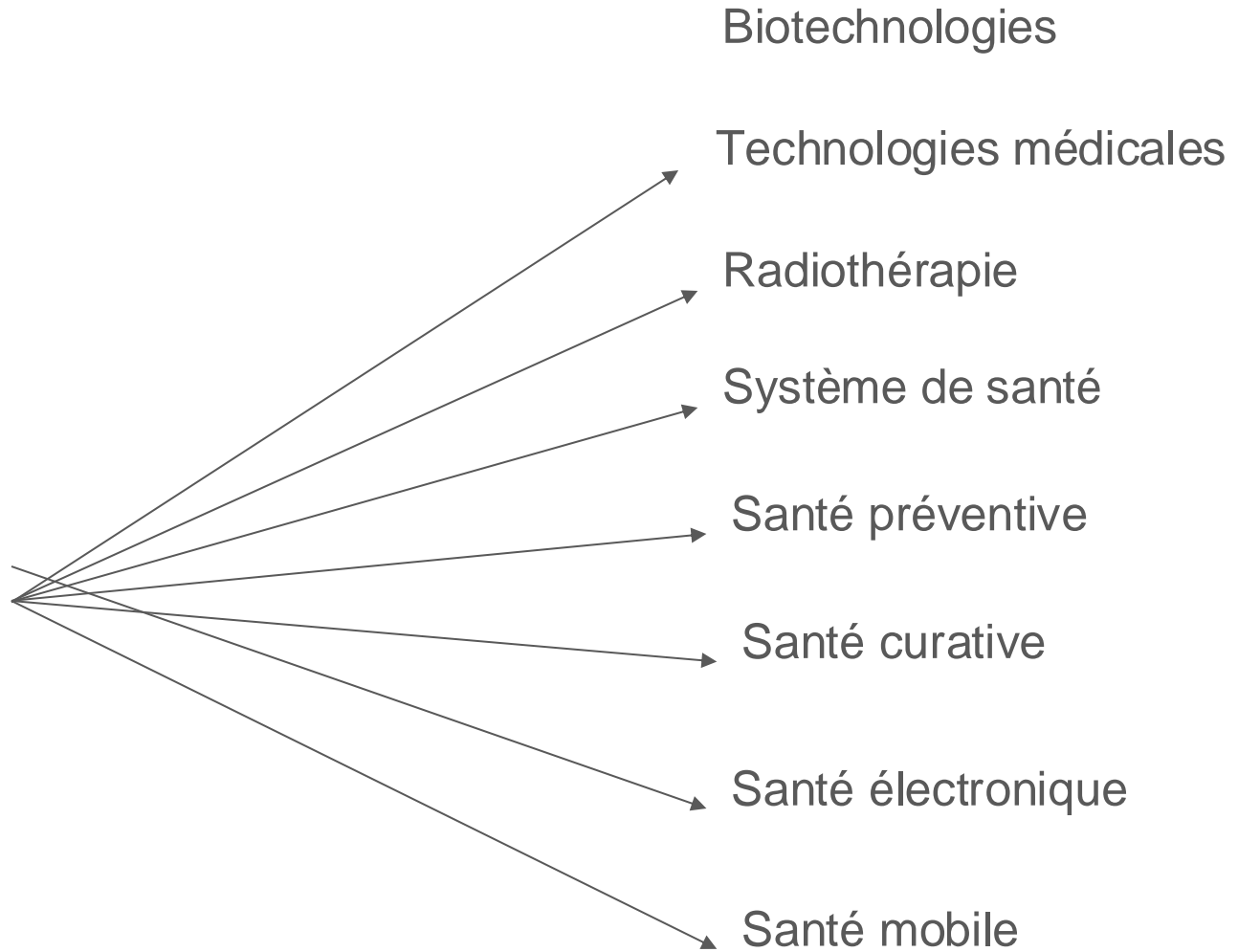
Système de santé

Santé préventive

Santé curative

Santé électronique

Santé mobile

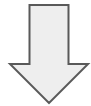


# Exemples de défis scientifiques (candidats + briques factory)

CPSET - Cyber Physical System in Energy conversion & Transport



Roadmap CPSET : Brique technologique générique - Cybersecurity test bench



CyberWal

Défi industriel collectif

Automatisation de la vérification cyber de CPS (Cyber Physical Systems)

**Défis scientifiques**

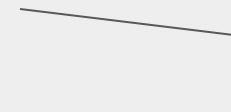
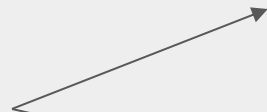
Automatisation des tests fonctionnels de cybersécurité

Automatisation des tests

**Brique technologique**

Générateur de tests de cybersécurité

Générateur de tests d'intrusion.



# CyberExcellence

## Objectifs du projet

- Talents formés à la recherche en cybersécurité
  - A terme, toute entreprise wallonne pourra engager des chercheurs de CYBEREXCELLENCE
  - Ultra qualifiés et demandés dans le monde entier
- Valorisation
  - Mise à disposition des résultats aux entreprises
  - Toute entreprise wallonne pourra participer aux défis industriels et à l'expérimentation des briques technologiques dans la factory
  - Augmentation de l'innovation et la compétitivité
  - Création de start-ups
- Création d'une communauté wallonne qui génère d'autres projets et qui fédère les existants
- Visibilité à l'international
  - Publications scientifiques, workshops internationaux, création d'une école cyber, ...
  - Positionnement de la Wallonie en Belgique, à l'Europe et dans le monde

# Que veut dire « collaborer » dans CyberExcellence?

- Dans les projets académiques, collaborer veut souvent dire co-diriger des thèses et écrire des articles communs.
- La thématique de CyberExcellence n'est pas unique, ce n'est pas un projet européen où tous doivent travailler sur les mêmes technologies dans le même WP. Ici le but est d'explorer et d'être large.
- **Au sein de CyberExcellence :**
  - Mettre les personnes ensemble et savoir qui fait quoi (et éviter de faire 2 fois la même chose) ;
  - Résoudre des défis communs en combinant des techniques de pointe ;
  - Collaborer avec les entreprises et impacter le tissu socio-économique en résolvant des défis ;
  - Créer une communauté et de nouveaux projets pour assurer la pérennité du pôle.
- **En Résumé :** CyberExcellence pose les fondations d'une collaboration et d'un dialogue de long terme entre les acteurs cyber wallons. Le projet explore le futur de la cybersécurité Wallonne.

# Résultats du projet après 2 ans (résumé)



- Les chercheurs ont été engagés (ça n'a pas été simple)
- Les WP donnent d'excellents résultats (nombreuses publications + défis)
- De plus en plus d'entreprises nous rejoignent et proposent des défis
- Une communauté cyber a été créée autour de CyberWal
- Nous avons drastiquement augmenté le nombre de projets fédéraux et EU en Cyber (première thématique à succès en Wallonie)
- Notre visibilité à l'international ne cesse de croître (projets, écoles, ...)



# Résumé d'indicateurs de réussite

- Nombre de chercheurs financés CyberExcellence : 63 (31 en 2022)
- Nombre de chercheurs affiliés à la communauté : 130 (86 en 2022)
- Environs 20 Professeurs
- Nombre de publications par des chercheurs financés CyberExcellence : 134 (13 en 2022)
- Nombre de projet européen: 10 (2 en 2022) et de nombreuses nouvelles soumissions
- Participation importante à l'école d'hiver: 222 participants !
- Collaboration accrue avec la Flandre (ex : projet AIDE, CyberActive, AMC3)
- Plus de 20 réunions de travail par an

**En bref : la recherche et la création de la communauté au travers de l'IIS sont des succès.**

# Avancées du WP1

- Tâche sur la certification au moyen de modèles mathématiques (T1.1)
  - Spécification formelle d'un système: Terminée (Ivy, mCRL2, Bach)
  - Vérification formelle: En cours (UPPAAL-SMC, Anemone)
  - Applications pratiques: En cours (QUIC, BGP, crypto-finance, CPSs)
- Tâche sur le test (T1.2)
  - Recommandation d'approche de test/fuzzing: En cours (enquête industrielle, analyse de GAs)
  - Fuzzing: Terminée (Black-box fuzzing, règles de sécurité)
  - Applications pratiques: En cours (CPS, semgrep, directives EU)
- Tâche sur la virologie informatique (T1.3)
  - Analyse de malwares: Terminée (SEMA)
  - Détection de malwares: En cours (SMT solving)
- Tâche sur le lien logiciel/matériel (T1.4)
  - Simulation d'injection de faute matériel : Terminée (Transient Effect Ring Oscillator PUF)
  - Applications pratiques: En cours (FPGA, RISC-V)

## Avancées du WP2

- Tâche sur l'observabilité (T 2.1) : en cours
  - Développement d'algorithmes et techniques pour surveiller les infrastructures informatiques
    - e.g., In-Situ OAM (IOAM), uTNT, Cross-Layer Telemetry
- Tâche sur la réponse dynamique (T 2.2) : en cours
  - Développement d'algorithmes et techniques pour permettre la réponse dynamique
    - e.g., unikernels, Smoothie
- Tâche sur la réaction (T 2.3) : en cours
  - Développement de méthodes et techniques pour l'analyse de la résilience du système
    - e.g., Micro-Services Topology Generator, CSoD
- En cas de prolongation
  - Réalisation complète des activités de recherche en lien avec NIST-2

# Avancées du WP3



- Tâche de vulgarisation du RGPD (T 3.1) : Terminée (fiches et vidéos)
- Méthodes de validation formelles (T3.2) : Terminée: formalisation des propriétés du RGPD et mise en relation avec le WP1
- Algorithmes d'anonymisation : en cours et création d'un défis médical
- En cas de prolongation :
  - Concentration sur la directive NIS-2 (extension Tâche 3.1 et lien WP1) et la tâche 3.3 (continuité du défis médical)
  - Application de ChatGPT pour génération automatique de modèles

## Avancées du WP4

- Sécurité des interactions avec le cloud (T4.1) – Travail en cours
- Déploiement sûr à travers des continuum des clouds et edges souverains (T4.2) – Travail en cours
- Chiffrement et robustesse des chiffrements cryptographiques (T4.3) –Travail en cours
- Implémentations matérielles et logicielles sécurisées contre les attaques physiques (T4.4) –Travail en cours

## Avancées du WP5

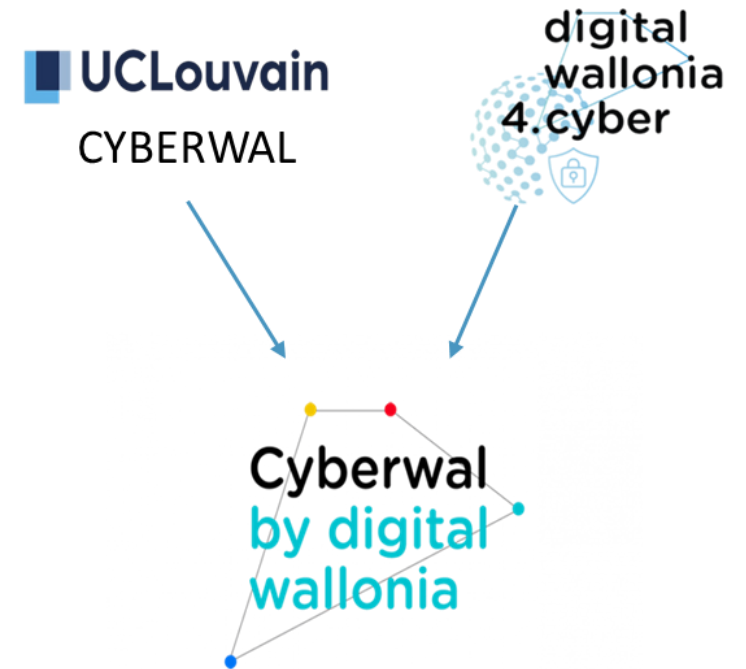


- Tâches sur l'acceptation par les utilisateurs (T5.1) : succès au travers de mise en place d'une évaluation d'un cyber range industriel (CRS)
- Synthèse d'attaques à partir de vulnérabilité (T5.2) : en cours et remise en force dans le WP (state-space exploration)
- Les tâches d'hybridation (T5.3) et de Devsecops (T5.4) n'ont pas encore commencé (comme prévu dans le cahier des charges)
- Une tâche supplémentaire pour la configuration et le déploiement de ranges (Uliège, ULB) a été ajoutée. En cas de prolongation nous désirons capitaliser sur ces ranges

# L'IIS CyberWal

## Un constat

- Beaucoup de savoir-faire en cybersécurité en Wallonie parsemé partout sur le territoire
  - Compétences n'attirent pas à l'international
  - Impact moins important sur le tissu socio-économique
- En 2021, sous l'impulsion du professeur Axel Legay, les différentes universités, centres de recherches et de nombreuses entreprises actives dans le domaine se rassemblent pour créer CyberWal
- Dans le même temps, Digital Wallonia crée un programme « Digital Wallonia 4 cyber »



# L'IIS CyberWal

## Un IIS, un consortium

- Consortium réunissant les acteurs de la recherche et du tissu socio-économique wallon
  - Plus de 130 chercheurs
  - Plus de 80 entreprises
  - Fédérations patronales
  - Incubateur d'entreprise
  - Etc.
- Trois comités : comité de pilotage, scientifique et éthique, business
- Philosophie : rapprocher les acteurs de la recherche et du monde de l'entreprise pour maximiser la valorisation de l'innovation

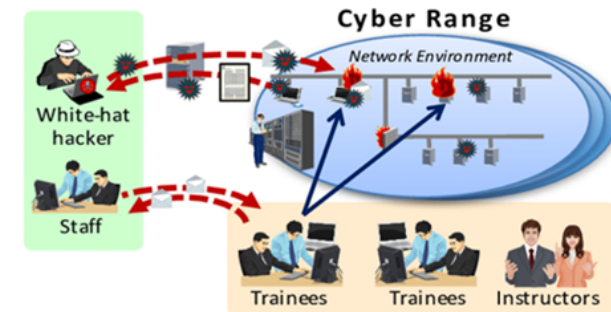




# L'IIS CyberWal

## Un « Hub » de l'innovation

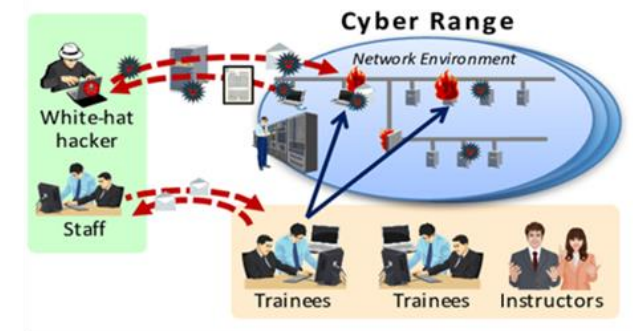
- Des projets de recherche :
  - CyberExcellence
  - AMC3 (Defense-Related Research Action)
  - BeQCI
  - ...
- Formation
  - CyberWal in Galaxia (école éphémère en cybersécurité)
    - Ecole gratuite
    - 5 jours, plusieurs thématiques
    - Plus de 200 participants
  - CyberActive
- Benchtest, POC & démonstrateurs
  - DIANA
  - CyberGalaxia, ordinateur quantique et cyber range



# L'IIS CyberWal

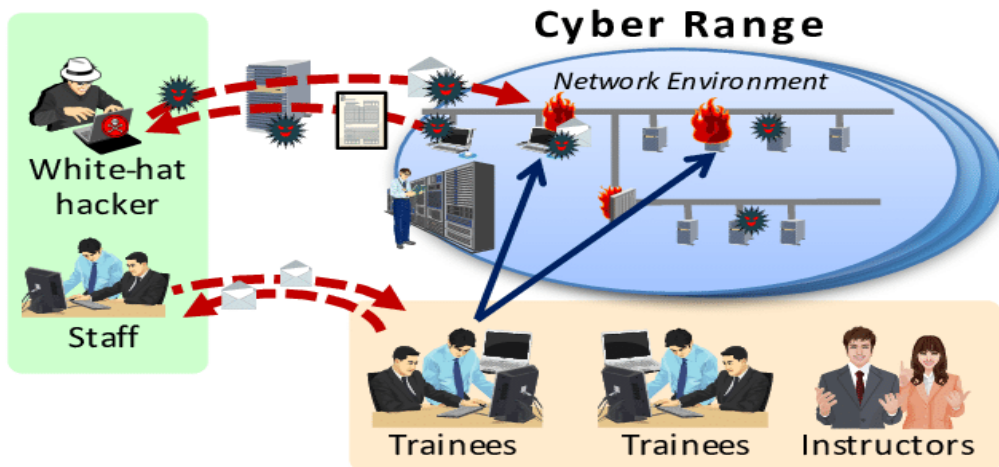
## Un « Hub » de l'innovation

- Des projets de recherche :
  - CyberExcellence
  - AMC3 (Defense-Related Research Action)
  - BeQCI
  - ...
- Formation
  - CyberWal in Galaxia (école éphémère en cybersécurité)
    - Ecole gratuite
    - 5 jours, plusieurs thématiques
    - Plus de 200 participants
  - CyberActive
- Benchtest, POC & démonstrateurs
  - DIANA
  - CyberGalaxia, démonstrateur quantique et cyber range



## Deux démonstrateurs de pointe (projet issu des WP4 et 5)

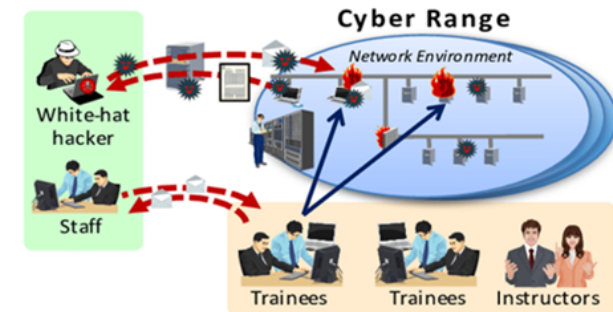
- Les recherches des WP4 et 5 ont motivé deux entreprises (RHEA et Thalès) ainsi que le gouvernement wallon à financer deux démonstrateurs de pointe.
- Hébergés et développés par IDELUX
- Travail sur d'autres projets (CRS2)



# L'IIS CyberWal

## Un « Hub » de l'innovation

- Des projets de recherche :
  - CyberExcellence
  - AMC3 (Defense-Related Research Action)
  - BeQCI
  - ...
- Formation
  - CyberWal in Galaxia (école éphémère en cybersécurité)
    - Ecole gratuite
    - 5 jours, plusieurs thématiques
    - Plus de 200 participants
  - CyberActive
- Benchtest, POC & démonstrateurs
  - **DIANA**
  - CyberGalaxia, ordinateur quantique et cyber range





# L'intégration DIANA

- CyberExcellence devient le premier test center de l'initiative DIANA
- Diana incube des startups qui répondent aux problématiques de l'OTAN
- Nouvelle collaboration avec l'ERM au travers de semestres thématiques
- Le premier projet commun ERM-CyberExcellence est AMC3 (2023) il est issu du WP1
- Collaboration avec le cyber command (DGA à la belge) et premier militaire en thèse dans une université francophone

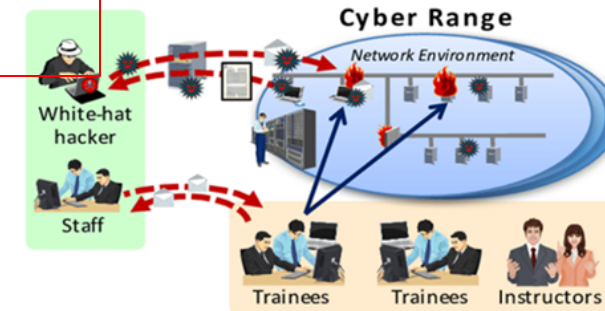


The banner features a blue background with a faint image of a building. On the left, there is a logo for 'Defence Innovation Accelerator for the North Atlantic' which includes the NATO star and the text 'NATO | OTAN'. To the right of this logo, the text reads 'Fostering innovation in NATO : DIANA and the NATO Innovation Fund'. On the far right, there is the logo for 'ROYAL HIGHER INSTITUTE 150-year think tank for DEFENCE'. At the bottom of the banner, the text 'Workshop, 26 June 2023, Brussels (campus Renaissance)' is displayed in white.

# L'IIS CyberWal

## Un « Hub » de l'innovation

- Des projets de recherche :
  - CyberExcellence
  - AMC3 (Defense-Related Research Action)
  - BeQCI
  - ...
- Formation
  - CyberWal in Galaxia (école éphémère en cybersécurité)
    - Ecole gratuite
    - 5 jours, plusieurs thématiques
    - Plus de 200 participants
  - CyberActive
- Benchtest, POC & démonstrateurs
  - DIANA
  - CyberGalaxia, ordinateur quantique et cyber range



# Ecole d'hiver en cybersécurité



Ecole annuelle à Redu réunissant des profils variés : académie, industrie, police judiciaire, entreprise,...

**Plus de 220 participants ! (100 en 2022)**

**Enseignement sur des sujets:**

- non-abordés dans les cursus traditionnels
- choisis suivant des discussions avec des entreprises



# Ecole d'hiver en cybersécurité - IA (Jour 1) et Quantique (Jour 2)



Jour IA organisé par le **CETIC** sur l'interaction IA/Sécurité

Jour organisé par **RHEA** pour sensibiliser sur la thématique quantique



Quantum Potential



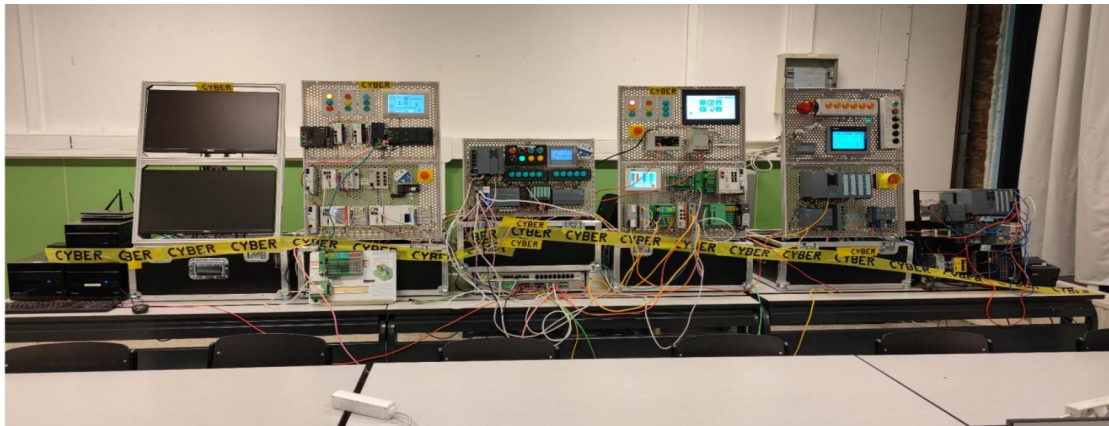
Quantum Risk



# Ecole d'hiver en cybersécurité - Entreprise (Jour 3) et OT (Jour 4)



- Jour Entreprise organisé par l'AdN et **Deloitte** pour sensibiliser aux défis industriels
- Jour OT organisé par **Howest** pour sensibiliser aux challenges de la sécurité de l'OT



# Ecole d'hiver en cybersécurité - Espionnage et sécurité mobile (Jour 5)



- Jour Espionnage et sécurité mobile
- Intervention de la **sûreté de l'Etat** suivi de l'étude de la sécurité des application mobiles organisé par **Nviso**



## CyberWal in Galaxia – programme 2024

- Lundi : IA & cyber
- Mardi : Quantique
- Mercredi : Journée de l'industrie
- Jeudi Block Chain et cloud
- Vendredi : Hackathon & police judiciaire

# CyberWal

## UNE RÉUSSITE nationale avec une ambition internationale

- **Expertise consolidée**
  - Une approche désormais **unifiée et centralisée**
  - Cyber Excellence est devenu un véritable **pôle d'excellence**
- Notre ambition : s'étendre à l'international
- **Crédibilité et légitimité**
  - Projets européens (Horizon Europe,...)
  - Fédérations de recherche (collaborations nationales et internationales)
- **Collaborations stratégiques**
  - **AWEX & WBI** : valorisation de notre expertise à l'étranger (événements, mises en contact)
  - **NCP** : ciblage des projets européens et thématiques stratégiques, partenaires internationaux, conseils
  - **ECCC** : mise en relation avec des acteurs pertinents en cybersécurité



# Canada

## Positionnement stratégique

- Eligibilité à participer aux appels du programme “Horizon Europe”, programmes bilatéraux
- Importance de se positionner rapidement sur ce nouveau marché
- Visibilité et opportunité sur le continent américain
- Positionnement stratégique
- Forum InCyber
- IMC2 : taille similaire à notre consortium

# Canada

## Mission CyberExcellence

- Mission à Montréal du 28 octobre au 1er novembre
- Organisation grandement facilitée par le WBI
- Délégation de 15 personnes
- Echanges prévus avec des chercheurs, des industriels (en collaboration avec l'AdN) et des centres de recherche canadiens
- Programme :
  - Participation au forum InCyber
  - Rencontre avec IMC2
  - Rencontre avec Concordia

# Allemagne

## Positionnement stratégique

### **Mission de prospection de Cyber Excellence en Bavière et Saarbrücken (mars 2025 )**

- Centres de recherche prédominants, écosystème dynamique d'excellence mondiale
- Proximité géographique
- Différentes possibilités de financement
- Bons résultats en termes d'appels à projets européens remportés

#### **Nos intérêts :**

- CISPA Helmholtz Center for Information Security
- DFKI
- Fraunhofer

# Participation à des événements à portée internationale



- Participation à de nombreuses conférences internationales (30) :
  - IETF, NSDI, **BlackHat**, ISoLA, NDSS,...
- 89 publications par les chercheurs financés CyberExcellence (13 en 2022)
- Participation à 60 activités ayant une dimension internationale



# CyberExcellence rencontre la Flandre

- Projet fédéral AIDE (2023-2026)
- Liens fort entre l'IA et la cybersécurité
- Avec IMEC et KULEUVEN
- Construit sur les WP1, 2 et 4



# European AI week (collaboration Wallonie + Flandre)

## THE EUROPEAN AI WEEK

MARCH 27-31  
2023 BRUSSELS

### Towards tech convergence



AI WEB 3 CYBER DATA E-SKILLS

28.03.2023 09:30 - 18:00 + RECEPTION

FPS BOSA

### Track Cyber Security

The digitalization is ever more present in our daily environment. Let's make Belgium one of the least cyber vulnerable countries in Europe!



Book your spot: [aiweek.ai4belgium.be](https://aiweek.ai4belgium.be)

Participation à la track  
Cybersecurity

# SMARTNATION

AI4Belgium Blockchain4Belgium  .be

# ERASMUS MUNDUS CYBERUS



- ULB, Université de Bretagne Sud, TalTech, Université du Luxembourg
- Recrutement : 128 étudiants sur 4 ans, équilibre UE/reste du monde
- Partenaires : 47 internationaux, recherche, industrie, enseignement
- Doctorats : 2 financés par CYBEREXCELLENCE, co-tutelle avec UBS
- Réseau industriel : 50 partenaires principaux, stages, séminaires
- Statistiques : 600 dossiers, 200 évalués, 60 interviews, 30 bourses



# Conclusion : impact sur la formation au sein des universités

- Multiplication des TFE dans le domaine
- Création d'un poste de Professeur à Mons
- Renforcement des liens avec l'enseignement non universitaire
- Création d'option Cybersécurité: exemple UCLouvain
- Interventions dans d'autres filières (UX, médecine, ...)

# .AGORIA

**Eric Van Cangh**

Agoria



# Cyber Innovations

BSDI / CMiB  
To CMiB4DEF

**.AGORIA**



# AGENDA

- BSDI in nutshell
- AGORIA Cybersecurity building blocks
  - Cyber Aware Programme (CAP) - Agoria Connect – Digital@Services
  - CMiB
- Innovative collaboration Public / Private
  - Collaboration Path for the Cyber Command
  - CMiB4DEF – Triparties – CMiB / BSDI and Defence / CyCom
- Interactions with CMiB4Talent FG and CMIB4ICS/OT FG
- Conclusion

# Belgian Security & Defence Industry

Role, outlook and challenges

**Technology**



**to protect**



**society**



Cluster: ASCD  
Security & Defence

# Aero Space, Safety, Security, Cyber - Defence



AERONAUTICS



SPACE



SAFETY



SECURITY



CYBER



DEFENCE

Embracing technology  
Embracing ambition

**.AGORIA**

# Mission

**.AGORIA | BSDi**

Belgian Security & Defence Industry



Security



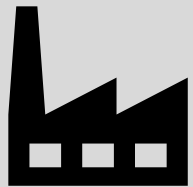
Defence

Provide and maintain equipment  
for use in a **very demanding environment**  
where **reliability is critical**,  
in order to  
**safeguard and defend**  
the **society**  
of/against threats of human nature

Technology to protect society

# 2022 in numbers...

## SECURITY & DEFENCE



**115**



**5.800 (15800)**



**1,98 (4,75)**

**B€**

90%



Flanders	Wallonia	Brussels
51	55	9
981	4 164	640
296 M	1 556 M	129 M

# A BDSI Members 170+



Jeroen Poesen  
BGL BDSI

### AGORIA BSDI Members

Security and Defence industry Service providers

**AGORIA BSDI** Belgian Security & Defence industry

### Research and Technology Organizations

Partners

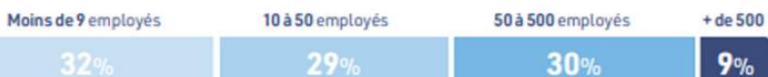


# BSDI in Nutshell

## About Belgian Security & Defence Industry (BSDI)

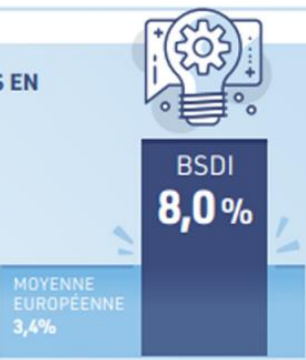
BSDI connects and unites **Agoria members and other companies and stakeholders** with a specific interest in **Security or Defence technology**. Companies range from material production over component manufacturing, conceiving mechanical, electronic or digital systems till realizing final assembly and integration, all for specific law enforcement or military use. We share **relevant information** on technology, regulations and business opportunities promoting **bench marking** and best practices. We bring together **customers and providers** along the entire supply chain, from material manufacturers till the end customer, through dedicated sessions, with the aim to stimulate growth and **business development** to the benefit of all.

UNE GRANDE DIVERSITÉ DANS LA TAILLE DES ENTREPRISES QUI DÉMONTRE LA STABILITÉ ET LE DYNAMISME DU SECTEUR



### INVESTISSEMENTS EN R&D

Le secteur étant porté sur les technologies de pointe, les entreprises investissent en moyenne **8% de leur chiffre d'affaires** en recherche et développement.



Les entreprises du secteur peuvent se targuer du **dépôt de**

**46 BREVETS**

en l'espace de quatre ans.

## 15.400 EMPLOIS DIRECTS

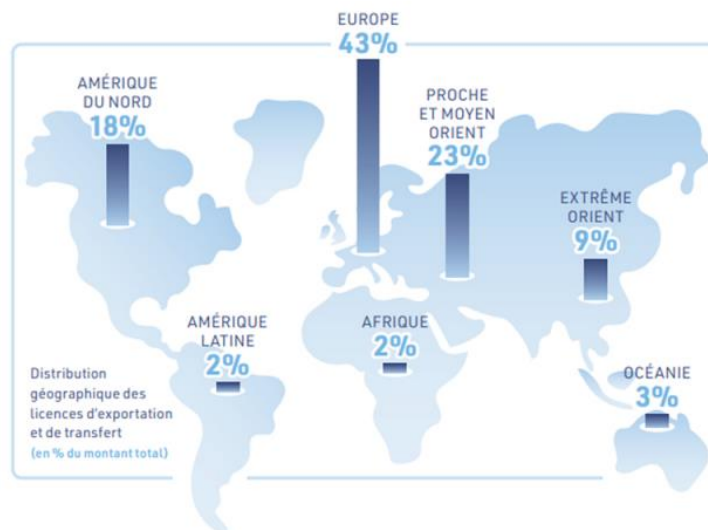
SECTEUR DE HAUTE TECHNOLOGIE

**20%**  
D'INGÉNIEURS



AVEC UNE FORTE ASSISE INDUSTRIELLE

**38%**  
D'OUVRIERS



# AGENDA

- BSDI in nutshell
- AGORIA Cybersecurity building blocks
  - Cyber Aware Programme (CAP) - Agoria Connect – Digital@Services
  - CMiB
- Innovative collaboration Public / Private
  - Collaboration Path for the Cyber Command
  - CMiB4DEF – Triparties – CMiB / BSDI and Defence / CyCom
- Interactions with CMiB4Talent FG and CMIB4ICS/OT FG
- Conclusion

# Agoria Cyber Security Building Blocks

**Cyber Made in  
Belgium (CMiB)**

**Digital@Services**

**Cyber Aware  
Programme (CAP)**

**AgoriaConnect**

# Cyber Aware Programme (CAP)

<https://www.agoria.be/cyberstart>

**Cyber Aware Programme (CAP)**

**Cyber Aware: WHAT?**

1. Email training "Virtual CS Coach for SME's"
2. Promotional tactics that will help drive traffic:
  1. Paid online & social media campaign
  2. Printed postcard action
  3. Presence at events with hacking demo
  4. Partnership with five IP sector partners through video (Sirris)
3. NL & FR - Launch January 2023

**Cyber Aware: WHY?**

- Ensuring the business continuity of Belgian companies and organisations in an increasingly unstable and threatening environment
- By 2025, 95% of member companies have and implement a cybersecurity plan in self-assessment of the business impact in terms of finance, R&D, operations and compliance
- Shape the right context to strengthen the Belgian cybersecurity industry



**Emilie Parthoens**  
Project Officer



**Raphael Slachmuylders**  
Project Officer



**Arnaud Martin**  
Expert Digital & ICT  
Standardisation



**Eric Van Canghai**  
Business Group Leader Digital

**.CYBERSTART**

La cybersécurité n'est plus une option, mais une nécessité absolue!  
**Il est moins une !**  
Améliorez vos connaissances en matière de cybersécurité et offrez à votre entreprise et à vos clients la sérénité dont ils ont besoin.

**.AGORIA** **WALHUB** **Cyberwal by digital wallonia**

Inscrivez-vous à notre e-tutoriel hebdomadaire et profitez de ses avantages

- Gratuit
- Pas à pas
- Explication claire
- Gain de temps et d'argent
- Équilibre entre théorie et pratique
- Préparation à la nouvelle législation européenne

**.CYBERSTART**

Cybersecurity is niet langer een optie, maar een absolute noodzaak!  
**Het is 2 voor 12!**  
Vergroot je kennis over cybersecurity en geef je bedrijf en je klanten de nodige gemoedsrust.

**.AGORIA** **sirris** **samen voor #sterkondernemen**

Onze wekelijkse e-tutorial in een notendop

- Gratis
- Stap voor stap
- Helder uitgelegd
- Bespaar tijd en geld
- Evenwicht tussen theorie & praktijk
- Klaar voor nieuwe Europese wetgeving



# New e-learning module (based on cyberstart)

<https://www.agoria.be/cyberboost>

Cyberboost  
Accélérons la cybersécurité de votre PME

Inscrivez-vous à ce cours en ligne

AGORIA Academy

WALHUB

Co-funded by the European Union

Wallonie

A man in a white shirt and black trousers, wearing a red cape, is running while holding a laptop. The background is a plain, light-colored wall.

Cyberboost  
Met volle kracht naar een cyberveilige kmo

Schrijf u in op de online cursus

AGORIA Academy

WALHUB

Co-funded by the European Union

Wallonie

A man in a white shirt and black trousers, wearing a red cape, is running while holding a laptop. The background is a plain, light-colored wall.

SUPPORT



Agoria Commitment:  
95% Members CS PLAN

End of 2025

# AGORIA CONNECT

<https://www.agoriacconnect.be/fr/>

**SHOW ROOM OF DIGITAL SUPPLIERS**

SNEL EEN SPECIALIST IN CYBERSECURITY VINDEN?  
**CLICK & CONNECT**



.AGORIANCONNECT

TROUVER RAPIDEMENT UN SPÉCIALISTE EN CYBERSÉCURITÉ ?  
**CLIQUEZ & CONNECTEZ-VOUS**



.AGORIANCONNECT


<https://www.agoria.be/agoriacconnect-vind-uw-cybersecurity-specialist>

<https://www.agoria.be/agoriacconnect-trouvez-votre-specialiste-en-cybersecurite>


# Agoria Digital@Services

## Cyber security services for Agoria members:

- A more individual follow-up by our experts related to CS regulations and directives at European level
- > **Working Group**
- **Master classes**
  - Cyber Security in 30 steps (NL/FR + UK)
  - **NIS 2**
- **Agoria Red Line**
- Development of a FAQ on our cybersecurity webpage




### The WG team



Marc Cumps



Ilse Haesaert



Arnaud Martin

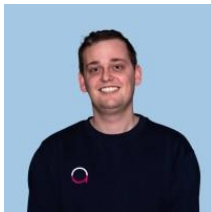


Bart Meert

CS Regulation/Directive	Agoria Expert
Cyber Security Act (CSA)	Arnaud Martin
Radio Equipment Directive (RED)	Marc Cumps
Cyber resilience Act (CRA)	Arnaud Martin
Network and Information Security Directive (NIS2) + CER	Ilse Haesaert & Arnaud Martin
Electronic Identification Authentication and trust Services (eIDAS)	Bart Meert

Classification: Internal

10



**Maximiliaan Muylaert**  
Digital Expert

# AGENDA

- Agoria Cyber Security Updates
  - Cyber Aware Programme (CAP) - Agoria Connect – Digital@Services
  - ➔ ▪ CMiB updates
    - CMiB Steerco 2024-2025 Priorities
    - Focus Group Defence
    - Focus Group Talent
    - Focus Group Manufacturing (ICS/OT)
- NIS 2.0 Updates

# Agoria Cybersecurity Building Blocks

Cyber Made in  
Belgium (**CMiB**)

Digital@Services

Cyber Aware  
Programme (**CAP**)

AgoriaConnect

# Introduction - Video CMiB

## CMiB – Cyber Made in Belgium

### Start:

- Agoria Initiative – started in 2021
- Part of the Agoria Digital Framework
- Represent the Cyber security economic sector next to



### Vision:

Be the **privileged platform** giving the cybersecurity service providers in Belgium a face, a voice and a listening ear to all relevant stakeholders (governments, companies, and citizens at large).

**Mission:** Remove barriers and facilitate creation of enablers for cyber resilience uptake in Belgium supporting the digitalization of the society at large.

18

Classification: Internal

## Agoria's business group = Cyber Made in Belgium (CMiB)

### • 3 Priorities

- CS players are recognized as **critical sector**
  - Socio-Economical Study on Cyber Security
  - CS industry positioning in our Belgian defense programs
- Increase the **Cyber Resilience** of our Industries  
Commitment: 95% of Agoria members have a CS plan in 2025
  - Influencing Business Leaders – Talks & presentations
  - Cyber Start ([www.cyberstart.be](http://www.cyberstart.be))
  - Cyber Talent&Skills
- Boost CS innovation in the **manufacturing Sector - ICS/OT**



### • 3 Focus Groups

- Defense : CMiB4Def (P1)
- Education : CMiB4Talents (P2)
- Manufacturing : CMiB4ICS/OT (P3)

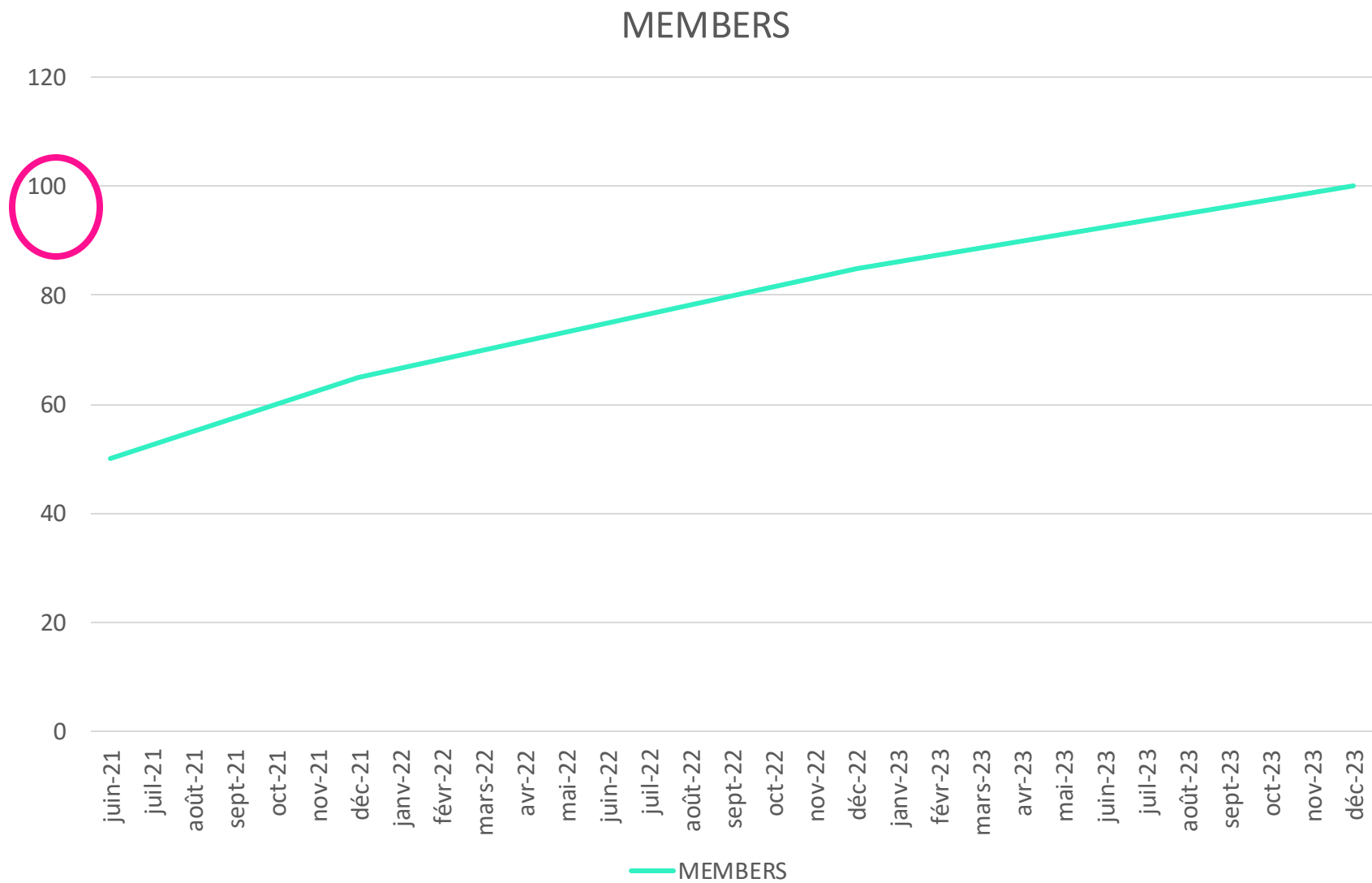
• **70+ Agoria Members with Cyber Offering Products and Services ([agoriacconnect.be](http://agoriacconnect.be))**



Classification: Internal

[local link video](#)

# CMiB members progression





# Welcome to our new CMiB members 2023/2024

axians

NAVAL  
GROUP

Cresco  
Cybersecurity



ABOUTIT

EONIX  
Sensitive IT, Reliable Partner

TREND  
MICRO

SIEMENS

soterics



VIGILANTOPS

CRANIUM

HeadMind Partners

( expleo )

kyndryl

Inetum  
REALDOLMEN

easi

AXS | GUARD

PRIVACY  
PRAXIS

PLAY IT  
GAME BASED LEARNING



WAVESTONE

Schneider  
Electric

CYBER  
SECURITY  
MANAGEMENT

nomios

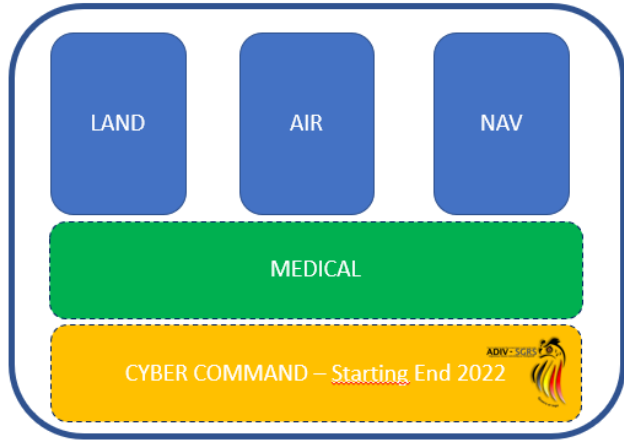
# CMiB – Partners



# AGENDA

- BSDI in nutshell
- AGORIA Cybersecurity building blocks
  - Cyber Aware Programme (CAP) - Agoria Connect – Digital@Services
  - CMiB
- Innovative collaboration Public / Private
  - Collaboration Path for the Cyber Command
  - CMiB4DEF – Triparties – CMiB / BSDI and Defence / CyCom
- Interactions with CMiB4Talent FG and CMiB4ICS/OT FG
- Conclusion

# March 2022 – The needs



Belgian industries

Cyber Security Offering



CMIB4DEF

Cleared



DEFENSIE  
LA DÉFENSE



Synergies

- Platform representing the Belgian industries
- With a Cyber Security focus
- Speaking the same Language (taxonomy)
- Have a NATIONAL security clearance



**CyBOK** Home At a Glance Knowledgebase People News & Events Resources Use Cases

For the community, by the community

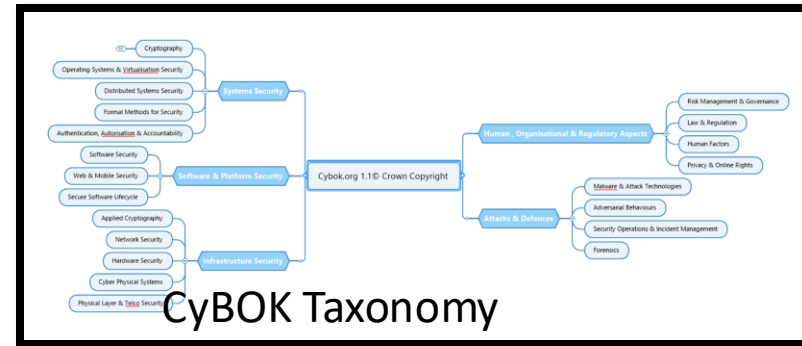
115 Developed by world experts

International effort

21 Knowledge Areas

Free to use for everyone

In partnership with: University of BRISTOL, Department for Digital, Culture, Media & Sport, UK CYBER SECURITY COUNCIL



CyBOK Taxonomy

(<https://www.cybok.org/>)

# March 2022 - Governance CMiB 2.0

## Cyber Made in Belgium (CMiB)

### Composition

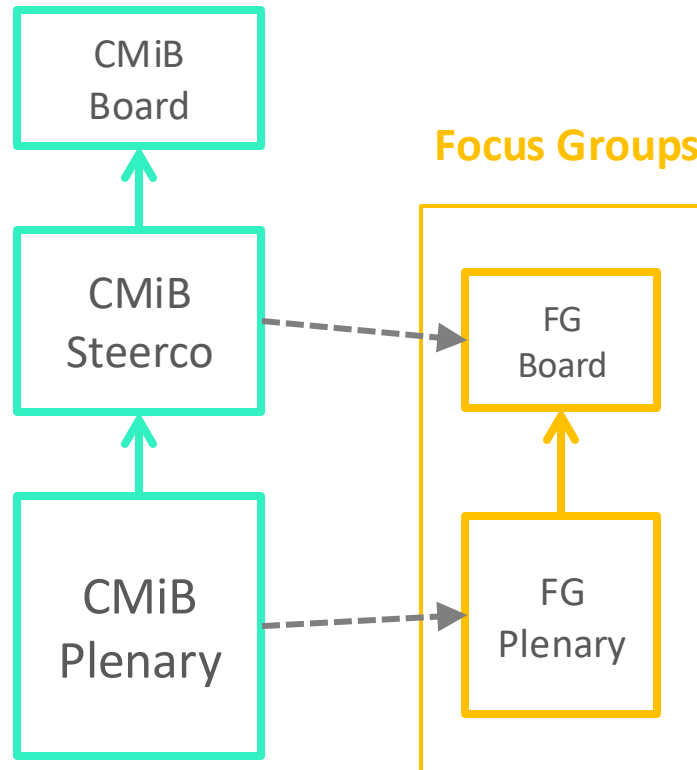
- Agoria Cyber BG leader
- CMiB Chair + Vice-Chair

### Composition

- Enablers and sponsors of CMiB initiatives
- 10 members elected for 2 years
- Frequency
- Every 6 weeks

### Composition

- All CMiB members + Partners
- ### Frequency
- Bi-annually + event-based



### FG Missions

The focus group missions or objectives are:

- to be part on the 4 CMiB Priorities
- to reinforce the Cyber resilience within Belgium
- To **address a global problematic** or a thematic that CMiB members could contribute

### ... and the FG Board will:

- Define the deliverables, the action plan and success metrics to achieve their mission
- Document the conditions for access (accreditations..), elections
- Invite the CMiB Members on the plenary session
- Report to the CMiB steerco the progression of the discussions
- Send to the CMiB Steerco the agenda upfront 2 days before the FG Board session

# March 2022

**.AGORIA**

## Synergies Defence - Industries



**QUEL AVENIR POUR L'ARMÉE BELGE ?**

37:35 "Une initiative en cours avec Agoria, Cyber Made in Belgium , qui vise à développer cette base industrielle (Coopération) en Belgique dans le domaine Cyber"

<https://www.in24.be/2022-03-28/pour-info-quel-avenir-pour-larmee-belge>



# June 2022 – 1st CMiB plenary session

## CMiB - The Agoria Cyber Business Group

Kick off – Plenary Session

29/06/2022

Embracing technology  
Embracing ambition



## A voice from the CMiB partners



Beltug

WOMEN  
4CYBER  
EUROPEAN CYBER SECURITY ORGANISATION

Embracing technology  
Embracing ambition

.AGORIA



# Cyber Month – October 2022



Partnership CMiB-Defence  
at Cyber Command kick off



# Nov 2022 – 1<sup>st</sup> CS Socio-economic study

4000 openstaande vacatures, 100 cyberaanvallen per dag



Eric Van Canghai (Agoria), Dominique Demonte (Agoria), Ludivine Dedonder (MOD), Kolonel Pierre Cipari (Defense), Miguel Debruycker (CCB), Filip Verstockt (Orange Cyberdefense)

.AGORIA

Special thanks to our sponsors (CMiB Partners and CMiB Steerco)



Classification: Internal



First socio-economic study on the cyber security sector in Belgium

November 2022

Embracing technology  
Embracing ambition

.AGORIA



# Nov 2022 - 1<sup>st</sup> CS Socio-economic study

**.AGORIA**

## Belgium's cyber security ecosystem

Cyber security providers and services

	Cyber security providers	Cyber security services
Generalists	Organizations that offer multiple cyber services	Consulting and audits
Consultants	Consultants regarding cyber security services	Certification and accreditation
Integrators	Organizations that integrate products and/or services in industrial environments	Security products (SIEM, HIDS, SIEM, Intrusion Detection)
Specialists (the players)	Organizations that focus on one specific cyber domain	Security solutions (Integration & Engineering)
Specialists (the players)	Organizations that focus on one specific sector or vertical (e.g. telecom, public services, insurance)	Managed security services (Monitoring, Detection & Response)
Specialists (the players)	Organizations that mainly offer cyber education and certifications	Incidents and malware handling (CERT, CERT)
Training, education and certification entities		Security training, education and certifications
Innovators	Start-ups and scale-ups that focus on innovative product or service	Research, development and innovation

Overview main schools that offer cyber courses (incl. online programmes)

© AGORIA 2022

**.AGORIA**

## The Belgian cyber security landscape (2021)

**441 Companies**

441 companies active in cyber security

- €1.58 billion Total sales figure in cyber security
- €600 million Total value added in cyber security
- 0.1% of the Belgian GDP
- 6,405 FTEs Total employment in cyber security

Women: 19% | Men: 81%

50+ years old: 10% | 30-50 years old: 55% | 18-29 years old: 35%

**WOMEN 4 CYBER**

Classification: Internal

# Nov 2022 - 1<sup>st</sup> CS Socio-economic study

## The Belgian cyber security landscape (2021)



Classification: Internal

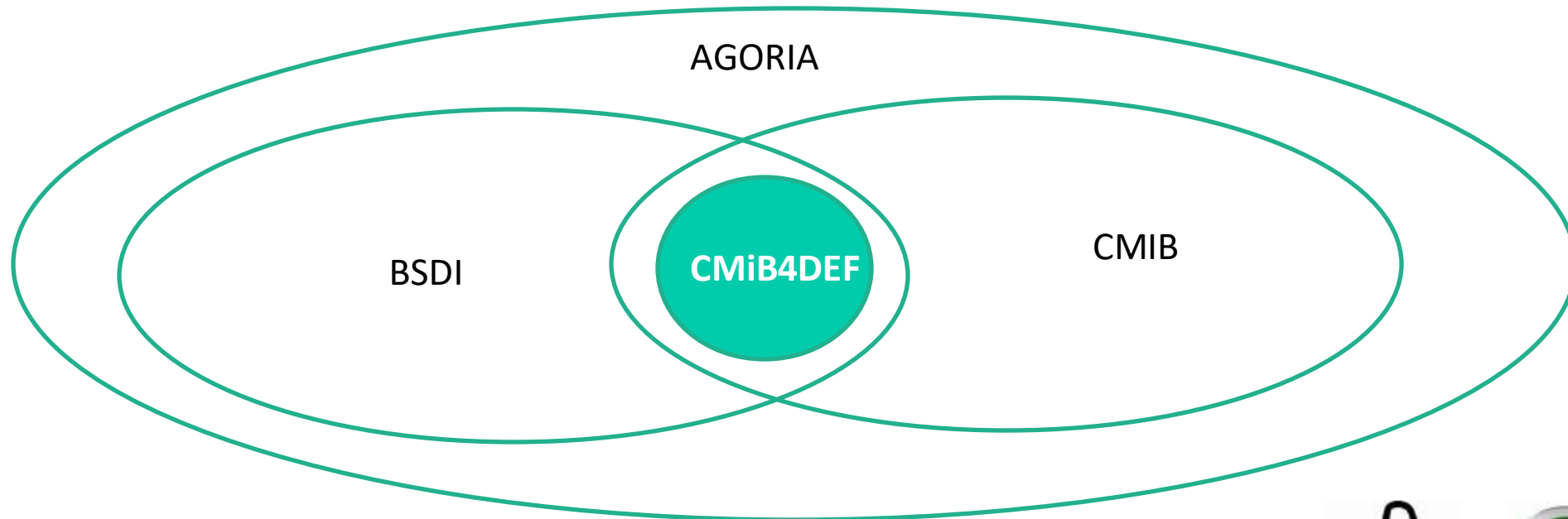
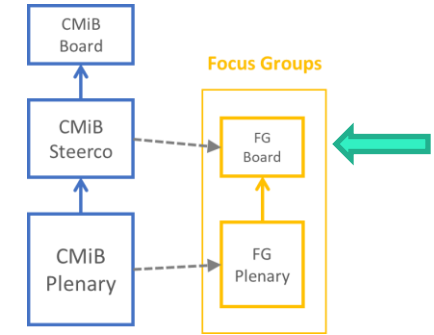
## Five recommendations around three themes

<b>Development of talent and education curricula</b>	1. Increase our country's overall capacity for higher cyber education, and spotlight cyber security careers
<b>Awareness</b>	2. Launch regional and national awareness campaigns, targeting management levels in the public and private sector, and the different governments 3. Inspire sector federations and governments to set a cyber security plan objective for 2025
<b>Growth roadmap for the sector</b>	4. Invite all regions and other stakeholders to consider supporting cyber start-ups and scale-ups 5. Promote export trade and facilitate foreign investments in Belgian cyber security skills and services

Classification: Internal

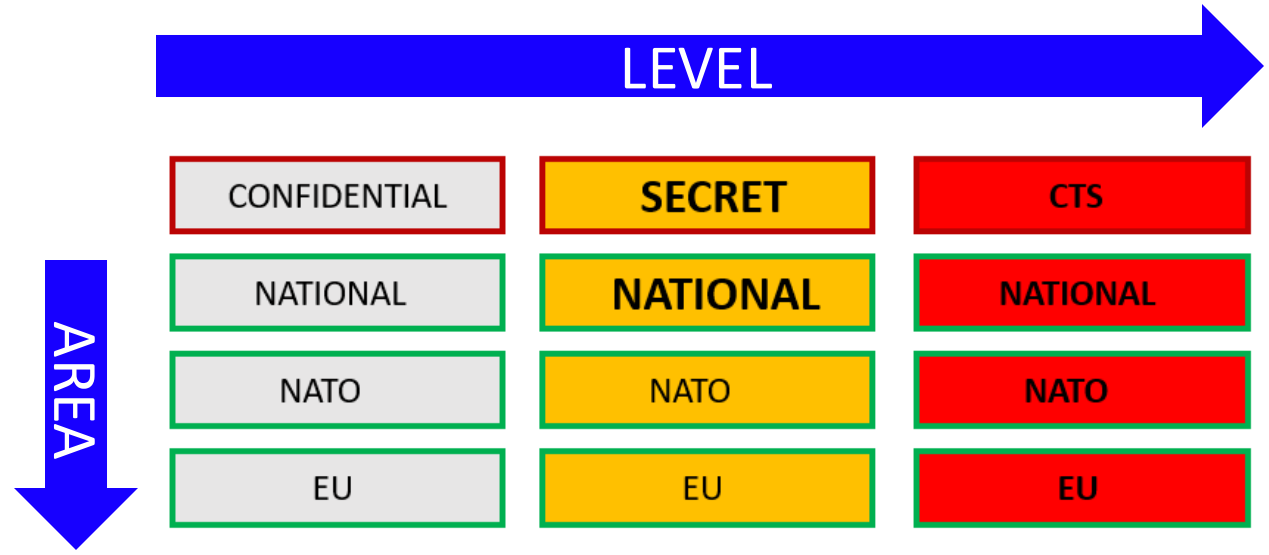
# Nov 2022 - Define CMiB4DEF Board GOV

- Governance of CMiB Board : 8 seats
- Identify the candidates CMiB4DEF plenary



# Regulations – security clearance – CMiB4Def

- Classification Levels



**NATIONAL SECRET is MANDATORY for the CMiB4DEF participants**

The security level can be increased in the futur if requested



# December 2022 – CMiB4DEF kick-off



CMiB4DEF  
Kick-off

December 1<sup>st</sup> 2022

Embracing technology  
Embracing ambition

*The Cyber Made in Belgium*  
**'Tis the Season!**  
*This is*

First Kick-off of the CMiB4DEF  
A cocktail for the 2<sup>nd</sup> CMiB plenary

**.AGORIA | BSDI**  
Belgian Security & Defence Industry

December 1<sup>st</sup>  
14:30 – 20:30

**.AGORIA**



# Synergies (vision 2022)

CMIB4DEF

- 3 streams – Synergies with Industries



**DEFENSIE**  
**LA DÉFENSE**

Cyber Resilience Force (CRF)



WG2

Develop Cyber Domain Priorities  
*(based on Cybok taxonomy)*

Cyber Defence Skills (Technical)



WG4

# March 2023 – CMiB4DEF Workshop



A screenshot of the CyBOK website homepage. The header includes the CyBOK logo and navigation links: Home, At a Glance, Knowledgebase, People, News &amp; Events, Resources, and Use Cases. The main content area features five key statistics: 'For the community, by the community' with a network icon; 'Developed by world experts' with the number 115; 'International effort' with a globe icon; 'Knowledge Areas' with the number 21; and 'Free to use for everyone' with a padlock icon. At the bottom, it lists partnerships with the University of Bristol, the National Cyber Security Centre, and the UK Cyber Security Council.

CMiB4DEF  
Board



# CMiB4DEF Board operational 2022-2024

**.AGORIA | BSDI**  
Belgian Security & Defence Industry

Board presentation

**Anne-Marie Covemaeker (PROXIMUS)**



**VP**

- Anne-Marie Covemaeker is Product Owner Lead Federal Government in the Proximus Enterprise Business Unit.
- She owns a Master in Business Economics, Production and Logistics and an Academic Bachelor in Psychology.
- In her current role, she is responsible for all commercial and service delivery activities for the Federal Government.
- She has been active in the Proximus Group for 24 years and has a background in sales, delivery and operations.
- Her domain of expertise is End-to-End ICT servicing for the Public Sector, including Cyber Security Servicing.

**.AGORIA | BSDI**  
Belgian Security & Defence Industry

Board presentation

**Olivier Croix (THALES BELGIUM)**




**VP**

- After 20 years working in the space domain for Ariane launchers, Olivier switched to the Defence and Cyber-Security domain.
- He managed the development of the Thales Belgium Cryptographic product portfolio protecting information classified up to Secret Level.
- Olivier is Cyber Product Line Manager in charge of the product range and services strategy.
- Together with the Thales Cyber Defence experts and the local cybersecurity actors, Olivier prepares the new products solutions compliant with emerging threats.

**.AGORIA | BSDI**  
Belgian Security & Defence Industry

Board presentation

**Steve De Vos (OCD)**




- Steve De Vos is Sales Manager at Orange Cyberdefense responsible for the Public Sector (Healthcare, Government and Education). Steve is with Orange Cyberdefense (before SecureLink) for more than 17 years and leads a team of Account Managers with a focus on the large organizations in the Public Sector. He has more than 25 years of experience in different commercial roles at Xerox, CTG, Real Software and others.
- Steve holds a Masters Degree of Applied Economics from the University of Antwerp and is fluent in Dutch, French and English.
- When he is not working, Steve likes to play tennis and golf. Living in Antwerp he is also a big fan of R. Antwerp FC. Steve enjoys travelling, cooking and enjoys a good glass of wine

**.AGORIA | BSDI**  
Belgian Security & Defence Industry

Board presentation

**Michael Raison (APPROACH)**



**Pr**

- Consultant for Approach, a pure player in the cybersecurity.
- Michael Raison is a trained and certified specialist having 20 years experience in Management roles, Lead auditor and coaching for cybersecurity.
- Currently Head of Compliance & Risk and CISO for Sabca group, and advisor for many companies in the defence & aerospace sector in Belgium.
- He is currently building and reinforcing several networks and practices on the defence and aerospace industrial base, including the drive of some emerging hot topics like NIS, CMNC and industry cybersecurity.
- His role encompasses cybersecurity perspective but also many compliance items that are in close link with cybersecurity at board level, including trade compliance, physical security, business ethics, sustainability where he usually acts as a coordination central piece as Head of Compliance.

**.AGORIA | BSDI**  
Belgian Security & Defence Industry

Board presentation

**Patrick Okerman (INNOCOM)**




**VP**

- Patrick Okerman is the lead for the Essential Security Interests (ESI) program at INNOCOM, is currently conducting for Cyber Command (Belgian Defence).
- He defined the scope and the approach of this program that has also the ambition to support the sharing of cybersecurity knowledge and experience between Defence, Government agencies, Industry and Academia.
- Patrick participated in the founding of INNOCOM back in 1998, after having been Delivery Manager at IBM Professional Services.
- He has been responsible for successfully realizing a multitude of missions at INNOCOM, in several management positions. His experience is focused on Digital Strategy & Transformations, IT Governance & Delivery and Innovation.
- He holds a Master degree in Computer Science from the University of Brussels as well as a degree in Business Administration from the University of Leuven.
- He is also active as an independent court expert for ICT subjects

**.AGORIA | BSDI**  
Belgian Security & Defence Industry

Board presentation

**Kurt Ceuppens (NVISO)**



- Kurt Ceuppens is CEO at NVISO, a firm he co-founded in January 2013.
- NVISO is a pure-play cyber security services firm with a mission to safeguard the foundations of European society. NVISO has offices in Brussels, Frankfurt, Munich, Vienna & Athens and is currently 280 people strong.
- At NVISO, Kurt is responsible for setting out the strategy and ensuring its proper implementation. Next to this, Kurt manages the relation with NVISO's key accounts in the Benelux region and.

Classification: Internal

# March 2023 - FIC 2023

**.AGORIA**



**CMiB**  
**“Cyber Made in Belgium”**  
A voice for the Belgian cyber security industry  
**FIC 2023 – Booth H4**

Classification: Internal

**La ministre Dedonder rend visite à Agoria** FIC 2023  
**à l'International Cybersecurity Forum**



Publié le 02/04/23 f t in e m

La cybersécurité est au cœur de l'actualité. C'est pourquoi Agoria a participé au Forum International de la Cybersécurité (FIC) à Lille avec un pavillon belge réunissant quelques entreprises de la communauté Cyber Made in Belgium (CMiB), le business group cybersécurité d'Agoria.

<https://www.agoria.be/n/digitalisering/cybersecurity/agoria-op-vrucht-minister-dedonder-op-international-cybersecurity-forum>

Classification: Internal

# March 2024 - FIC 2024 RETROSPECTIVE

- Biggest representation – 20 entities / 182 people registered in the Belgian Dashboard
- Huge Program with dedicated thematics (defence / industries / talents skills)
- Cmib evenings – Networking activities (kick off evening / VIP evening / GALA evening..)

**.AGORIA**

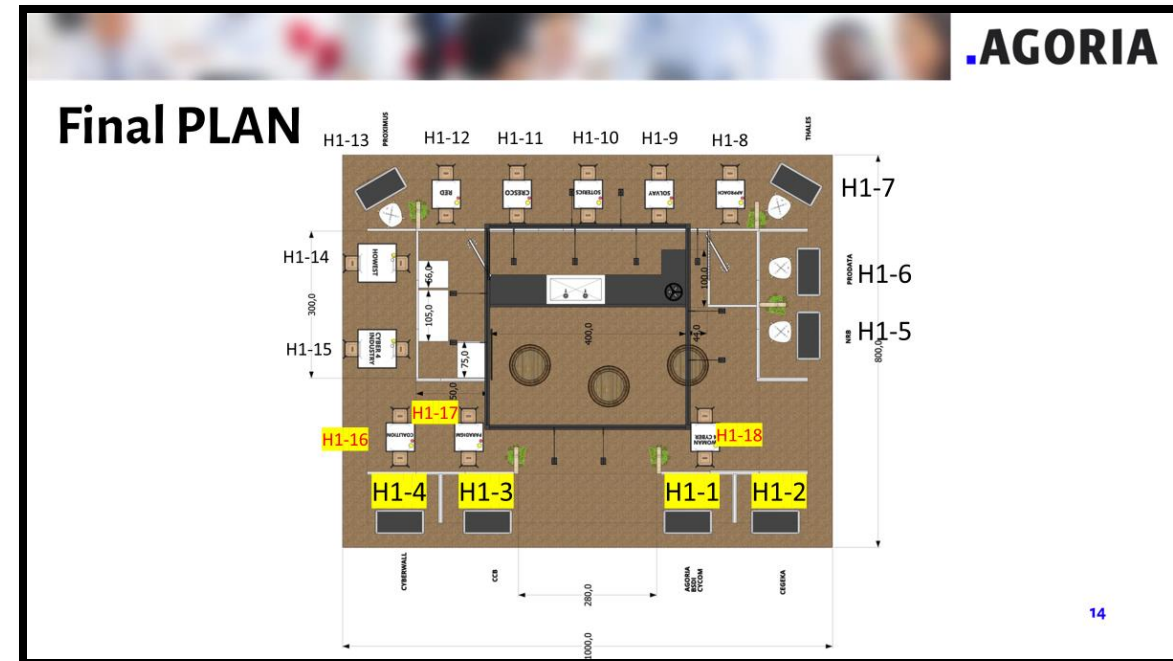
## Fic 2024 – (status 27/02/2024)

**Belgium Delegation (on the pavilion)**

**Sponsors:**

TLP:AMBER - Limited disclosure, restricted to participants' organizations.

11





# March 2024 - FIC 2024 RETROSPECTIVE

## Booth Agoria/ BSDI / Defence



Big BAR

(with Triple Karmeliet and Maredsous^^)



PRIVATE VIP ROOM

Panneaux 01b

H2473 mm x L985 mm  
-> Visuel CMiB + BSDI 1/2

H2473 mm x L489 mm  
-> Visuel CMiB + BSDI 2/2

H2473 mm x L985 mm  
-> Cyber Command

 A detailed graphic layout of the booth panels. The layout is divided into three main sections:
 

- Left Panel (H2473 mm x L985 mm):** Features the CMiB logo with the tagline "Cyber Made in Belgium" and "A voice for the Belgian cyber security industry". Below this is a QR code and the text "Agoria Cyber Security Services". A list of services includes "Cyber attack Hotline" (Agoria REEDline: tel: +32 2 706 88 77), "Basic training" (Cyberstart.be - free e-tutorial), and "Advanced training" (NIS 2.0 Academy - Cyber Security in 30 steps). It also lists "Companies offering Cyber Security technologies in Belgium" and "Belgian Federal Public Cyber CMiB partners" (Cybersecurity Belgium, COALITION). The CMiB Steering Committee members listed are Cyberdefense, Microsoft, TONON Y, APPROACH CYBER, cegeka, WAVESTONE, THE PURE GROUP, NIVISO, RHER, and NOCIA. The Agoria logo is at the bottom.
- Middle Panel (H2473 mm x L489 mm):** Features the Agoria BSDI logo with the tagline "Belgian Security & Defence industry". It includes a QR code, a photo of a fighter jet, a photo of server racks, and a photo of a person using a computer. The Agoria logo is at the bottom.
- Right Panel (H2473 mm x L985 mm):** Features the Cyber Command logo with the tagline "CYBER COMMAND PROTECT, DEFEND, COLLECT AND FIGHT". It includes a QR code and the text "CYBER FORCE THROUGH PARTNERSHIPS". The logo for "DEFENSE LA DÉFENSE" and the CMiB logo are at the bottom.



# March 2024 - FIC 2024 RETROSPECTIVE





# Fic – defence DAY – 26/03/2024

Programme :

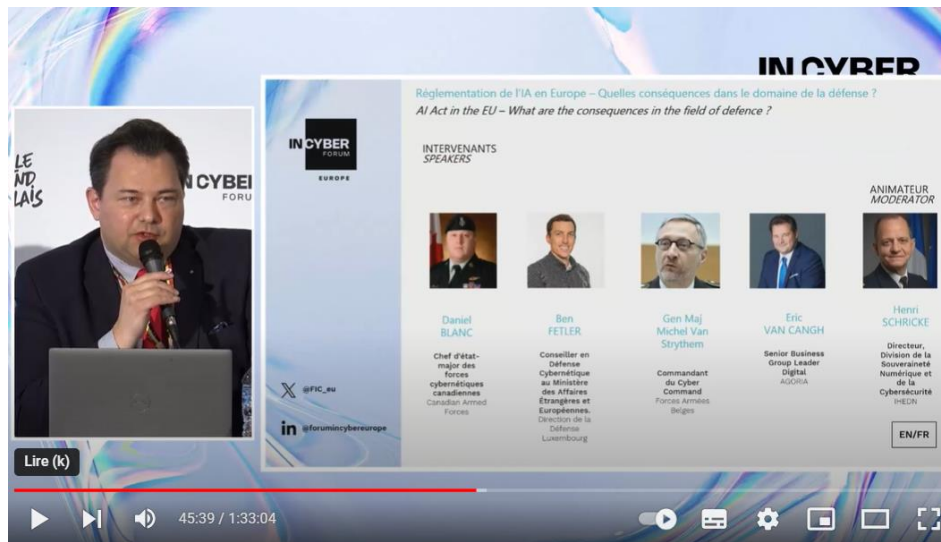
11 :00-13 :00 table ronde avec le cycomBE , diplomatie BE , industrie BE , officiel FR, Cycom LUX

13 :00 -13 :30 VIP lunch devant notre stand belge

14 :00 – 16 :30 BELUX cyber defence

16 :30-17 :30 présence au pitch européen – avec les industries



17 :30-18 :00 réception visite du stand belge



30 INCYBER Règlementation de l'IA en Europe – Quelles conséquences dans le domaine de la défense




# 16/04/2024 – New cyber defence Factory at A6K




 **ERIC VAN CANGH** • You  
Cyber Security and new technologies ambassador  
3w • Edited • 

This morning - Opening ceremony of the cyber defence factory part 2.  
With [Ludivine Dedonder Belgian Cyber Command](#) [Abd-Samad Habbachi](#)  
and [Agoria #CMiB4DEF](#)

Amazing panel discussion , lot of inspirations

Many cyber exchanges on different projects  
With Agoria management [Clarisse Ramakers](#) [Christophe Lebrun](#)  
With lot of [#CMiB4DEF](#) cyber friends  
[Michaël Raison](#) , [Olivier Croix](#) , [Lorenzo Bernardi](#) , [Grégoire Grison](#) , Vastmans Carl  
Michel Van Strythem , SE [Pierre Gillon](#) , Beatrice de Mahieu [Damien Hubaux](#)  
 , [Stéphanie Toussaint](#) , [Jeremy Grandclaudon](#) , [Victor Tavernier Van Hecke](#)  
[Bernard](#)



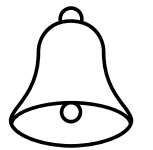
   Maximiliana Muylaert and 31 others

1 comment



Partenariat avec AGORIA, la fédéra-  
tion des entreprises technologiques.

(CMiB4Def), une initiative conjointe  
d'AGORIA, la fédération des entreprises  
technologiques et du Cyber Command.  
Elle part du constat que l'amélioration de  
notre cyberdéfense et de notre résilience  
collective passe nécessairement par  
un rapprochement entre la Défense et  
l'industrie.

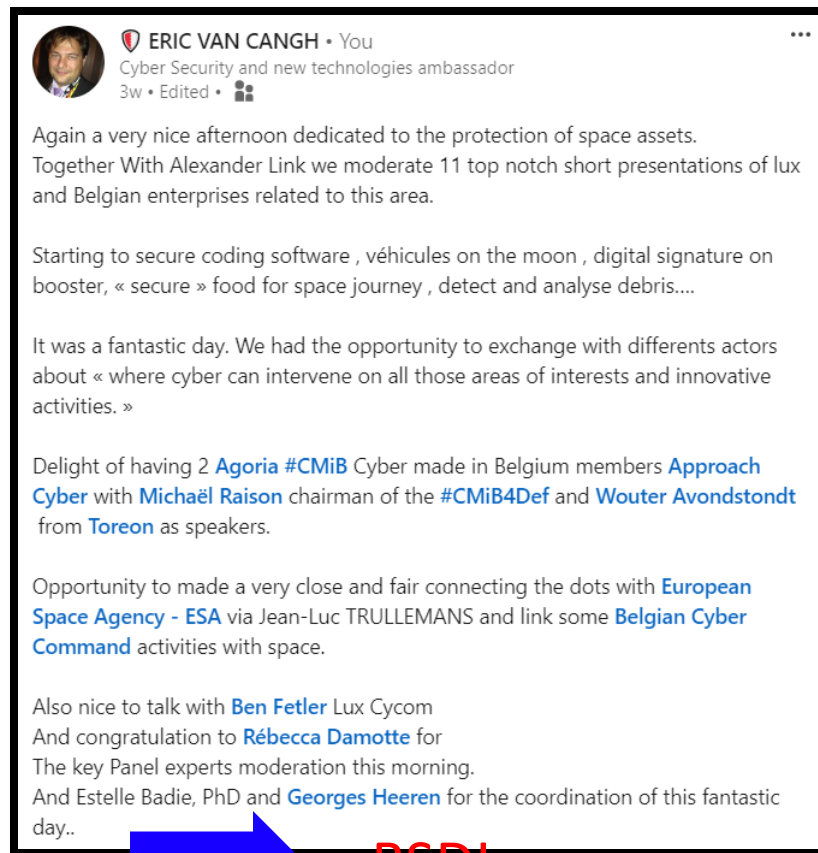


<https://www.sgrs.be/2024/06/26/le-sgrs-publie-son-deuxieme-rapport-historique/>

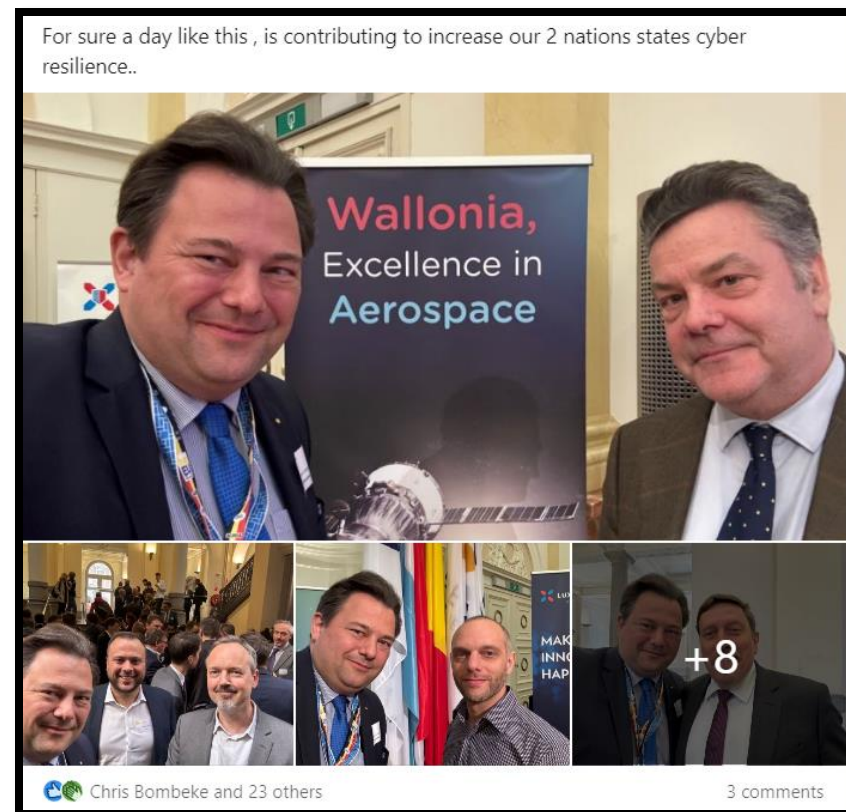
[https://www.sgrs.be/wp-content/uploads/2023\\_RapportAnnuel.pdf](https://www.sgrs.be/wp-content/uploads/2023_RapportAnnuel.pdf)



# 17-18/04 /2024 State visit LUX-BE – Cyber Defence



BSDI



# 24/04/24 Secure the castle – STIE platform born



**ERIC VAN CANGH** • You  
Cyber Security and new technologies ambassador  
2w • Edited •

Today attended to **Kortrijk Xpo Meeting Center** with **Belgian Cyber Command** **European Corporate Security Association - ECSA** and many **Agoria** partners organised by the **BELGIAN SECURITY & DEFENCE INDUSTRY**

Congratulations to **Chris Bombeke Georges Heeren** and Delphine Kelemen **Sandra Van Nerom** for the organisation !

Amazing day to launch the Security, Technology & Innovation Ecosystem (**#STIE**) at Kortrijk XPO during **Infopol XPO112**

Congratulation for the new **#STIE** forum

« a permanent forum that stimulates debate and the exchange of ideas and fosters innovation to contribute to a safer and more secure society on national, European and international level. Where the stakeholders involved, explore the opportunities technology and innovation can bring to security practitioners and society as a whole and the potential »

« a permanent forum that stimulates debate and the exchange of ideas and fosters innovation to contribute to a safer and more secure society on national, European and international level. Where the stakeholders involved, explore the opportunities technology and innovation can bring to security practitioners and society as a whole and the potential »

Opening key notes with deputy prime-minister and minister of justice **Paul Van Tigchelt**

With **Christophe Lebrun** Michel Van Strythem ir. **Yvan De Mesmaeker** **Nicolas de Laminne** and many others security experts





Chris Bombeke and 19 others



# 30/04/2024 – Charleroi – DEF day

BSDI + CMiB

 **ERIC VAN CANGH** • You  
Cyber Security and new technologies ambassador  
1w • 

Today was a fantastic day  
Bringing together industries and **Belgian Defence**  
An initiative during the **Belgian Presidency of the Council of the European Union 2024**  
We had the honor to have **Ludivine Dedonder** Willy Borsus Thomas Dermine but also top speakers during to panel discussion

As the discussions were in closed and trusted environnement.. find the open interesting quotes

« Tips to onboard more SME !!! On European calls »  
Come with the hardest problem - suscite innovation with brilliant brains  
Then you will have to find the best questions (for calls)  
Then we come classified info - need to module  
Expect an answer a raisonnable time »


« No sustainability without security !!! »


« Political still dreaming and not taking risk !!!  
Defence is now taking risks as industrial »

« The most innovative entities are SMEs and research and dev entities  
Economy is fueled (cost advantage(not in BE or competitive advantage) by SME and research !! »

Happy to see **Agoria BELGIAN SECURITY & DEFENCE INDUSTRY** and **#CMiB** members and partners all together making the IDBT..

With **Georges Heeren Delphine Kelemen Chris Bombeke** and all cyber friends they know they were selfiered ^^



 Chris Bombeke and 19 others

# June 2024 - CMiB4DEF Plenary



Presentation of the WG outputs + onboarding new companies

# 15/09/2024 – DIRS milestone

## DIRS UPDATE (Patrick / Steven)

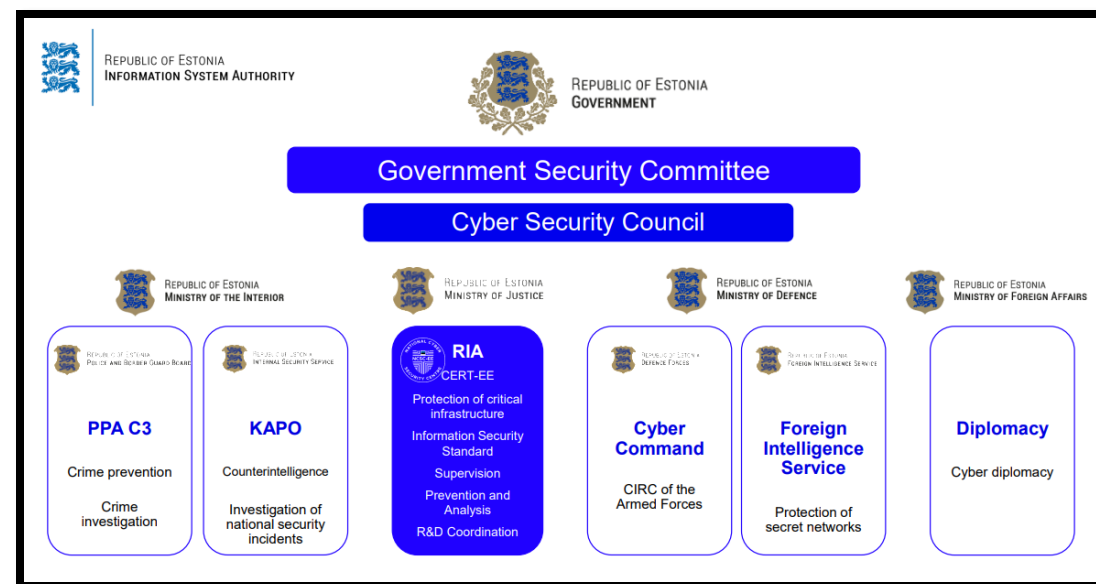
### Management summary

- Defence needs endorsement of the CMiB4DEF board for a feasibility study related to DIRS
- Targets :
  - **Increase the potential to access RDI budget for 2025**
  - **Have CMIB4Def recognized as an ecosystem for Defence related cyber**
- Need a “neutral” entity for this study
- ➔ INNOCOM Institute and Sirris TOGETHER as final proposal (AGORIA + DEF alignment)
- ➔ Timings -> preferably before 20/09 for a CMiB4def board and endorsement

# 30/09 -01/ 10/2024 – 2 days - Estonian Visit

TIME	Activity
30Sep AM	Presentations (Send in advance = tested before starting) Meet and match
	08.30: Lobby Hilton 08.45: bus to CR14 08.50: Group Photo at entrance CR14 09.00: Presentation CR14 09.30: Presentation of EST Defence Industry (Kalev KOIDUMÄE) 09.40: Presentation of BEL Defence Industry (Eric VAN CANGH) 09.50: Presentation BEL Cyber Command (Gunther GODEFRIDIS) 09.55: 2 minute Flash presentations of participating companies 10.45: Speedmatchen 12.10: Lunch 25 persons
30Sep PM	Visit EST industry
	13.15: Cybexer Technologies 14.30: Nordtal 1540: Cybernetica 1640: HILTON
01Oct	Visit other
	08.45: Lobby Hilton 09.00: RIA 10.30: Defence League 12.00: Lunch 13.00: E-Estonia 14.45: CCDCOE 17.00: HILTON

RIA = CCB the National Cyber Authority (NCA)





# 30/09 -01/ 10/2024 – 2 days - Estonian Visit

- Day 1





# 30/09 -01/ 10/2024 – 2 days - Estonian Visit

- Day 2



KAITSELIIT

**CYBER DEFENCE UNIT OF ESTONIAN DEFENCE LEAGUE**  
(„CYBER DEFENCE LEAGUE“)

KÜBERKAITSEÜKSUS

Eesti e-eluviisi kaitseks!

2007 – idea about cyber reserve - the need of community  
2009 – first Cyber defence platoons in 2 DL districts  
2011 – establishment of CDU as DL exterritorial district

# 11/10/2024 CMiB4DEF WKS2 -> CMiB4DEF 2.0

.AGORIA

## Quick recap concrete actions – 1 pager

.AGORIA


### WG 1 – CONCRETE ACTIONS for 2024

- **Big objective:** « 2029 Technology Roadmap » for the DIRS (Cyber)
  - By the Technical committees
- **In mutual collaboration with Belgian Defence and based on the « Big Topics » (see previous slide):**
  - Define the boundaries for the Roadmap (Timing, budget, government requirements...)
  - Further detailing of the topics, describing desired end states
  - Prioritisation / Intermediate milestones
  - Define Governance, Roles & responsibilities
- (Check synergies with EDA Captech Cyber)

.AGORIA

### WG 2 – CONCRETE ACTIONS for 2024

- **WG2 Organization**
  - Rolling Group animation starting with BHEA
- **Action Plan**
  - Action validation
  - Priority assignment
  - Deployment Planning
  - Stakeholders involvement
  - Regular reviews




.AGORIA

### WG3 - CONCRETE ACTIONS for 2024

Based on the needs, how can the industry respond

- **Support to get a view on the concrete needs:**
  - Discuss the needs & priorities (Product, Services and Systems) with the Cyber Command & Technical Committees
  - Prepare a proposal precisising the industry needs to the Future Certification Body in the Military Domain
- **What's in it for the Industry:**
  - BE Authorities and agencies alignment on standards recognition
  - Clear view on the priorities (and on the products)
  - Link with WG1 DIRS & Technical Committees




.AGORIA

### WG 4 – CONCRETE ACTIONS for 2024

Support Defence Cyber Skills development

- **Context (focus defence)**
  - Listing the gaps on the defence needs
  - Stimulating skills acquisition (CTF with IRMA)
  - Mapping offering and demand side (Industries / education...)
- **Reusing CMiB4Talents deliveries with the extension on Def Cyber requirements (ex. SANS training...)**
  - **Feeding CMiB4Talents via CMiB4DEF inputs**
    - Including Offensive teams, Influence teams...

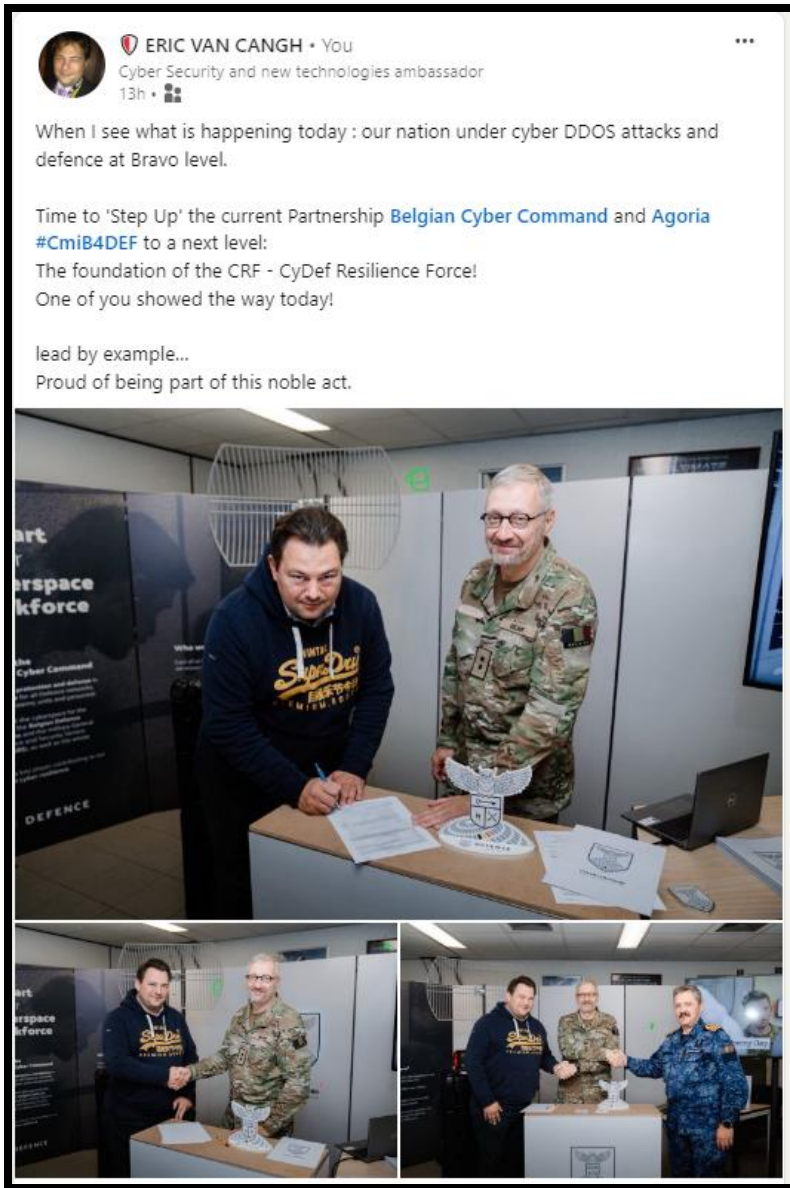


.AGORIA

### WG 5 – CONCRETE ACTIONS for 2024

	Action	Who	When
3	Inventory of relevant Fairs & Events	AGORIA	Q1
2	Identify the needs of the AGORIA Members	AGORIA	Q1
3	AGORIA – BSDI to provide support for selected Fairs (based on 1&2)	AGORIA (BSDI)	Continuous
4	Identify the community -> Database (FOD Econ & Def NAO) Meet & Greet events to expand the community beyond Agoria.	Def NAO	Start Q2
5	Coordinate Communication between AGORIA & STRATCOM	AGORIA / STRATCOM	Continuous
6	Request support from Defense in PR activities for selected fairs & activities (MI Attachés, Events on BE MI Vessels, ...)	AGORIA / CHOD	Continuous

# 12/10/2024 – CRF milestone – reservist Day





# CMiB4DEF – on track



Board meeting 05/2023



Plenary 06/2023



Workshop 2 : 09/10/2023



CORE TEAM  
DEFINED

BOARD  
DEFINED  
03/2023

BOARD 1  
13/04/2023

PLENARY DEF  
06/06/2023

BOARD 3  
Nov 2023

BOARD 1  
02/2024

BOARD 2  
03/2024

STRATEGY  
DEFINED

WORKSHOP 1  
DONE  
03/2023

BOARD 2  
WG DEFINED  
05/2023

WORKSHOP 2  
DONE  
09/10/2023

PLENARY DEF  
05/12/2023

Workshop 1  
03/2024

PLENARY DEF  
06/2024

# AGENDA

- BSDI in nutshell
- AGORIA Cybersecurity building blocks
  - Cyber Aware Programme (CAP) - Agoria Connect – Digital@Services
  - CMiB
- Innovative collaboration Public / Private
  - Collaboration Path for the Cyber Command
  - CMiB4DEF – Triparties – CMiB / BSDI and Defence / CyCom
- Interactions with CMiB4Talent FG and CMIB4ICS/OT FG
- Conclusion



# Interactions with CMiB4ICS/OT FG

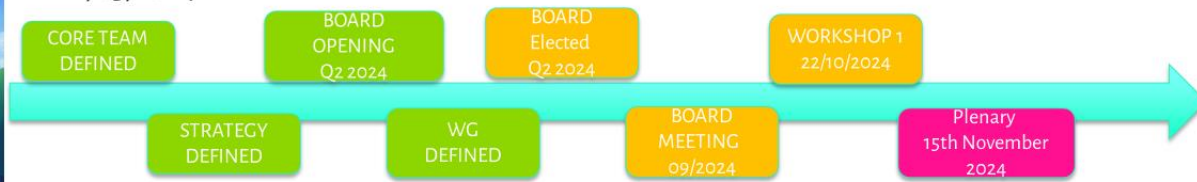
## CMiB4ICS/OT



Kick-Off meeting FG  
22/03/2024



Follow-up meeting 13/05/2023



## CMiB4ICS/OT : Overview of 6 WG

WG	WG TOPIC	PEOPLE Active
1	TOP MANAGEMENT AWARENESS CREATION	13
2	OT EVENTS and FAIRS PARTICIPATION	5
3	KISS COMPLIANCE (NIS 2/CRA OT/IT)	16
4	OT CRITICAL INFRASTRUCTURE	12
5	OT SKILLS / KNOWLEDGE SHARING	11
6	KISS SMEs – Supply Chain Security	8

# Interactions with CMiB4Talent FG

## CMiB4TALENT – on track



Board meeting 09/2023



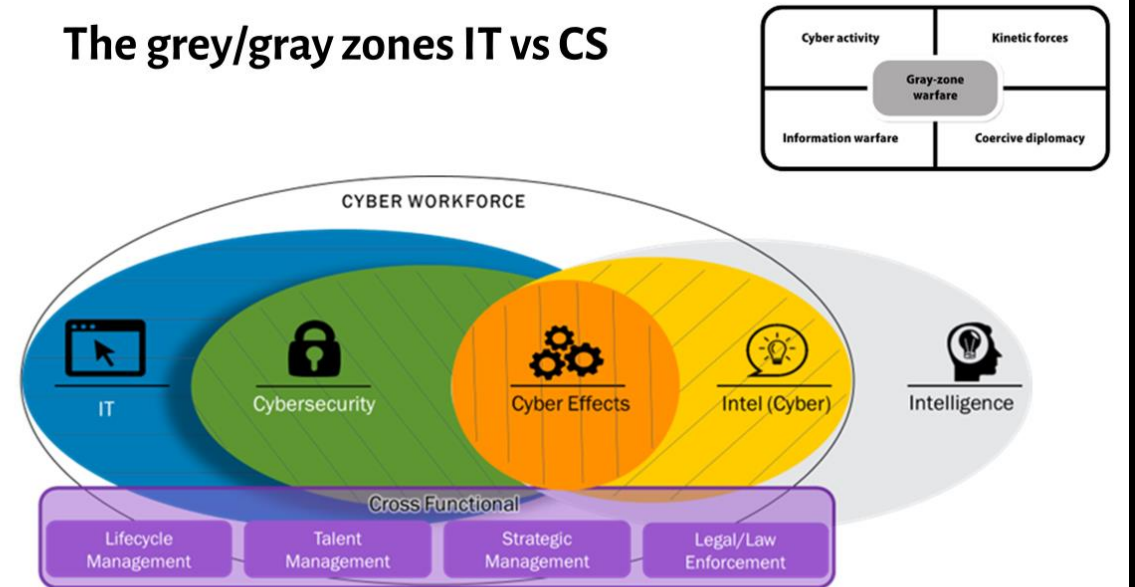
Kick off 27/09/2023



Workshop 1 - 23/04/2024



## The grey/gray zones IT vs CS



# Interactions with CMiB4Talent FG

## Action plan CyberTalents – 5 tracks

- **WG1 - Mapping and forecasting** (Georges Ataya/Solvay Business School)
- **WG2 - Create a national cybersecurity ecosystem for talents** (Agoria+Chair/VC)
- **WG3 - Improve cyber security expertise in companies** (Jasper Hooft/Toreon)
- **WG4 - More inflow in digital/CS studies & trainings** (Clément Laurens/Cresco)
- **WG5 - Work with universities & training centers** (Bart Asnot/Microsoft)

**WG 1 - Mapping & forecasting**

Objective: Map the demand of cybersecurity experts and the offer of training/education and identify the gap between  
Lead: Georges Ataya/Solvay LifeLong Learning

WORKPACKAGE/ CHALLENGE	ACTION	TIMING	OWNER/ PARTIC	DELIVERABLE
1.1. Mapping CS training & education offer	Map CS programmes in universities, "higher schools", non regular/public + contact (1/2024) and make them available for CS members.	2024	Sacha/Headend, Jeremy/ULB, Caroline/CCB, Georges/Solvay, Kurt/Hooft	May/June 2024: First analysis by students (Demand/questionnaire and Supply + expert panel)
1.2. Demand (CS jobs)	Mapping of soft and hard skills and roles from the job vacancies, based on 12 ENISA profiles (survey...) + workshop on results.	2024-25	Sacha/Headend, Manu/Intrinis, Carl/Defense, Georges/Solvay, Kurt/Hooft	Sept 2024: First draft National skills research report Dec 2024: Final report
1.3. Career path	Establish a career path to get a CS job (3 basic profiles - 10y, evolve in a CS career and help define training content.	2024-25	Jeremy/Ataya + RALCAI, Caroline/CCB, Manu/Intrinis, Carl/Defense, Georges/Solvay, Kurt/Hooft (7), + Jasper & Yves? Denise - HR collaboration	Sept 2024: Proposal for next Board meeting (2025) 2025: career path for 1 profile 2025: career path for 2 profiles

**WG 2 - Create a national cybersecurity ecosystem for talents**

Objective: Create a national CS ecosystem for talents and give it visibility  
Lead: Agoria + ASEP

WORKPACKAGE/ CHALLENGE	ACTION	TIMING	OWNER/ PARTIC	DELIVERABLE
2.1. Primary session	Organize 1 primary session a year to gather the public/private ecosystem and boost collaboration on priorities	14/09/2024	PVP	Sept 2024: Primary 24/9 - >70 participants
2.2. Board meetings	4 meetings/year to define the CyberTalents strategy & action plan	2024: 11/1, 2025: 2/16, 2025: 10/1	Agoria: Floriane PVP	Acty
2.3. Visit Campus Cyber in France	Visit the Campus Cyber in France for an exchange of best practices and more collaboration	2024-25	Agoria: Floriane	Sept 2024: content and date set
2.4. Give visibility to CyberTalents	Website Agoria website, Eur. Cyber Sec (May 2024), Cyber month, ...	2024-25	Agoria: Eric PVP	Sept 2024: visibility on 2 events + planned for Cyber month; webpage ready
2.5. EU funding for initiative	Participate in EU project for CyberSkills with DigitalEurope to window the CyberTalents actions	2024-26	Agoria: Floriane (lead) Georges/Solvay, Kurt/Hooft	See other WP (WP 1 for 2024) Agoria: Floriane

**WG 3 - Improve cybersecurity expertise in companies**

Objective: Improve cybersecurity expertise in companies (recruitment methods, employees' training...)  
Lead: Jasper Hooft, Toron

WORKPACKAGE/ CHALLENGE	ACTION	TIMING	OWNER/ PARTIC	DELIVERABLE
3.1. In-Company - CMB academy	Create training path for employees according to Career paths	2024-25	Jasper/Toreon, Agoria	Sept 2024: full
3.2. Skillbuilding target groups	Set up partnership with ATAS/FORM/Competence centers (for ANIMO/SMART) and CS members to create tailored support training	2024-25	Vivienne/Willem, Carl/Defense, Agoria/SMART, Jasper/Toreon	Sept 2024: collaboration identified, action plan ready
3.3. Workshop on recruitment	Set up a workshop on recruitment methods coordinated by Agoria Academy	2024	Agoria: Floriane Vivienne/Willem	Sept 2024: content and date are defined
3.4. Job lab	Find Partners to organize a CyberTalents/SMART joblab and organize this joblab with Agoria partners and associates	2024-25	Kurt/Hooft, Georges/Solvay Agoria: Eric	Sept 2024: partner identified
3.5. Internships	Create a space on CMB platform to connect interns with companies - CCB/Head 2 cyber - to check	2024	Agoria: Floriane + Vivien & Mathilde	Sept 2024: CyberTalent

**WG 4 - More inflow in digital/CS studies & trainings**

Objective: attract more people in digital and cybersecurity trainings and careers  
Lead: Clément Laurens, Cresco Cybersecurity

WORKPACKAGE/ CHALLENGE	ACTION	TIMING	OWNER/ PARTIC	DELIVERABLE
4.1. DIGITALS in all education programs	Promote digital and cybersecurity skills in education 1. Lobby all job parties for digital/CS in all programs 2. Support the creation of a complete education package (Focus on Teachers)	2024 - 2027	Proposed for 2024 Cécile de Wint/Belec Clément Laurens/Cresco Agoria - 1 & 2 - Floriane (SL, Laura, Viole)	Sept 2024: 1) Overview lobby work, 2) full
4.2. Assessments	Organize cyber awareness actions with partners (organize a Cyberday in wallonia, Flanders and French) 3. Support the creation of a complete education package (Focus on Teachers)	2024 - 2025	Proposed: +Christine Galleux/Digitalicity +Vivien Hooft/Agoria	Sept 2024: each regional partner and action defined
4.3. Agoria Company	Schools visit companies to talk about cybersecurity Target higher education (18-25 YO) + 1 visit in each region (BR, WL, FL)	2024-25	Proposed (to be validated): +Vivien Galleux/Hooft +Vivien Hooft/Agoria	Sept 2024: database & list created + call for participation during January

**WG 5 - Work with univ/higher education & training centers**

Objective: Create new learning programs and improve the quality of existing ones through a better collaboration between  
Lead: Bart Asnot, Microsoft

WORKPACKAGE/ CHALLENGE	ACTION	TIMING	OWNER/ PARTIC	DELIVERABLE
5.1. Experts Pool	Set up a pool of experts on diverse security topics for web & TV to call upon (mentoring, coaching, expertise, research, lectures, use cases) + Code of conduct + satisfaction survey	2024-25	Bart Asnot/Microsoft Denise/ULB, Vivien/Agoria, Bernard/Egmont, Victor/ULiama, Hubert/UCampus, Cathy/CC (collaboration)	Sept 2024: Launch new pool of experts
5.2. Summer Academy	"Train the trainer": Full day event for cybersec teachers introducing the expert pool + networking, giving an update on CMB, and a wider range of cybersecurity topics and innovation (not only technical but also pedagogical)	2025-26	Agoria: Eric + Floriane Yves/TEM + NEW (lead) Hana/Agoria, Hubert/UCampus, Tom/DMoore, Gabriel/Drewn, Bernard/Egmont	Nov 2025-26
5.3. Collaboration for "Observatory"	Companies collaborate for workplace learning (Digital) 1) Work with 2 edu institutions (PALN) 2) First Cybersecurity consultation (meet with members)	2024-25 MT (2024)	Agoria: Eric + Floriane Denise/MART, Vivien/Agoria, Hooft/UCampus	Sept 2024: 2 workshops to present partners' offer
NEW: S.A. CS courses in other departments & IT	Mandatory CS lessons in each technical part (IT certificates) and in other departments (Fundamentals) + law, engineering, MBA, ... + Together with companies that can explain CS in non technical terms (see: IBM basic lesson on CS)	End 2024	Georges/Solvay, Kurt/Hooft, Hana/Agoria, Victor/ULiama, Cathy/CC	End

# AGENDA

- BSDI in nutshell
- AGORIA Cybersecurity building blocks
  - Cyber Aware Programme (CAP) - Agoria Connect – Digital@Services
  - CMiB
- Innovative collaboration Public / Private
  - Collaboration Path for the Cyber Command
  - CMiB4DEF – Triparties – CMiB / BSDI and Defence / CyCom
- Interactions with CMiB4Talent FG and CMIB4ICS/OT FG
- Conclusion

# CONCLUSION : Together we are stronger

# .AGORIA | BSDi

Belgian Security & Defence Industry





# Questions & Answers

Thank you for your attention

**Eric Van Cangh**

**Senior Business Group Leader Digital  
Cyber Security**

**T: +32 2 706 78 25**

**M: +32492.23.24.34**

[Eric.Vancangh@agoria.be](mailto:Eric.Vancangh@agoria.be)

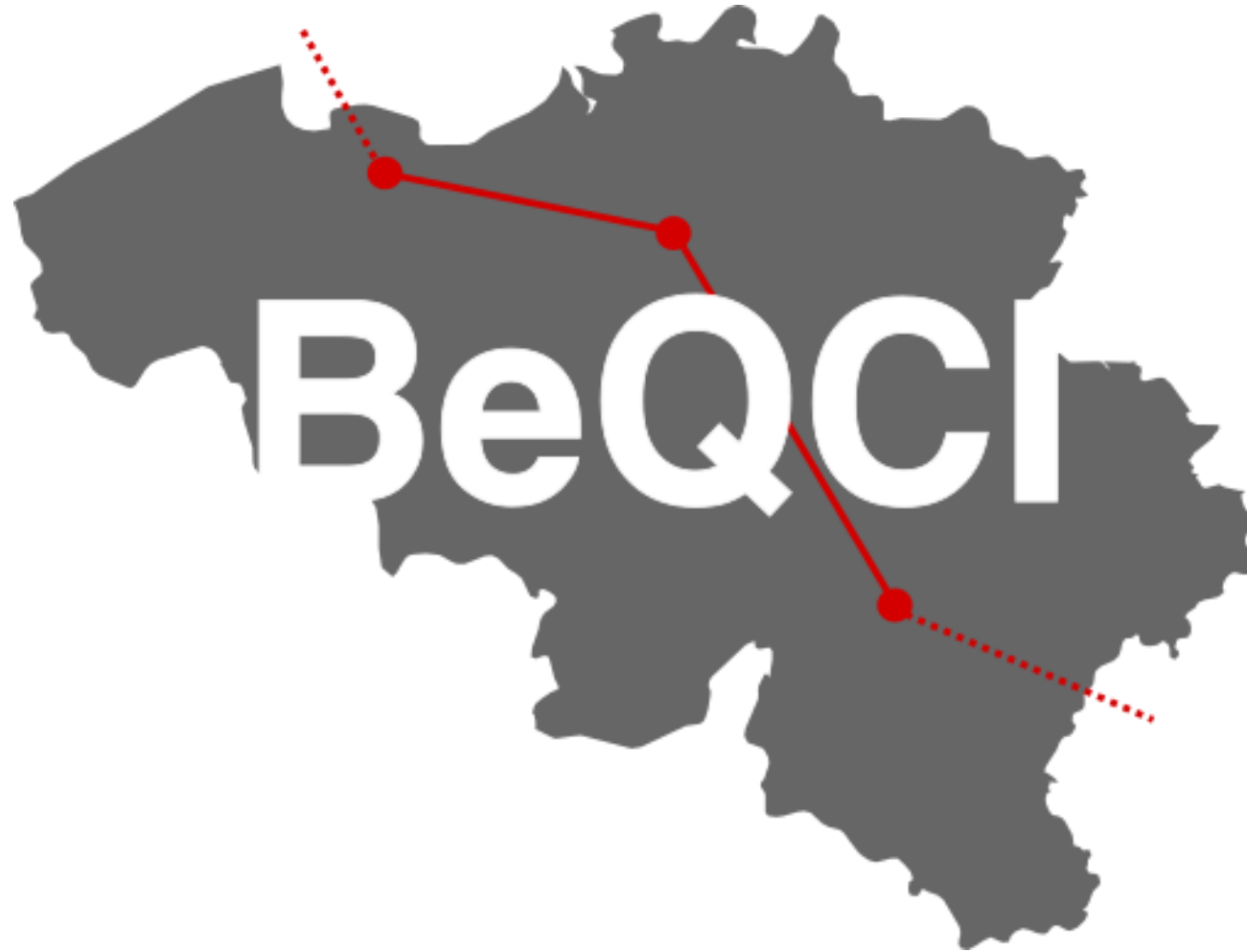


**Les conférences reprendront  
dans 15 minutes.**



**Karel Dumon**

Imec

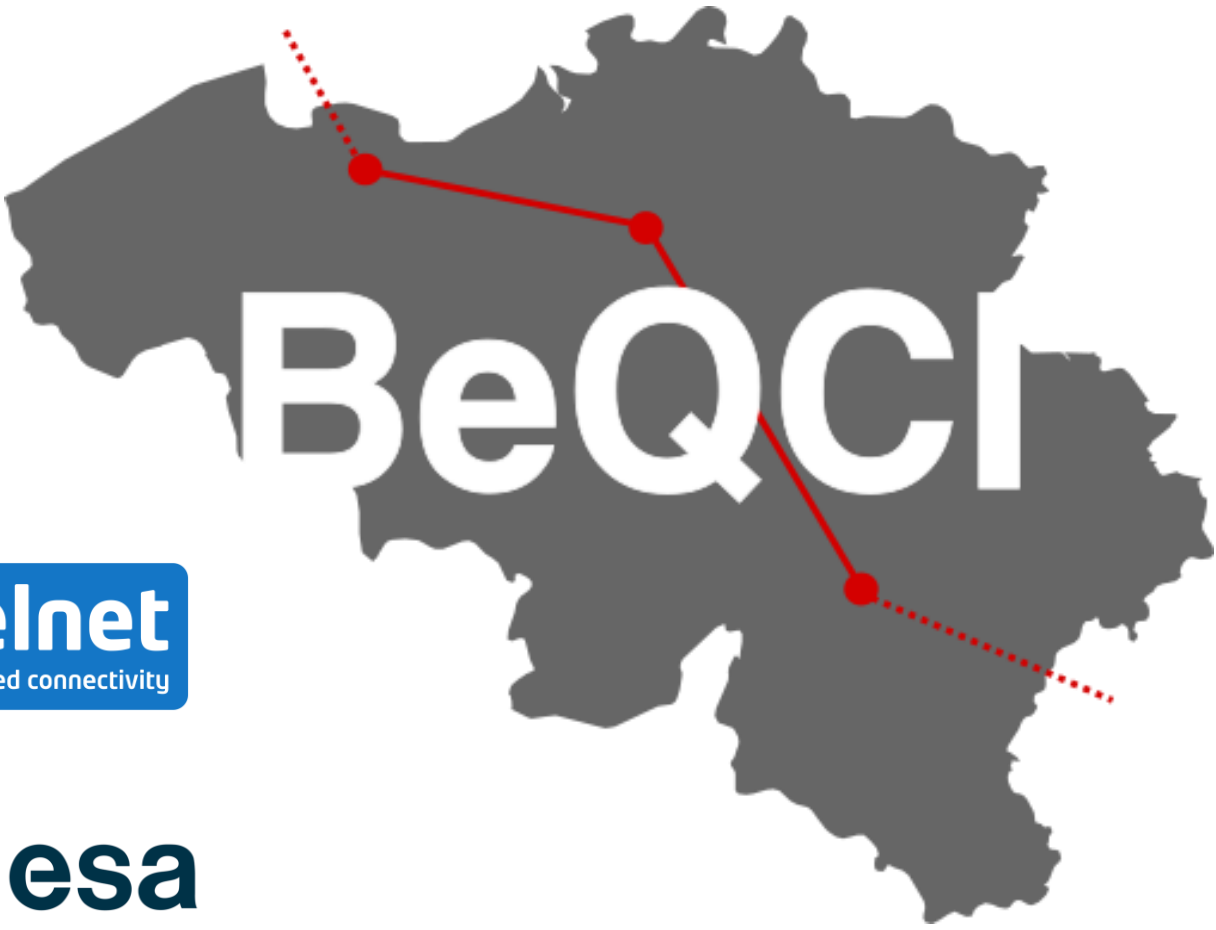


# BeQCI: Belgium Quantum Communication Infrastructure

Cyberweek – 17/10/2024 - [karel.dumon@imec.be](mailto:karel.dumon@imec.be)

# BeQCI: the first open Belgian quantum communication testbed

The image displays a collection of logos for the partner organizations involved in the BeQCI project. The logos are arranged in a grid-like fashion. From top-left to bottom-right, they include: EuroQCI (a globe icon), belspo (a colorful bar chart), imec (a blue square icon), Ghent University (a classical building icon), KU LEUVEN (a blue rectangular box), UHASSELT (a play button icon with the text 'KNOWLEDGE IN ACTION'), UCL (a blue rectangular box with 'Université catholique de Louvain' below), ULB (a blue rectangular box), RMA (Royal Military Academy, featuring a figure on a horse), Belnet (a blue rectangular box with 'dedicated connectivity' below), Multitel INNOVATION CENTRE (text-based logo), THALES (text-based logo), and esa (a circular icon with a dot).





# British intelligence hacked Belgacom then sabotaged investigation

Thursday 25 October 2018



The Belgian federal prosecutor's office has confirmed that it considers British intelligence as the main actor in the hacking of telecommunications company Belgacom, now known as Proximus. In addition, the office said the British intelligence-gathering headquarters GCHQ attempted to sabotage an investigation by the Belgian security services of the hacking incident.

# Britse geheime dienst bespioneerde jarenlang Belgacom-klienten



Hoofdkwartier van de Britse geheime dienst — © reuters

Bij de digitale aanval op Belgacom kon de Britse geheime dienst veel meer communicatie onderscheppen dan tot nu toe werd aangenomen. De geheime dienst GCHQ raakte in 2011 binnen in het netwerk door drie werknemers te hacken. Daarna kon de GCHQ twee en een half jaar lang ongestoord rondsnoeren in het netwerk van Belgacom en dochterbedrijf BICS. De geheime dienst kon zo de communicatie onderscheppen van de individuele klanten van Belgacom zelf, van de NAVO en de EU, en van de klanten van honderden internationale telecomproviders.

Nikolas Vanhecke

Zaterdag 13 december 2014 om 07:00





## Ruim 160 Russische schepen verdacht van spionage kabels en leidingen in Noordzee



@foto: Erwin Willems (marinetraffic)

LARS BOVÉ, STEPHANIE DE SMEDT

20 juni 2024 01:00

**Niet-militaire Russische schepen bespioneren onze pijpleidingen en kabels in de Noordzee en dat gebeurt op veel grotere schaal dan al bekend was. Onderzoek van De Tijd en het Nederlandse Follow the Money wijst op een massa verdachte acties die 167 Russische schepen al jarenlang uitvoeren rond kritieke infrastructuur in de Noordzee.**

Sinds de oorlog in Oekraïne in februari 2022 losbarstte, is al een tiental Russische schepen genoemd in de pers omdat ze verdacht vaargedrag vertoonden in de Noordzee en omliggende wateren. Zoals de oceanografische onderzoeksschepen Yantar en Evgeniy Gorilezhzhan. Dat zijn in werkelijkheid spionageschepen van de GUGI, het directoraat voor 'onderwateronderzoek' van de Russische Defensie dat zich bezighoudt met sabotage, inlichtingenwerk rond kritieke infrastructuur en het aftappen van onderzeekabels. Scandinavische media filmden vorig jaar

## Belgische bedrijven wapenen zich tegen Russische spionage in Noordzee



Er staat kritieke infrastructuur in onze Noordzee, zoals het zogenaamde stopcontact van Elia. Dat is een schakelplatform dat de stroomkabels van meerdere windparken bundelt om stroom aan land te brengen.

COLR  
0,77% ↗



ELI  
0,16% ↗



LARS BOVÉ, STEPHANIE DE SMEDT

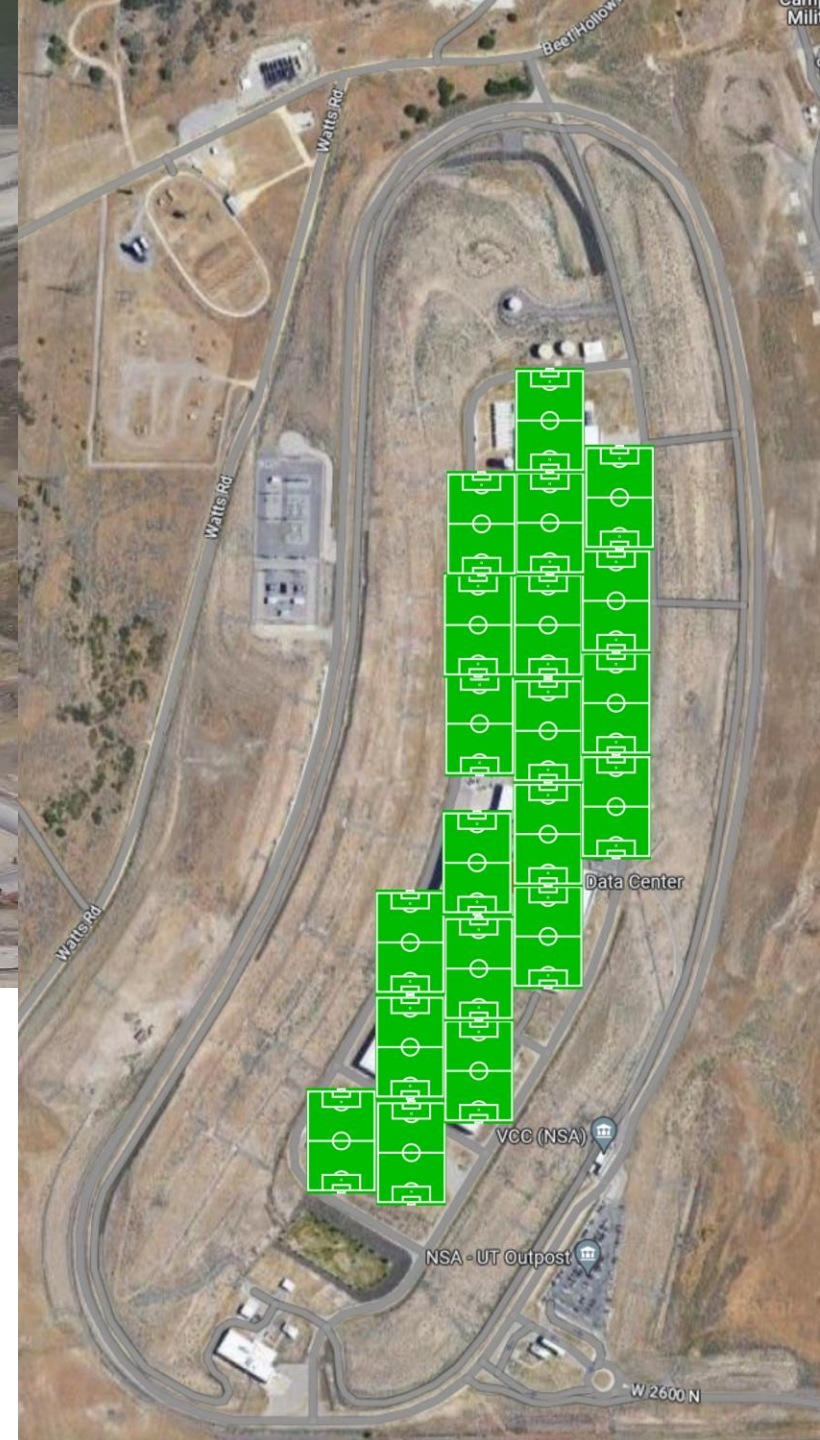
21 juni 2024 10:22

**Het gasnetbedrijf Fluxys laat zijn onderzeese gaspijpleidingen sinds kort continu bewaken en zelfs Colruyt moet een veiligheidsplan opstellen voor zijn mosselboerderij: ook bedrijven wapenen zich tegen mogelijke spionage en sabotage door de Russen in de Noordzee.**

‘H eel lang was beveiliging iets waarvan men dacht: dat zal wel ergens gecoverd zijn. Nu wordt het besproken in de raden van bestuur’, zo vat Christophe Dhaene, de topman van e-BO Enterprises, het samen. e-BO is een West-Vlaams technologiebedrijf dat onder meer voor alle windparken in de Belgische Noordzee de digitale systemen beheert. Dat gebeurt via permanent bemande controlekamers op



# Bumblehive – Utah



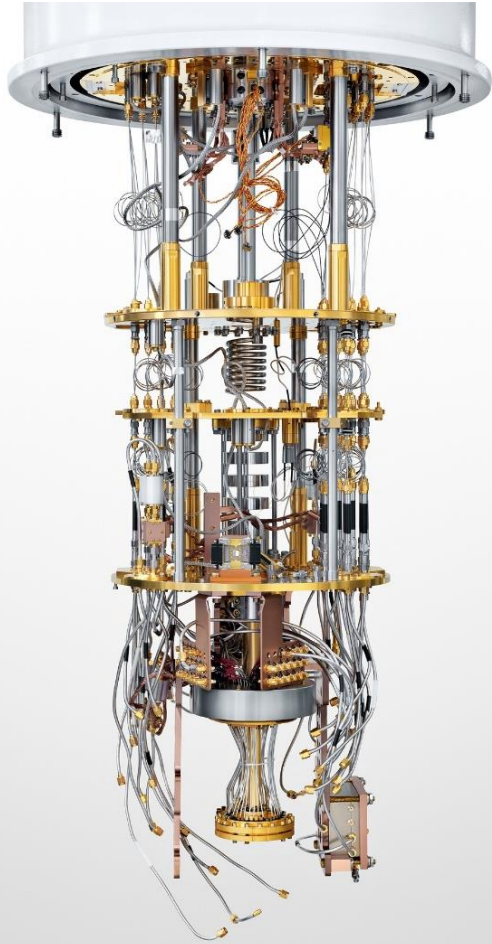
Cost: ~1.7 billion \$ (buildings) + several billion \$ (computer hardware)

Size: 100 000 m<sup>2</sup>

Capacity (2013): 10+ exabytes  
(10 exabyte = 10 000 000 000 000 000 bytes)

# The promise of quantum computers

## Examples of potential applications



### Simulation on a quantum level

*drug discovery*  
*battery materials*  
*room-temperature superconductors ...*

### Complex optimization problems

*logistics (travelling salesman)*  
*portfolio optimization (finance)*  
*circuit design ...*

### Speeding-up mathematical routines

*linear algebra (e.g. AI & ML)*  
*prime factorization*

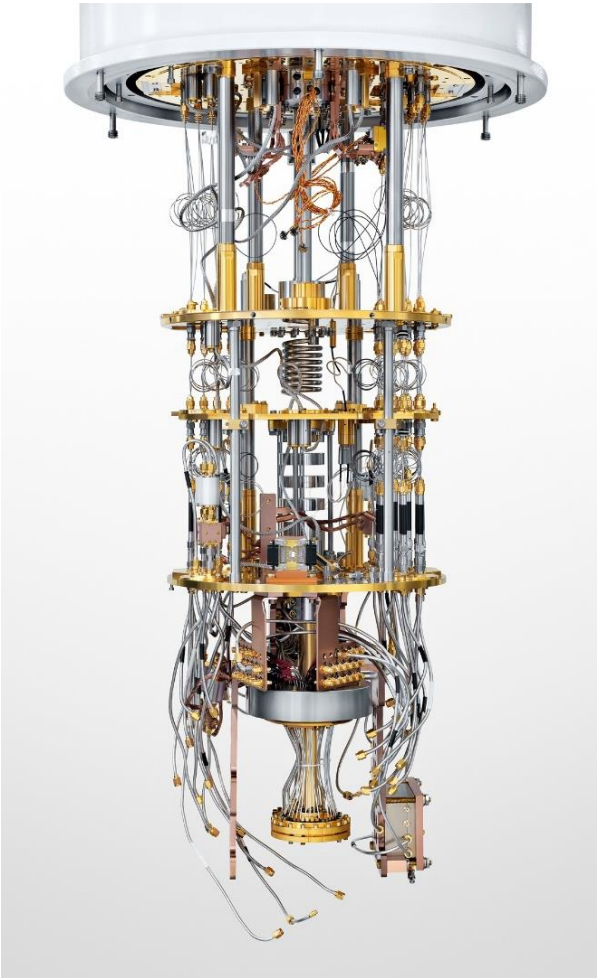
...

*and many more...*



# The promise of quantum computers

## Examples of potential applications



### Simulation on a quantum level

*drug discovery*  
*battery materials*  
*room-temperature superconductors ...*

### Complex optimization problems

*logistics (travelling salesman)*  
*portfolio optimization (finance)*  
*circuit design ...*

### Speeding-up mathematical routines

*linear algebra (e.g. AI & ML)*

**prime factorization**

...

*and many more...*



# History of encryption

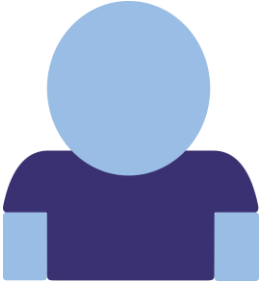
Before 1970s

Mfx7ISCNAs8por0J l j6jj3xBFiUPb  
GDC

Ok! Let me write that down.



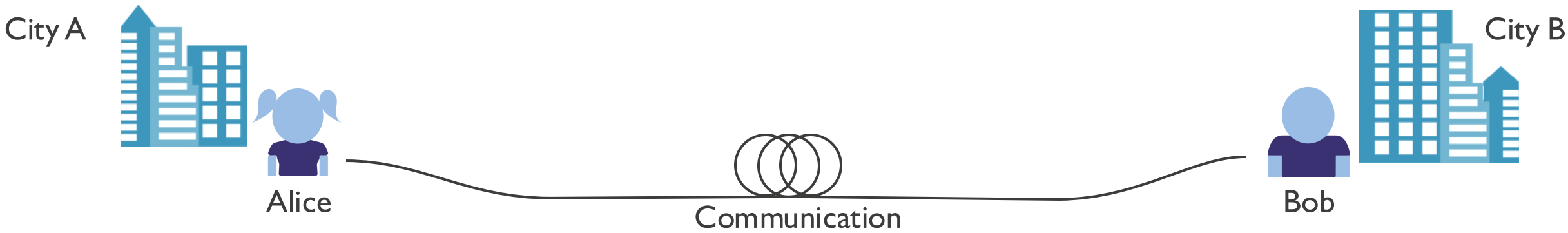
Alice



Bob

# History of encryption

Before 1970s



Key: Mfx71SCNAs8por0Jlj6jj3xBFiUPbGDC

Key: Mfx71SCNAs8por0Jlj6jj3xBFiUPbGDC

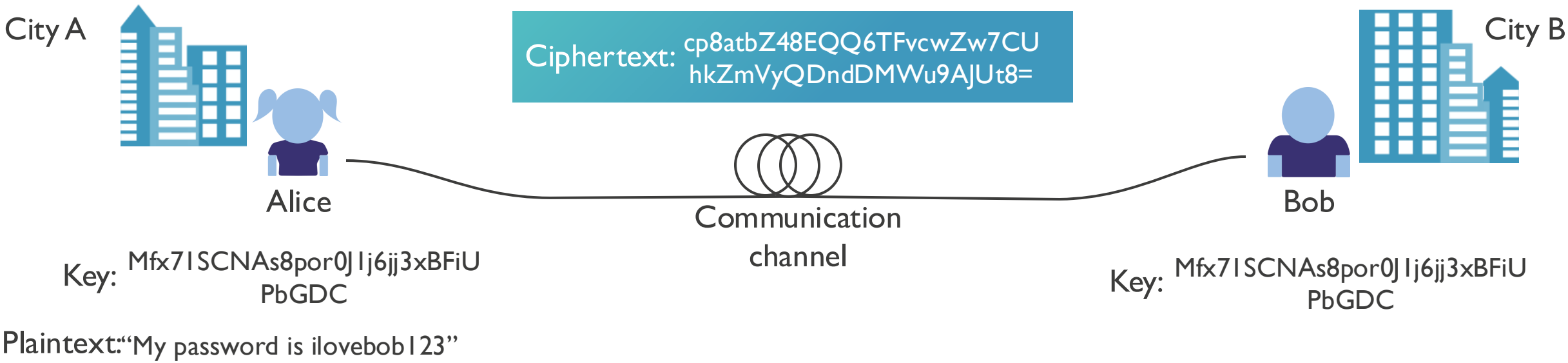
Plaintext: "My password is ilovebob123"



Ciphertext: cp8atbZ48EQQ6TFvcwZw7CU  
hkZmVyQDndDMWu9AJUt8=

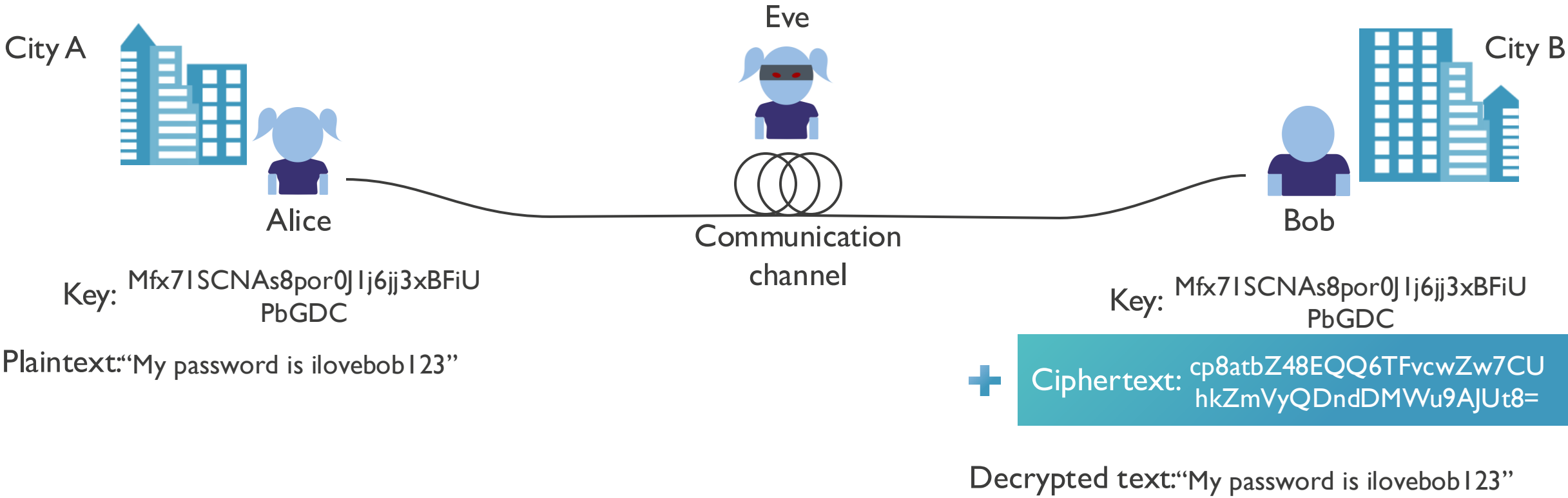
# History of encryption

Before 1970s



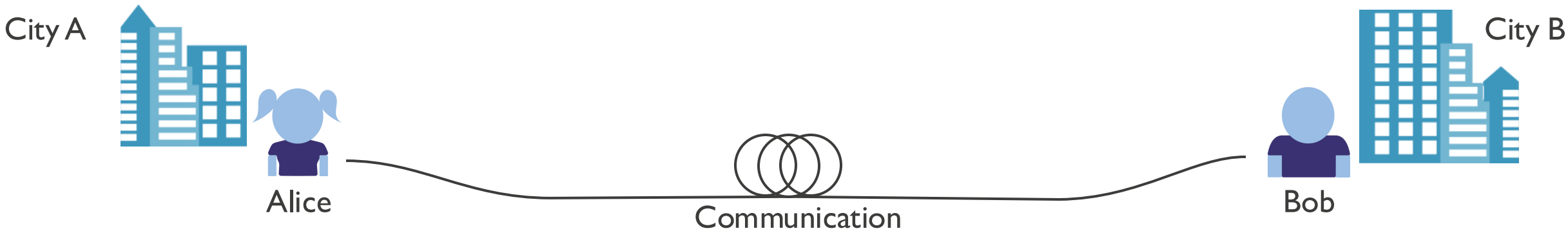
# History of encryption

Before 1970s



# History of encryption

## After 1970s: Public key cryptography



Prime 1: 1 1872035424589255887822295232985654 1295 1771 3236 15952921 91 894268803592497669 1675  
 601 1868666926475365335279 1923 10459474294307098498862369566023 130992802706003177  
 54776825403086338 1846 1771 5972399091 0049344704205831 1 230878588833862794 16920979  
 70081 238920257380 125540496530346252387371 99556295929761 2976235841 1852661

Prime 2: 177 158930287051 2864396861 6241 2785 1731 17 1831 48940069842892383591 7336482743983994  
 323084767204141 01 463359553761 4449 16262591 4210 1054544621 65 163691 3846675404 133904  
 7805571 479209978004 14626489 1342743238 13 1955602792250822393703 203646442395073044  
 498 18658391 5449 169681 6261 76 11 32636708094399882956373874 1 965404396456317



Modulus: 21032370961 5021 130386866947386859 132278053560039391 053458528741 7888695620310161  
 99106720402080099454840426997527205 190779 169907529926 14878961 5239224497 10854734  
 512345034475741 91 2705772774 15 137279956399357021 97860066055531 01 72148871 64536048  
 2622369754080 197423225929587332 139561 202602 1081 625306627032862928 10760641 554850  
 176739373567627023549 14850847553651 8448932699747760505425644895 1045079583 1101 18  
 7240572030265003330 124937704275 164630994341 17 12304309200303280262 153201 70062365  
 65051 663071 754651 136866707250789471 18488285324999 122461 068339008474908739844860  
 53904652591 64104303 1227308350 146174 124596429855785371 19 126709537

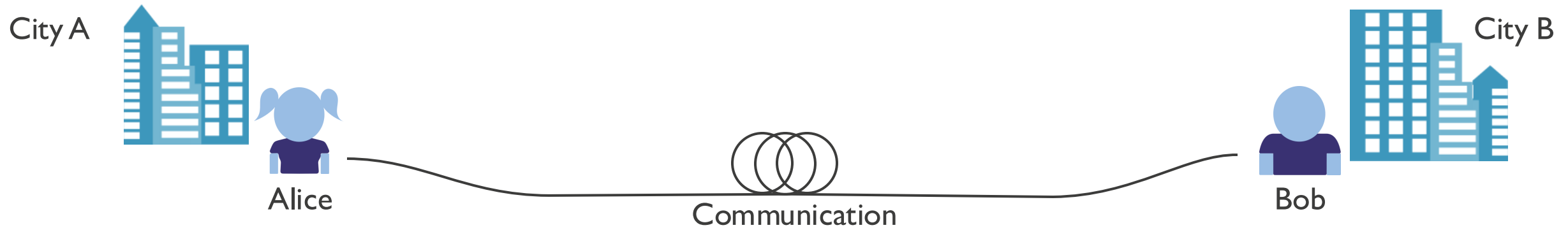


# History of encryption

After 1970s: Public key cryptography

Alice's  
Modulus

```
2 1032370961 5021 130386866947386859 132278053560039391 053458528741 7888695620310161
991 06720402080099454840426997527205 190779 169907529926 14878961 5239224497 10854734
5 12345034475741 91 2705772774 15 137279956399357021 97860066055531 01 72148871 64536048
2622369754080 197423225929587332 139561 202602 1081 625306627032862928 10760641 554850
176739373567627023549 14850847553651 8448932699747760505425644895 1045079583 1101 18
7240572030265003330 124937704275 164630994341 17 12304309200303280262 15320170062365
65051 663071 754651 136866707250789471 18488285324999 122461 068339008474908739844860
5390465259164 104303 12273083501461 74 124596429855785371 19126709537
```



Prime 1:

```
1 1872035424589255887822295232985654 1295 1771 3236 15952921 91 894268803592497669 1675
601 1868666926475365335279 1923 104594742943070984988623 69566023 1309928027060031 77
54776825403086338 1846 1771 5972399091 0049344704205831 11 230878588833862794 16920979
70081 238920257380 125540496530346252387371 99556295929761 2976235841 1852661
```

Prime 2:

```
177 158930287051 2864396861 6241 2785 1731 17 1831 48940069842892383591 7336482743983994
32308476720414101 4633595537614449 162625914210 1054544621 65 163691 3846675404 133904
7805571 479209978004 14626489 1342743238 13 1955602792250822393703 203646442395073044
498 18658391 5449 169681 6261 7611 32636708094399882956373874 11 965404396456317
```

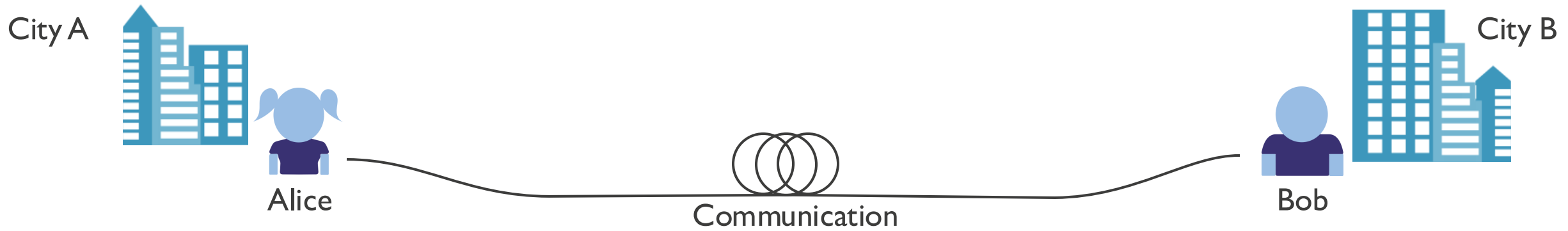
Plaintext: "Oh, Alice... I love you too!"

# History of encryption

After 1970s: Public key cryptography

Alice's Modulus

```
2 1032370961 5021 130386866947386859 132278053560039391 053458528741 788869562031 0161
991 06720402080099454840426997527205 190779 169907529926 14878961 5239224497 10854734
5 12345034475741 91 2705772774 15 137279956399357021 97860066055531 01 72 148871 64536048
2622369754080 197423225929587332 139561 202602 1081 625306627032862928 10760641 554850
176739373567627023549 14850847553651 8448932699747760505425644895 1045079583 11 01 18
7240572030265003330 124937704275 164630994341 17 12304309200303280262 153201 70062365
65051 663071 754651 136866707250789471 18488285324999 122461 068339008474908739844860
53904652591 64 104303 1227308350 1461 74 124596429855785371 19 126709537
```



Prime 1: 1 1872035424589255887822295232985654 1295 1771 3236 15952921 91 894268803592497669 1675  
601 1868666926475365335279 1923 10459474294307098498862369566023 1309928027060031 77  
54776825403086338 1846 1771 5972399091 0049344704205831 1 230878588833862794 16920979  
70081 238920257380 125540496530346252387371 99556295929761 2976235841 185266 1

Prime 2: 177 158930287051 2864396861 6241 2785 1731 17 1831 48940069842892383591 7336482743983994  
3230847672041 41 01 463359553761 4449 16262591 4210 1054544621 65 163691 3846675404 133904  
7805571 479209978004 14626489 1342743238 13 1955602792250822393703 203646442395073044  
49818658391 5449 169681 6261 76 11 32636708094399882956373874 11 96540439645631 7

Communication channel

Plaintext: "Oh, Alice... I love you too!"



Alice's Modulus

```
2 1032370961 5021 130386866947386859 132278053560039391 053458528741 788869562031 0161
991 06720402080099454840426997527205 190779 169907529926 14878961 5239224497 10854734
5 12345034475741 91 2705772774 15 137279956399357021 97860066055531 01 72 148871 64536048
2622369754080 197423225929587332 139561 202602 1081 625306627032862928 10760641 554850
176739373567627023549 14850847553651 8448932699747760505425644895 1045079583 11 01 18
7240572030265003330 124937704275 164630994341 17 12304309200303280262 153201 70062365
65051 663071 754651 136866707250789471 18488285324999 122461 068339008474908739844860
53904652591 64 104303 1227308350 1461 74 124596429855785371 19 126709537
```

Ciphertext: RlhedUTajUGifRG0kMxT23+BzXObjTVKwS9uuPEM/8VsRV dAKjsY0xZNR  
kKqBivwFqXEA UhK9f0gZXYQsneFF+yZ+AaanTlI7MEFb/+bj7xj4ynUh49T  
w jEtQi9Ru/9ps+kARCWQpAHylz0XWFOCluoG7lUxLrIh2lkeboQLYXYiUUr  
fEA8jhpNoesPgLScmwQVX70uwjfiZwbHAY0JzNvXvX8uTnHtpVW8qV7e wi  
ALu48lOziDWgug3OqEfgUwui2ga2Rij4ZE/D057s5g75amOX7SIcmiWfao2T  
OIOLThcHNcMh4I2pzVXVjhkgpU3CvcFqK/rghQTG6l5A/57pw==

# History of encryption

After 1970s: Public key cryptography

## Alice's Modulus

```
2 1032370961 5021 130386866947386859 132278053560039391 053458528741 7888695620310161
991 06720402080099454840426997527205 190779 169907529926 14878961 5239224497 10854734
5 12345034475741 91 270577274 15 137279956399357021 97860066055531 01 72148871 64536048
2622369754080 197423225929587332 139561 202602 1081 625306627032862928 10760641 554850
176739373567627023549 14850847553651 8448932699747760505425644895 1045079583 1101 18
7240572030265003330 124937704275 164630994341 17 12304309200303280262 15320170062365
65051663071754651 136866707250789471 18488285324999 122461 068339008474908739844860
5390465259164 104303 12273083501461 74 124596429855785371 19126709537
```

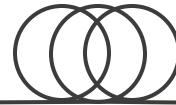
City A



Alice

Ciphertext:

```
RLhedUTajUGifRG0kMxT23+BzXObjTVKwS9uuPEM/8VsRVdAKjsY0xZNR
kKqBivwFqXEAUhK9f0gZXYQsneFF+yZ+AaanT1I7MEFb/+bj7xj4ynUh49Tw
jEtQi9Ru/9ps+kARCWQpAHylz0XWfoCluoG7IUxLrLh2lkebOqLYXYiUUr
fEA8jhpNoesPgLScmwQVX70uwjf/ZwbHAY0JzNvXvX8uTnHtpW8qV7eWi
ALu48lOziDWgug3OqEfgUwui2ga2Rij4ZE/D057s5g75amOX7SIcmiWfao2T
OIOLThcHNcMh4I2pzVXVjhkkgpU3CvcFqK/rgHQTG6l5A/57pw==
```



Communication channel



Bob

City B



Prime 1:

```
1 1872035424589255887822295232985654 1295 1771 3236 15952921 91 894268803592497669 1675
601 1868666926475365335279 1923 10459474294307098498862369566023 130992802706003177
54776825403086338 1846 1771 5972399091 0049344704205831 1 230878588833862794 16920979
70081 238920257380 125540496530346252387371 99556295929761 2976235841 1852661
```

Prime 2:

```
177 1589302870512864396861 6241 2785 1731 17 1831 48940069842892383591 7336482743983994
323084767204141014633595537614449 1626259142101054544621 65 163691 3846675404 133904
7805571 479209978004 14626489 1342743238 13 1955602792250822393703 203646442395073044
498 18658391 5449 169681 6261 76 11 32636708094399882956373874 11 965404396456317
```

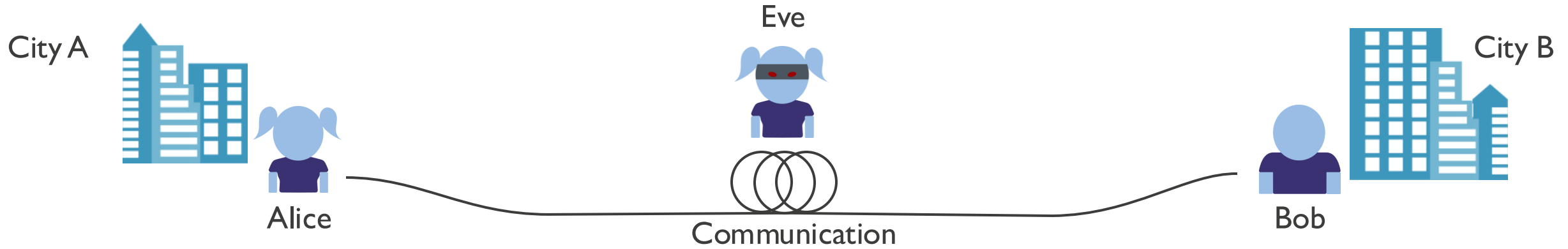
Plaintext: "Oh, Alice... I love you too!"

# History of encryption

After 1970s: Public key cryptography

Alice's Modulus

```
2 1032370961 5021 130386866947386859 132278053560039391 053458528741 7888695620310161
991 06720402080099454840426997527205 190779 169907529926 14878961 5239224497 10854734
5 12345034475741 91 2705772774 15 137279956399357021 97860066055531 01 72148871 64536048
2622369754080 197423225929587332 139561 202602 1081 625306627032862928 10760641 554850
176739373567627023549 14850847553651 8448932699747760505425644895 1045079583 11 01 18
7240572030265003330 124937704275 164630994341 17 12304309200303280262 15320170062365
65051 663071 754651 136866707250789471 18488285324999 122461 068339008474908739844860
53904652591 64 104303 1227308350 1461 74 124596429855785371 19126709537
```



Prime 1: 11872035424589255887822295232985654129517713236159529219189426880359249766916756011868666926475365335279192310459474294307098498862369566023130992802706003177547768254030863381846177159723990910049344704205831123087858883386279416920979700812389202573801255404965303462523873719955629592976129762358411852661

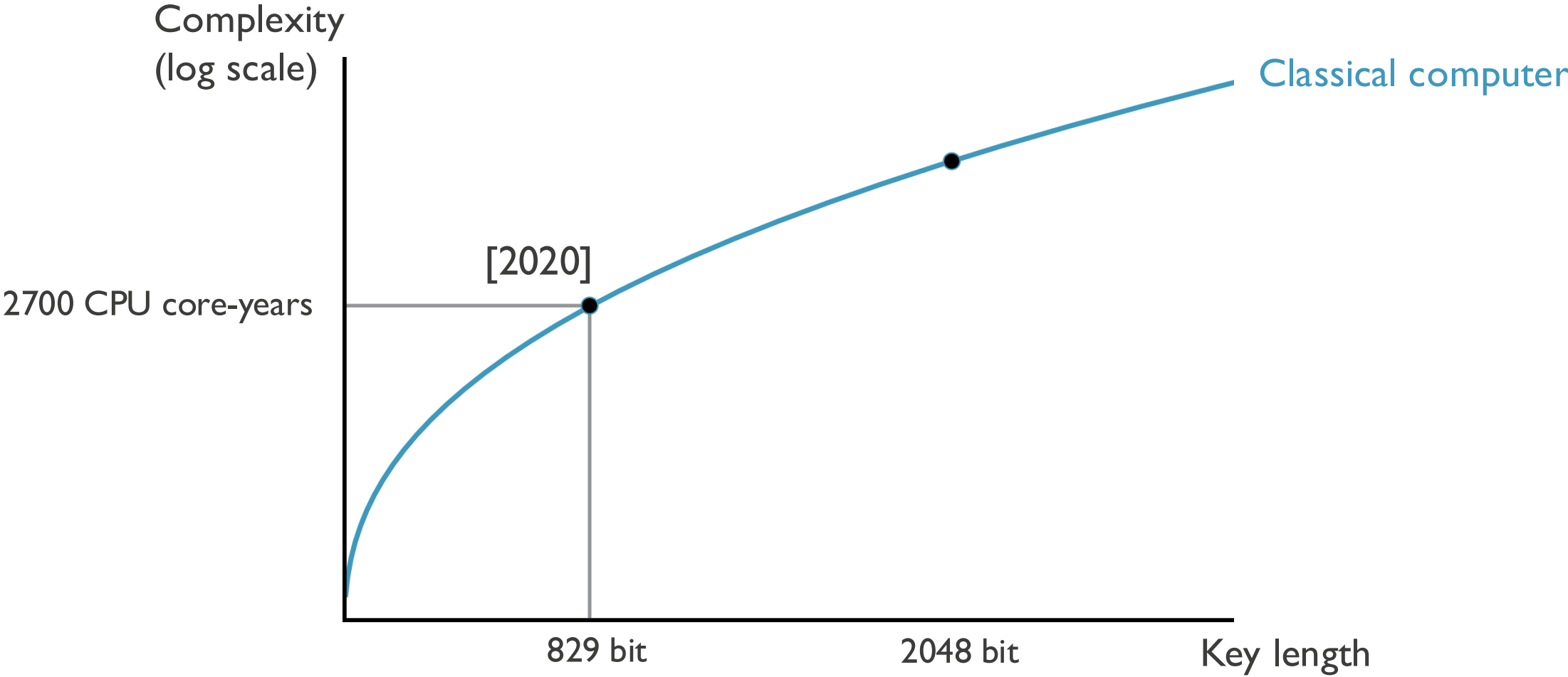
Prime 2: 177158930287051286439686162412785173117183148940069842892383591733648274398399432308476720414101463359553761444916262591421010545446216516369138466754041339047805571479209978004146264891342743238131955602792250822393703203646442395073044498186583915449169681626176113263670809439988295637387411965404396456317

Plaintext: "Oh, Alice... I love you too!"

Ciphertext: R.LhedUTajUGifRG0kMxT23+BzXObjTVKwS9uuPEM/8VsRVdAKjsY0xZNRkKqBivwFqXEAUhK9f0gZXYQsneFF+yZ+AaanTII7MEFb/+bj7xj4ynUh49TwjEtQi9Ru/9ps+kARCWQpAHylz0XWFOCluoG7IUxLrLh2lkebOqLYXYiUUr fEA8jhpNoesPgLScmwQVX70uwjff/ZwbHAY0JzNvXvX8uTnHtpW8qV7ewiALu48lOzlDWgug3OqEfgUwui2ga2Rij4ZE/D057s5g75amOX7SlCmiWfao2T OIOLThcHNcMh4I2pzXVXjhkgpU3CvcFqK/rghQTG6I5A/57pw==

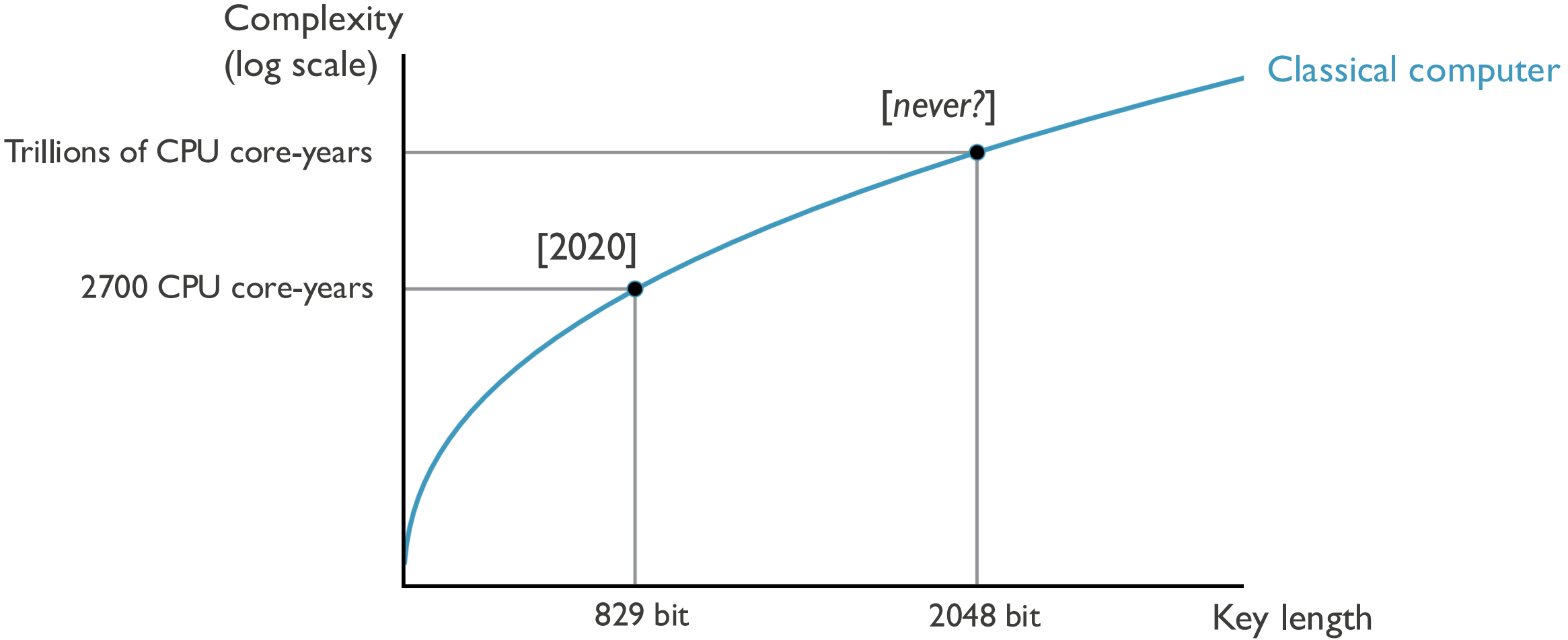
Decrypted text: "Oh, Alice... I love you too"

# RSA is very hard to break on a classical computer

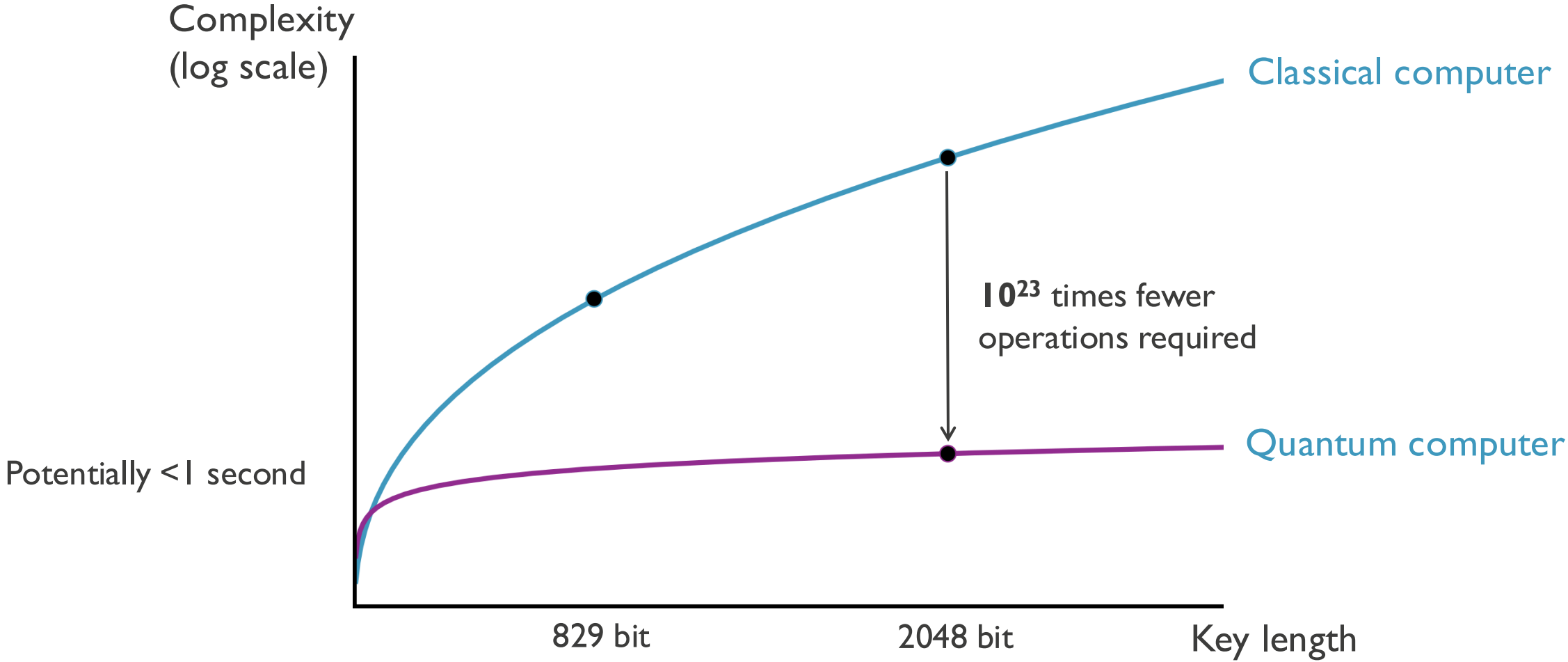




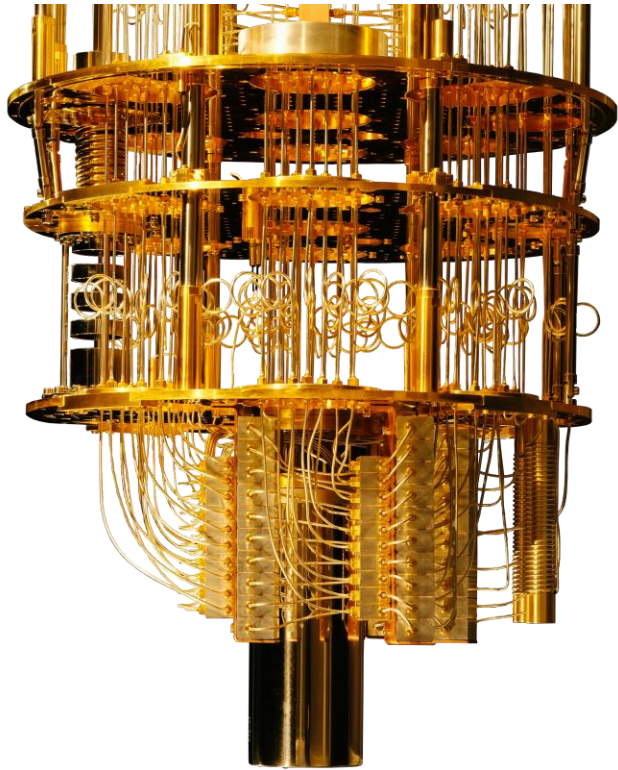
# RSA is very hard to break on a classical computer



# RSA is not hard to break on a quantum computer



# The threat being posed by quantum computers



Access to new, and **more efficient**  
quantum algorithms

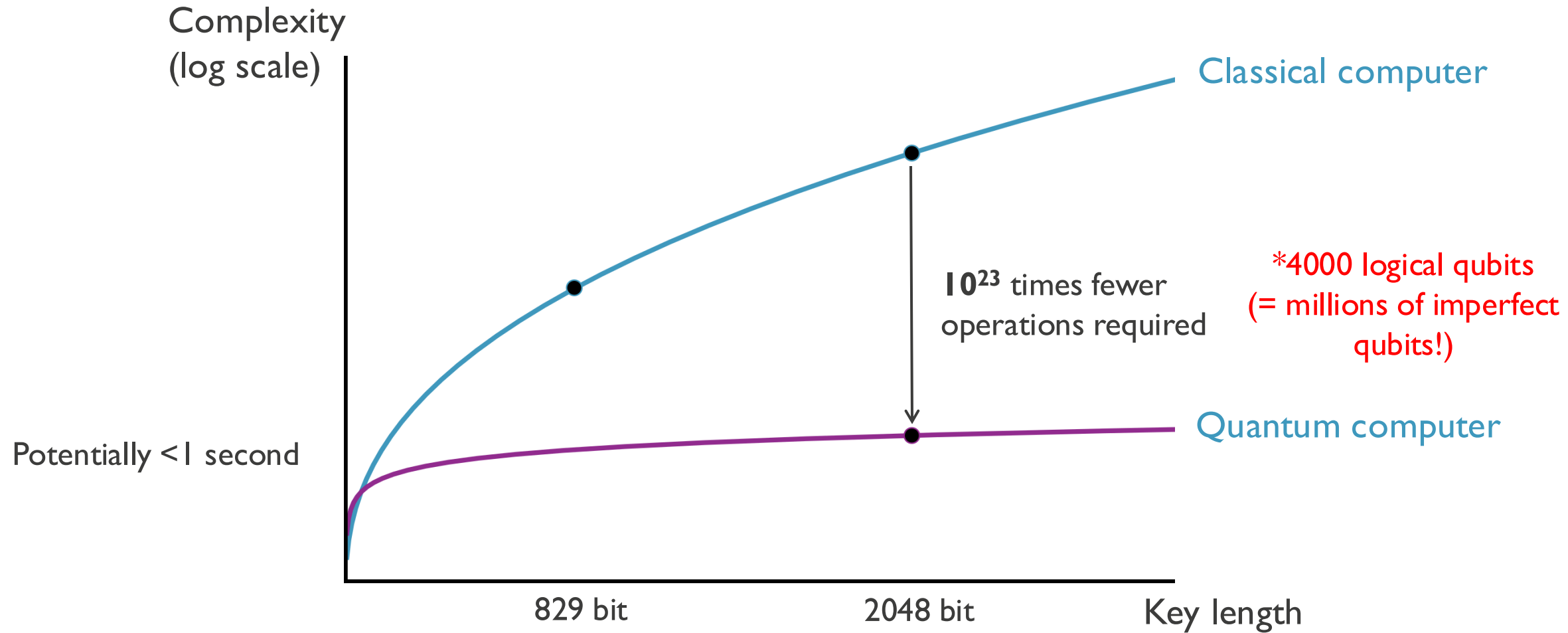


Public key cryptography **broken**

























**Internet communication no longer secure**

# RSA is not\* hard to break on a quantum computer



# Quantum Computing Market Map

Non exhaustive and in no particular order. Excludes details on control systems, assembly languages, circuit design, etc.

Users <i>Select examples</i>	Applications <i>Not mapped to verticals</i>	Software offerings <i>Includes control software</i>	QPUs <sup>2</sup>		Hardware / components <i>Select examples only – not representative of entire ecosystem</i>
Material Science	Not strictly categorized given diversity of operations <sup>1</sup>		Superconducting		Cryogenics (includes testing)
					
Finance					
			<p data-bbox="1248 721 1516 778">Ion Trap</p> <p data-bbox="1643 721 2020 778">Neutral Atoms</p> <p data-bbox="2025 721 2517 778">Lights and lasers</p> 		
Life Sciences			<p data-bbox="1248 949 1516 1006">Silicon</p> <p data-bbox="1643 949 2020 1006">Photonics</p> 		<p data-bbox="2025 949 2517 1006">Other componentry (examples)</p> 
	<p data-bbox="389 1085 779 1142">Cloud access to QPUs</p> <p data-bbox="784 1085 1243 1142">Simulators / q-inspired / etc</p> 		<p data-bbox="1248 1185 2020 1242">Other</p> 		
					

<sup>1</sup> Software offerings can be further classified into SDKs, firmware / enablers, algorithms / applications, simulators etc. but many companies are offering a mixture across the stack

<sup>2</sup> Many QPU providers are offering full stack services (e.g. Pasqal acquired Qu&Co, Quantinuum was originally CQC prior to merger with HQS, etc.)



# Mosca's theorem

**If  $x + y > z$ , then worry**

**X: security shelf life**  
**Y: migration time**  
**Z: collapse time**

# Quantum-resistant cryptography

Two paths towards making cybersecurity quantum-proof

## Post-Quantum Cryptography ('PQC')

Upgrading public key cryptography schemes against quantum algorithms

- Drop-in replacement
- Based on assumptions

# Quantum-resistant cryptography

Two paths towards making cybersecurity quantum-proof

## Post-Quantum Cryptography ('PQC')

Upgrading public key cryptography schemes against quantum algorithms

- Drop-in replacement
- Based on assumptions



### NEWS

## NIST Releases First 3 Finalized Post-Quantum Encryption Standards

August 13, 2024



- NIST has released a final set of encryption tools designed to withstand the attack of a quantum computer.
- These post-quantum encryption standards secure a wide range of electronic information, from confidential email messages to e-commerce transactions that propel the modern economy.
- NIST is encouraging computer system administrators to begin transitioning to the new standards as soon as possible.

<https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>

# Quantum-resistant cryptography

Two paths towards making cybersecurity quantum-proof

## Post-Quantum Cryptography ('PQC')

Upgrading public key cryptography schemes against quantum algorithms

- Drop-in replacement
- Based on assumptions

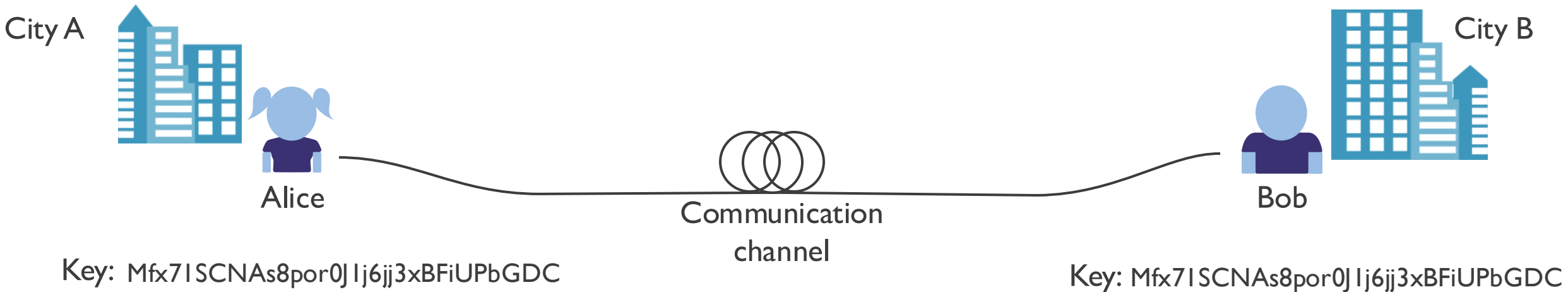
## Quantum Cryptography (e.g. QKD)

Employing quantum mechanics to enable secure communication

- Hardware-based, expensive (for now)
- Ultimate security

# Quantum key distribution

Securely sharing a secret key between Alice and Bob

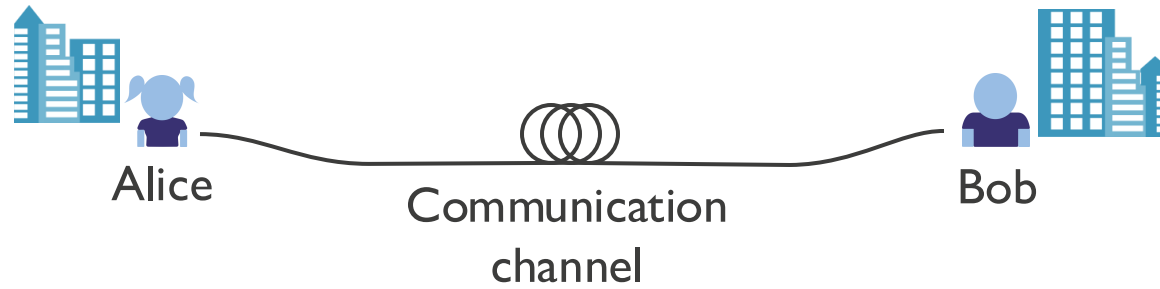


How do we securely share a key between Alice and Bob?

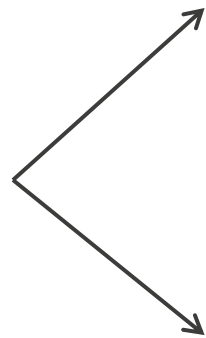


# Quantum key distribution

Securely sharing a secret key between Alice and Bob

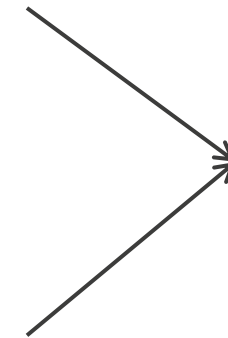


We can use the unique properties of quantum mechanics!



no-cloning principle

Heisenberg's uncertainty principle



**Unconditional security!**

# Quantum-resistant cryptography

Two paths towards making cybersecurity quantum-proof

## Post-Quantum Cryptography ('PQC')

Upgrading public key cryptography schemes against quantum algorithms

- Drop-in replacement
- Based on assumptions

## Quantum Cryptography (e.g. QKD)

Employing quantum mechanics to enable secure communication

- Hardware-based, expensive (for now)
- Ultimate security

BeQCI use cases

BeQCI research

# QKD is already available on the market

**TOSHIBA**



Multiplexed QKD System [Read More](#) Long Distance QKD System [Read More](#)



**Clavis XG QKD System**

- ▶ Long range (up to 150 km)
- ▶ Higher key rate on short distances: typical 14000 AES-256 Keys per hour @ 24 dB
- ▶ Complex network topologies (ring, hub and spoke, meshed, star)
- ▶ Controlled and monitored centrally
- ▶ Interoperability with major Ethernet and OTN encryptions

[PRODUCT DETAILS](#)



**Cerberis XG QKD System**

- ▶ Short/medium range (up to 90km)
- ▶ Standard key rate: typical 14000 AES-256 Keys per hour @ 18 dB
- ▶ Complex network topologies (ring, hub and spoke, meshed, star)
- ▶ Controlled and monitored centrally
- ▶ Interoperability with major Ethernet and OTN encryptions

[PRODUCT DETAILS](#)



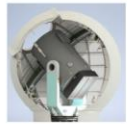
**LuxQuanta® NOVA LQ®**  
Quantum Key Distribution | CV-QKD

NOVA LQ® is our first Quantum Key Distribution solution for distributing highly secure keys in metropolitan networks. The continuous variable technology inside (CV-QKD) allows the integration of the system into existing optical fiber links, coexisting with conventional telecommunication technologies.

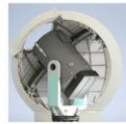
[Contact us](#) [Request brochure](#)



## Free Space Quantum Key Distribution



Optical Ground Station 40cm: OGS 400 [READ MORE](#)



Optical Ground Station 80cm: OGS 800 [READ MORE](#)



Space-Qualified Quantum Sources [READ MORE](#)

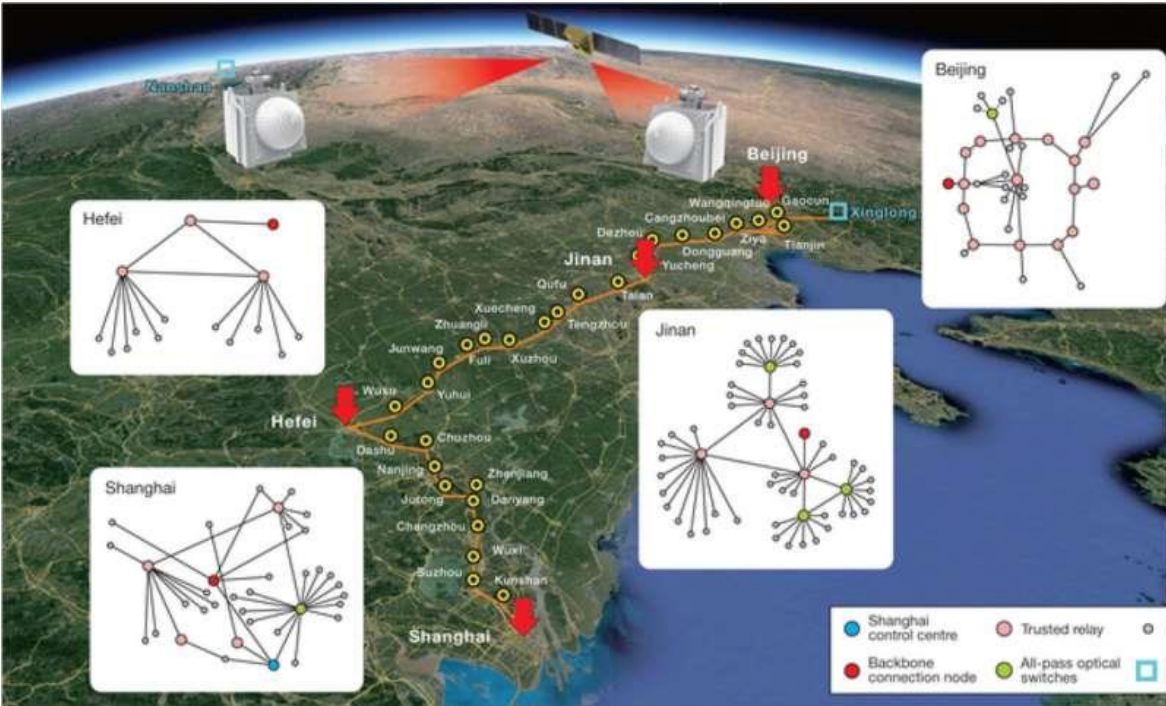


Free-Space Terrestrial Link [READ MORE](#)



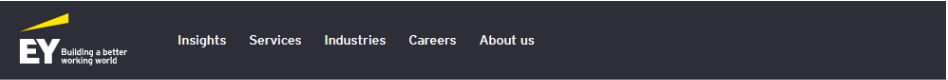
# QKD is maturing and being deployed worldwide

## Example: China



700 fibers, 2 ground-to-sat stations  
 QKD over 4600km available

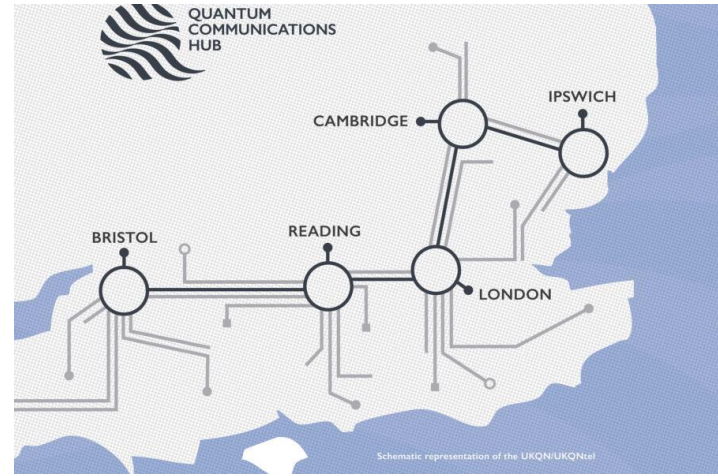
## Example: UK



Press release  
 27 Apr 2022 | London, GB

BT and Toshiba launch first commercial trial of quantum secured communication services - EY becomes first commercial customer

*commercial & non-commercial initiatives*



# EuroQCI: European Quantum Communication Infrastructure initiative

Towards technological autonomy in quantum communications

Advanced national QCI networks  
using existing telco infrastructure

Public & private use cases



EU technologically autonomous  
quantum communications industry

Raise awareness and skill-level



# BeQCI: the first Belgian quantum communication testbed

## Objectives and activities

### Deployment of QKD network

*4 phases*

*4 technologies*

### Demonstration of use cases

*government, hospitals, banks, research centers,  
universities, NGOs ...*

### Cross-border connections

*Connect to LuxQCI*

*Prepare for EU-wide network: EuroQCI*

### Research to strengthen QKD

*chipscale transceivers*

*post-quantum cryptography*

*fiber-compatible quantum memories,  
security analysis of QKD protocols & infrastructure*

# Rollout in 3 phases of 6 months, starting early 2024



LUXQUANTA (CV)  
CONNECTS 2 SITES



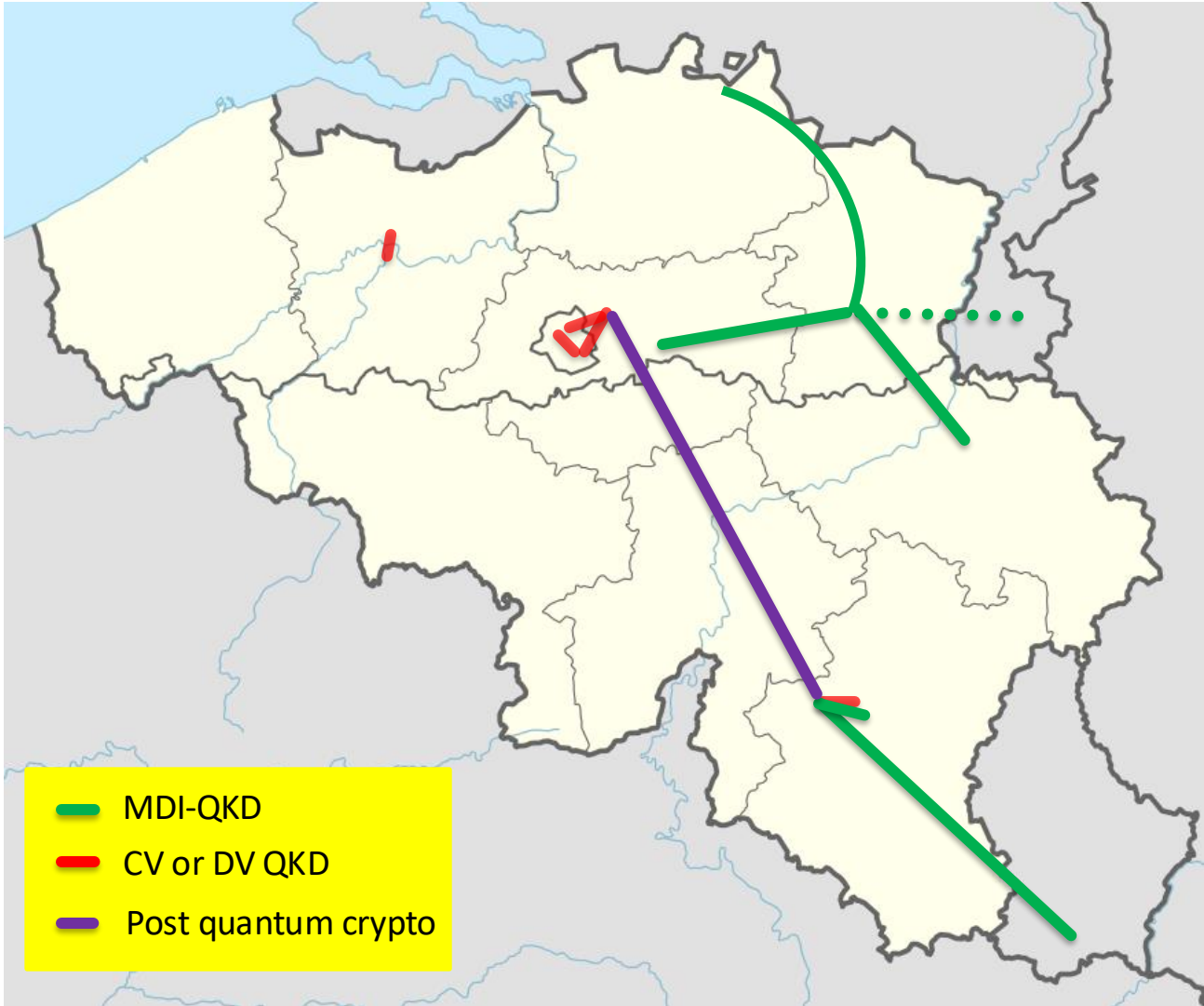
THINKQUANTUM (DV)  
CONNECTS 2 SITES



IDQUANTIQUE (DV)  
CONNECTS 2 SITES

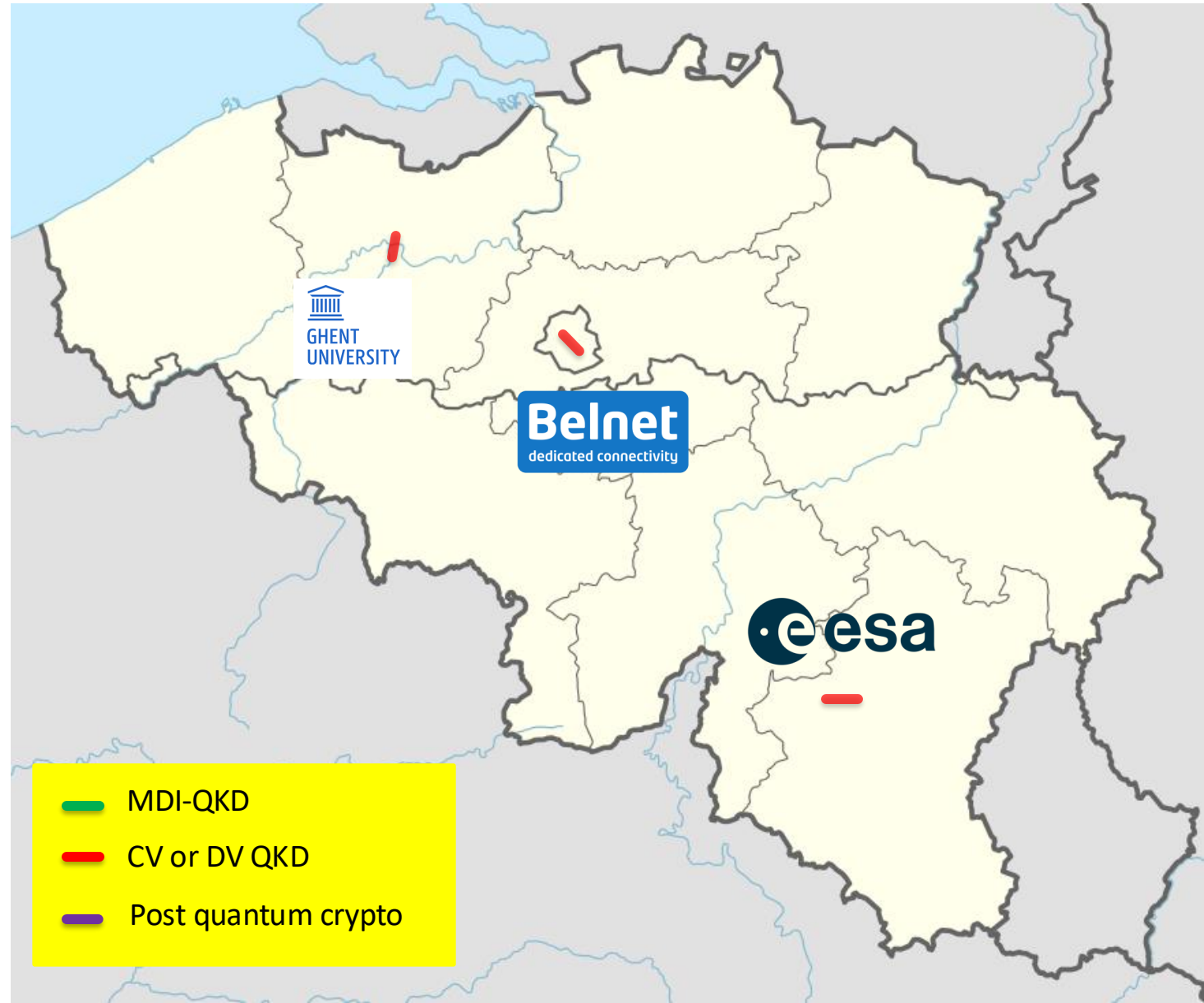
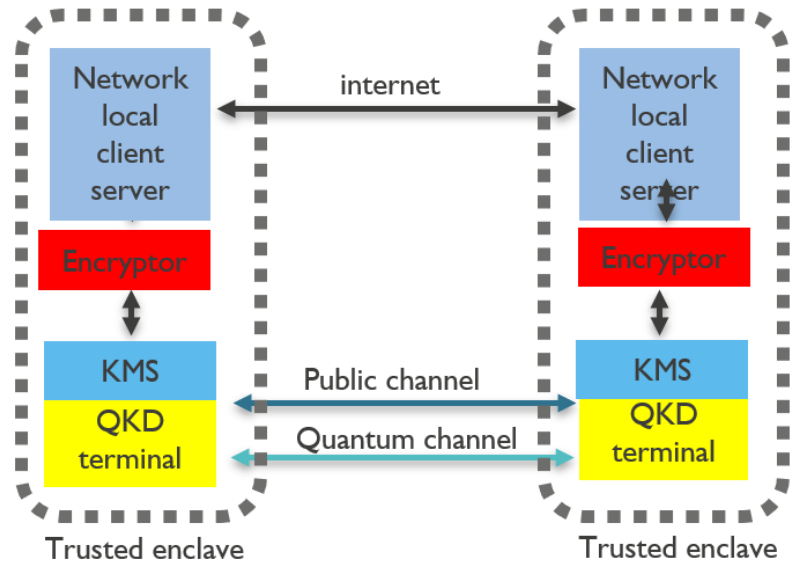


Q\*BIRD (MDI)  
CONNECTS 5 SITES  
ONE STEP CLOSER TO QCI



# Phase I: Hello World 😊

- Starting simple: point-to-point
- Getting to know the QKD systems
- 3 short links with 6 commercial boxes



# First use cases are deployed and operational



LUXQUANTA (CV)  
CONNECTS 2 SITES

5.1 km QKD link  
between two campuses  
in Gent.  
**Use case:** research +  
co-existence classical  
communications



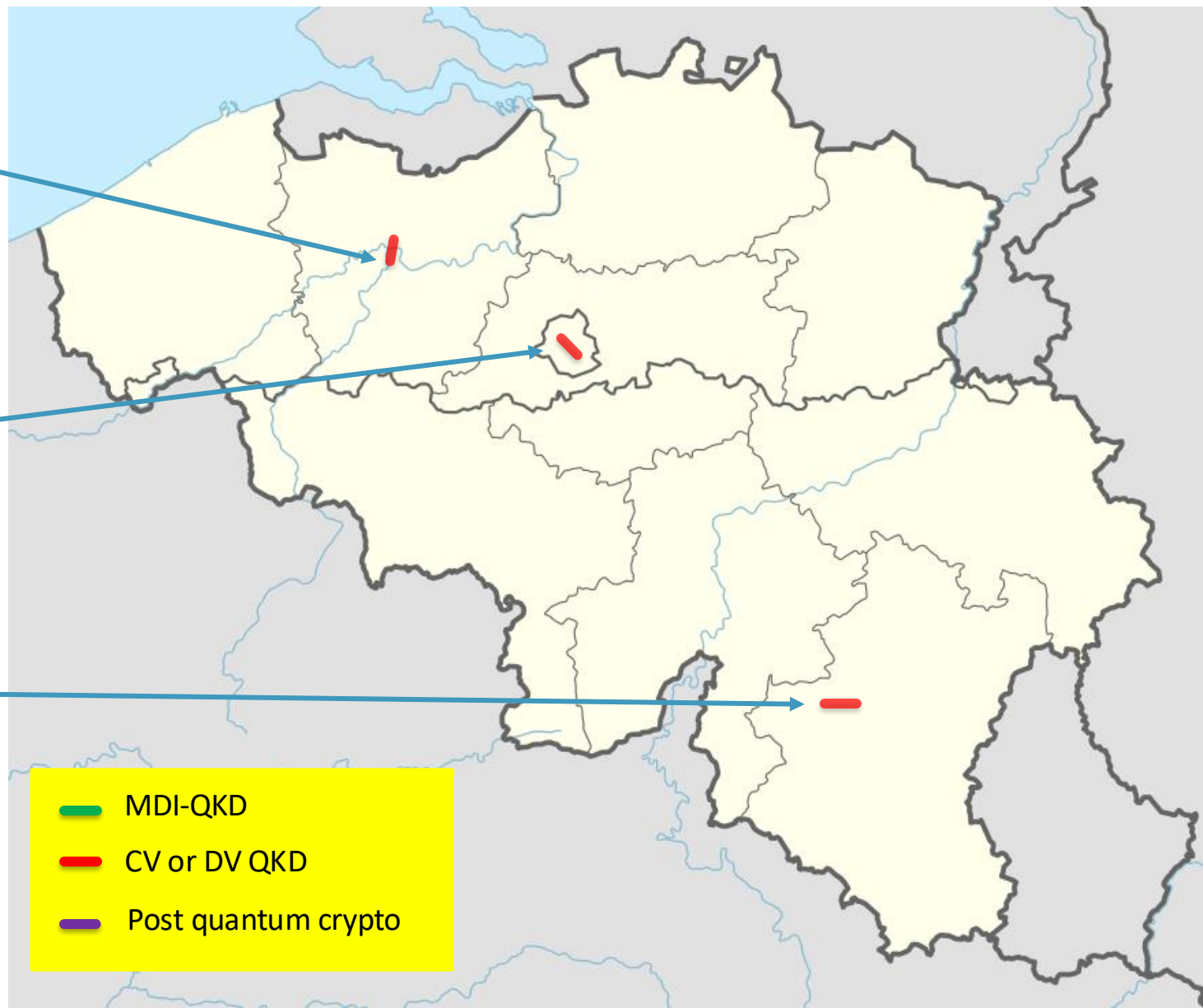
THINKQUANTUM (DV)  
CONNECTS 2 SITES

QKD link between two  
Belnet datacenters.  
**Use case:** data  
transfer, network  
management



IDQUANTIQUE (DV)  
CONNECTS 2 SITES

QKD link between  
Redu and Transinne.  
**Use case:** IoT  
middleware integration  
with QKD

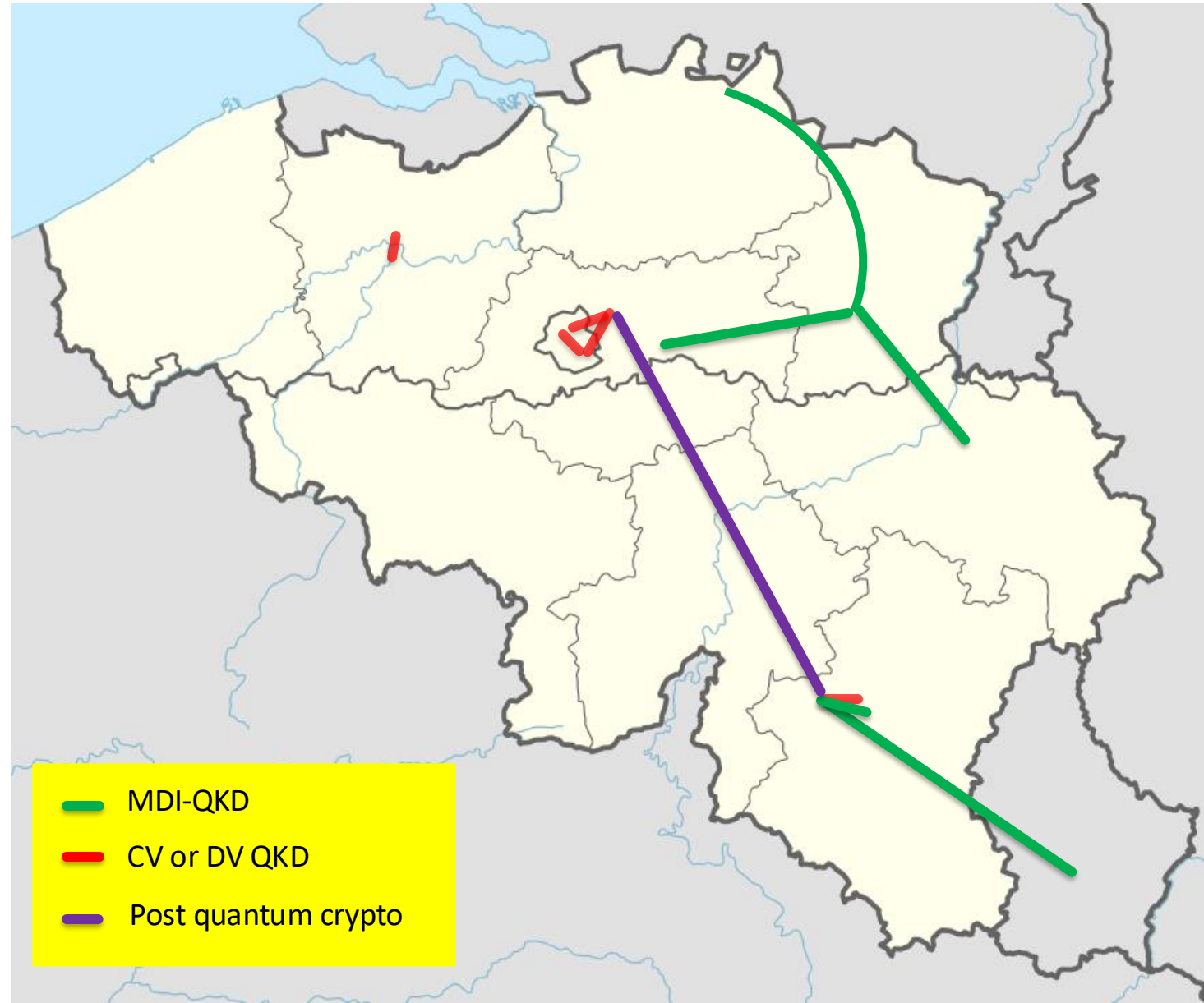




# Next steps: expand and increase complexity of the network

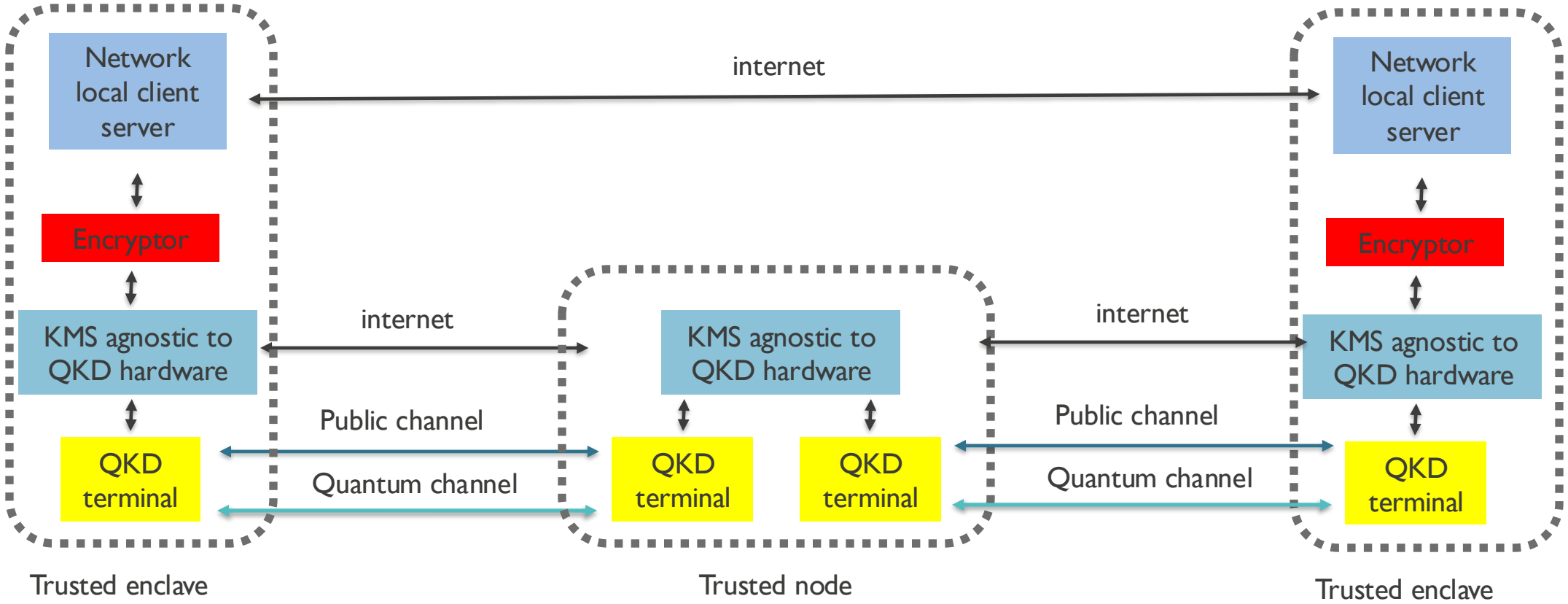
Exploring non-trivial connectivity:

- Trusted nodes
- Interface of different systems
- Loop topology
- Cross-border link: Lux4QCI

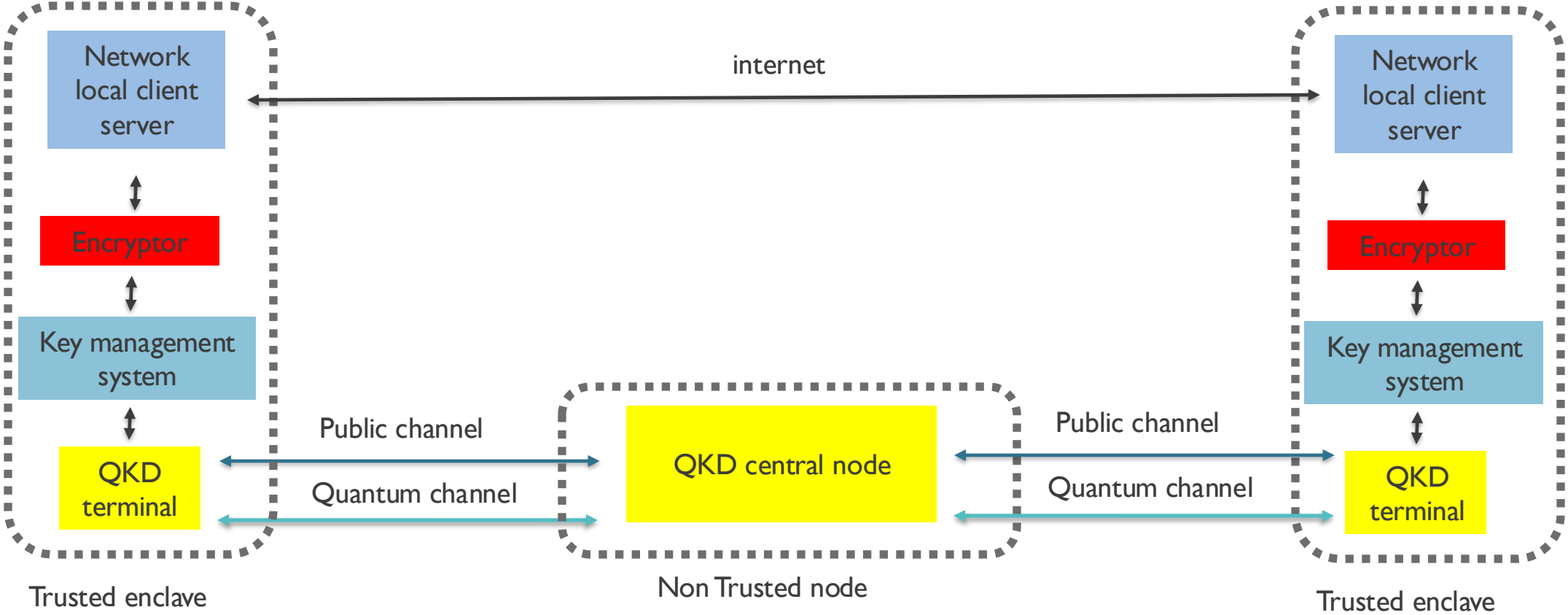




# Point-to-point with trusted nodes



# Point-to-point with central node



# Next steps: expand and increase complexity of the network

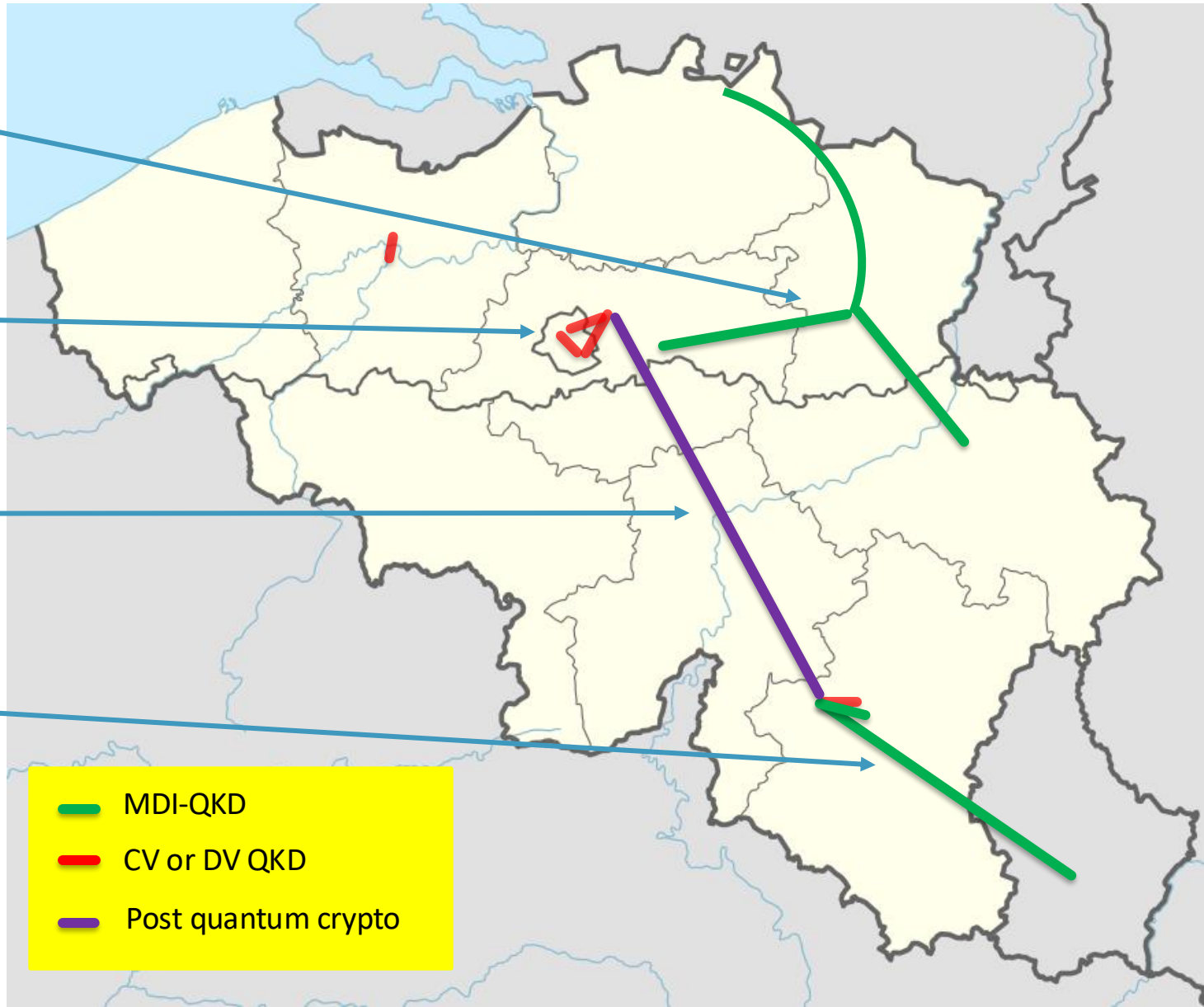
MDI-QKD deployment in Hasselt

Extend the network in Brussels with trusted nodes and hybrid technology for more complex use cases

PQC link between Brussels and Redu

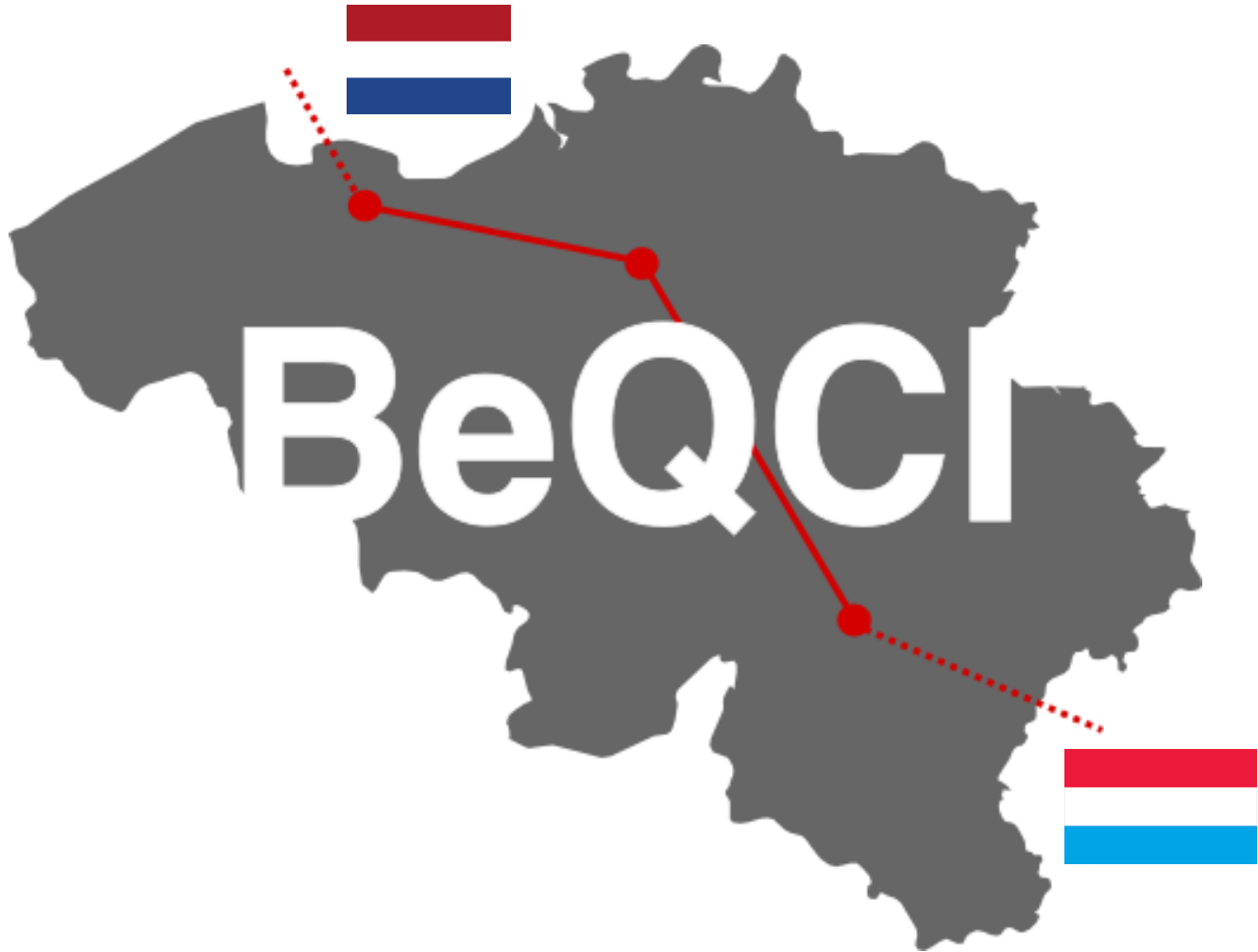
Cross-border link with Luxembourg as first collaboration to establish a European QCI

Open for external end users!



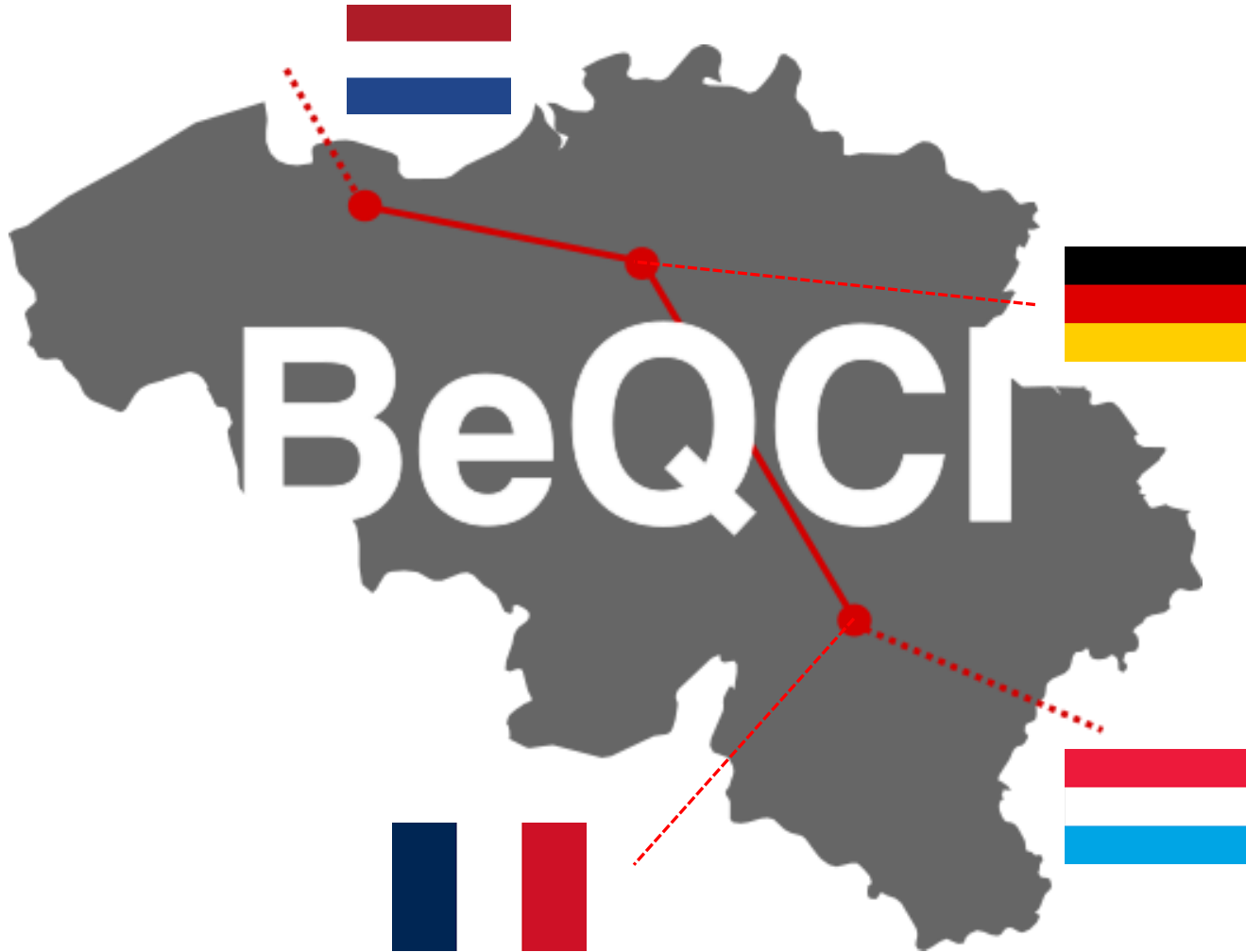
- MDI-QKD
- CV or DV QKD
- Post quantum crypto

# Beyond mid-2025: cross-border & space



- Cross-border connection of national networks:

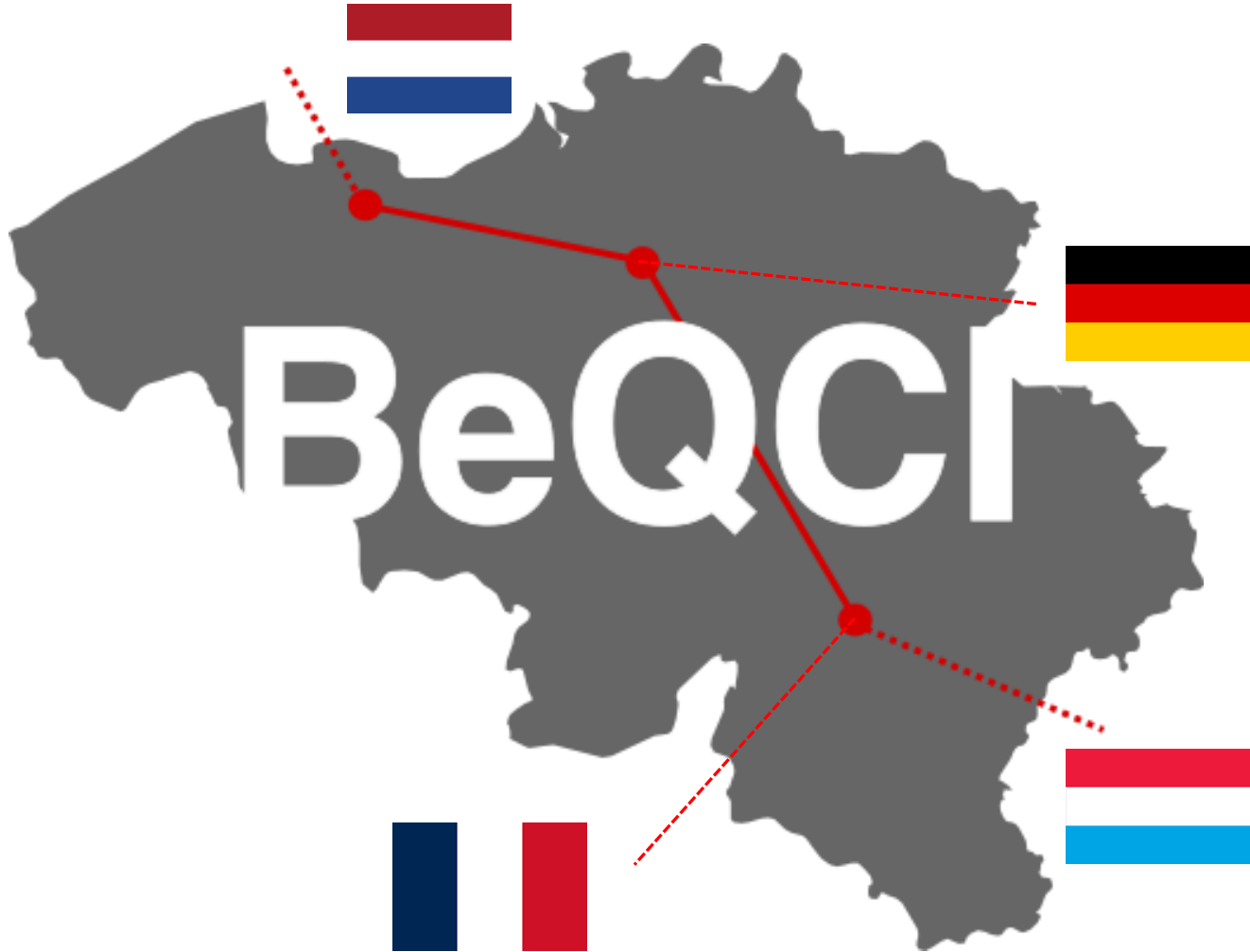
# Beyond mid-2025: cross-border & space



- Cross-border connection of national networks:
  - For example *Benelux backbone*: Amsterdam-Rotterdam-Brussels-Luxembourg



# Beyond mid-2025: cross-border & space

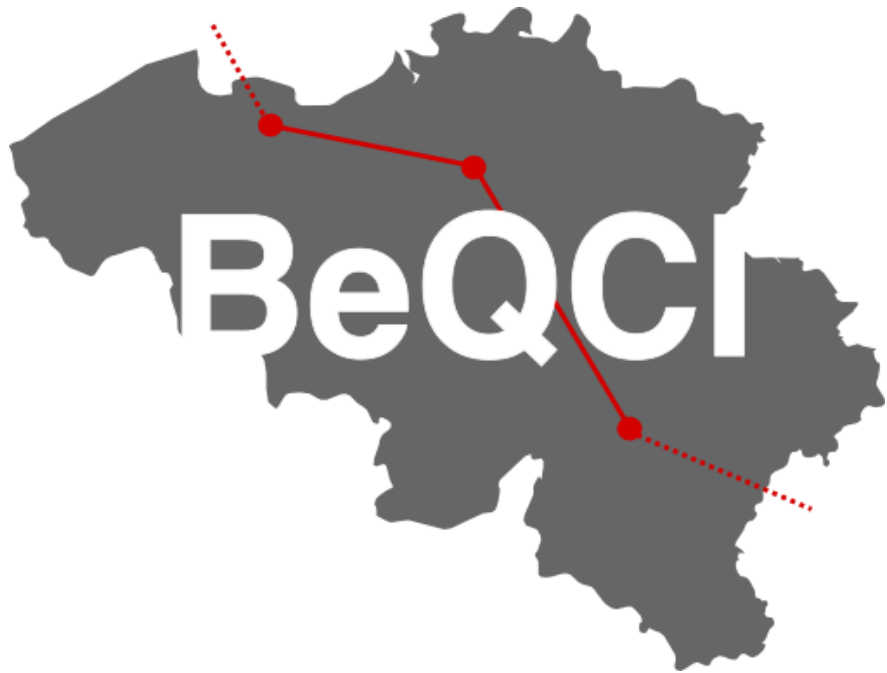


- Cross-border connection of national networks:
  - For example *Benelux backbone*: Amsterdam-Rotterdam-Brussels-Luxembourg
- Option: Satellite ground station at ESEC to connect to ESA's space segment (Eagle-I)



# Join the first Belgian QCI testbed!

*Could quantum secure data transmission be useful for your organization?*



- Realization of **selected QKD use cases**
  - **Training and testing facilities**
  - For **government, non-profit & companies**
    - **User community**

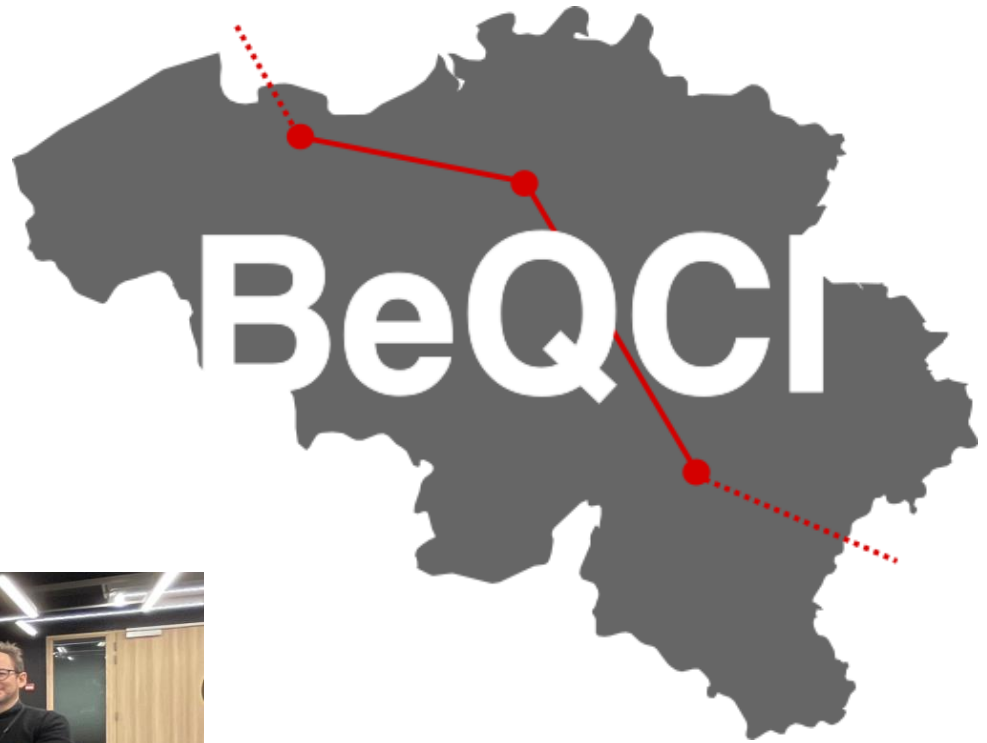
*Learn more & explore the possibilities:*

[www.beqci.eu](http://www.beqci.eu)

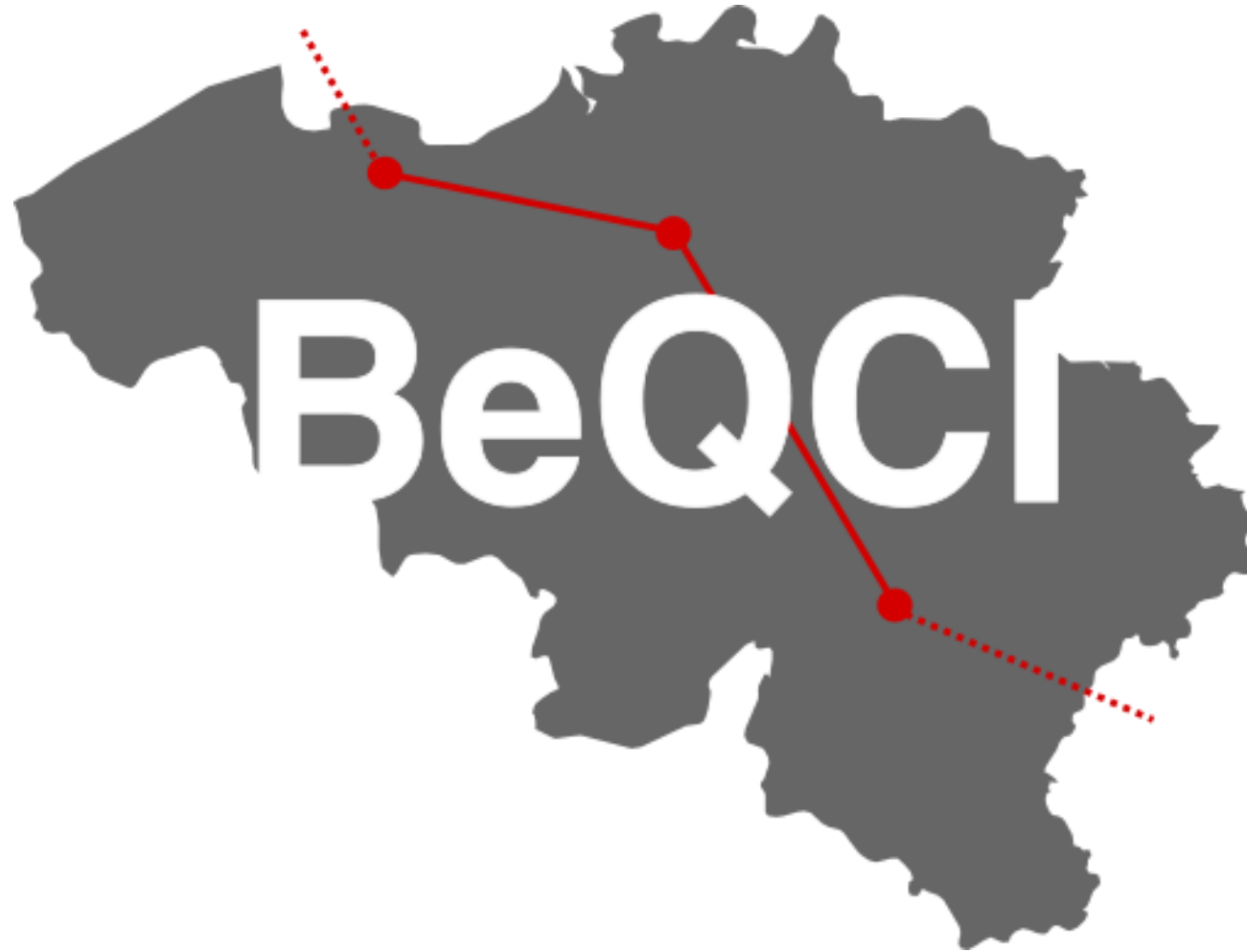
[info@beqci.eu](mailto:info@beqci.eu)

[Karel.Dumon@imec.be](mailto:Karel.Dumon@imec.be)

# BeQCI: the first Belgian quantum communication testbed



Funded by EU & BELSPO



# BeQCI: Belgium Quantum Communication Infrastructure

Cyberweek – 17/10/2024 - [karel.dumon@imec.be](mailto:karel.dumon@imec.be)



CENTRE FOR  
**CYBERSECURITY**  
BELGIUM

**Ellen Stassart**

CCB





CENTRE FOR  
CYBERSECURITY  
BELGIUM

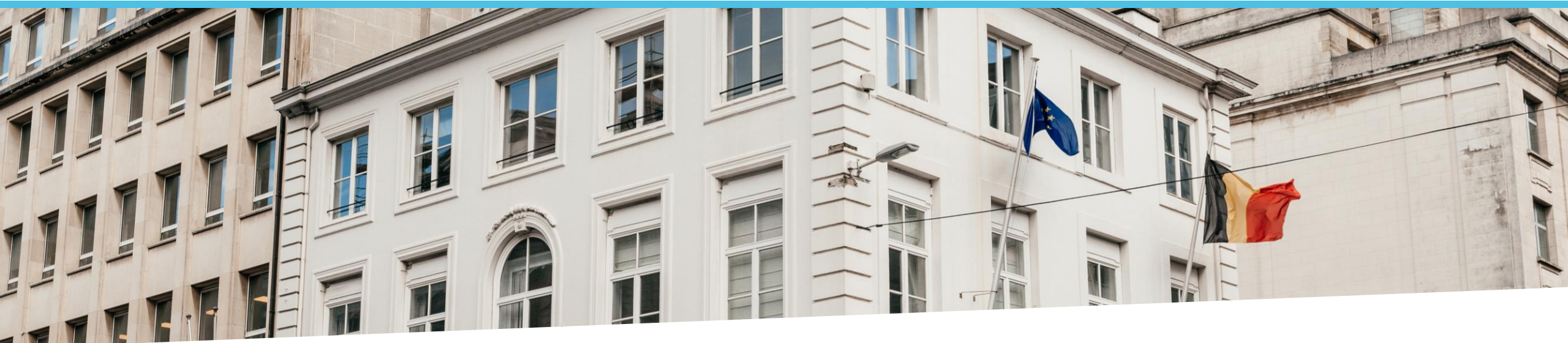


**NCC-BE**

BELGIUM CYBERSECURITY  
COORDINATION CENTRE



Centre for Cybersecurity Belgium  
*Under the authority of the Prime Minister*



# ● Le cadre ECCC et le NCC-BE à l'appui de la recherche sur la cybersécurité

17 October 2024 – Cyberweek, Namur

Ellen STASSART – Director CCB & Head of the NCC-BE



# ● Agenda

1

Qu'est-ce que le CCB?

2

Introduction de l'ECCC et du NCC-BE

3

Le NCC-BE en pratique

4

Sources de financement disponibles

5

Points à retenir

6

Questions et réponses + session interactive

—

01

# Le Centre pour la Cybersécurité Belgique «Le CCB »



# Centre for Cybersecurity Belgium (CCB)



*Sous l'autorité du premier ministre*

- **Créé par l'Arrêté Royal du 10 octobre 2014**, c'est l'autorité nationale pour la cybersécurité
- Responsable de la mise en oeuvre de NIS1 & NIS2
- Le CCB désigné comme centre national de coordination pour la cybersécurité: le **"NCC-BE"** par arrêté royal du 16 février 2022



Notre mission est de faire de la Belgique l'un des pays les moins vulnérables d'Europe

Ceci est fait grâce

- › A la stratégie nationale du CCB

Stratégie Nationale  
de la cybersécurité 2.0  
vers la 3.0



- › L'approche de **cyber protection active (ACP)**



Construire la  
confiance

Partager les  
connaissances

Comprendre  
la menace

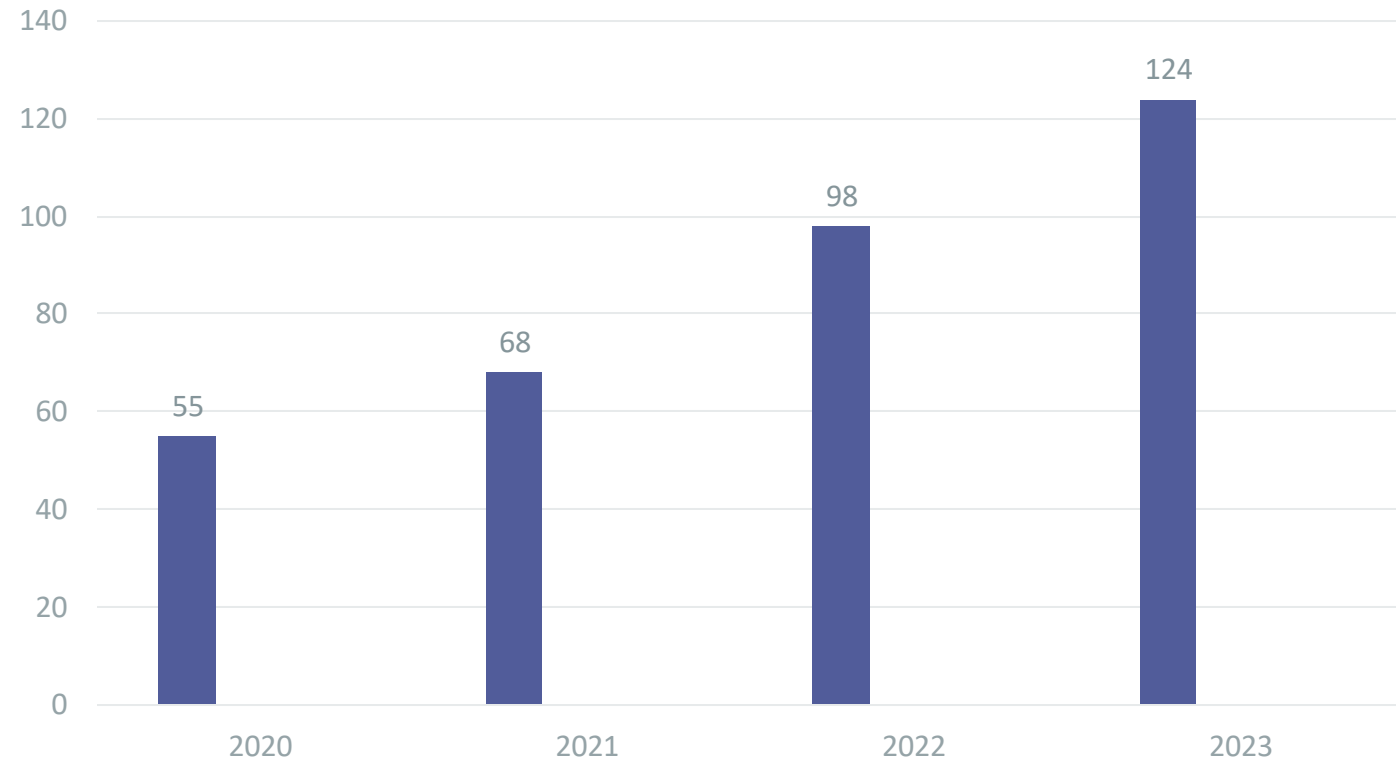


# Quelques chiffres

## Crises nexus

- ✓ COVID
- ✓ Conflits / guerres
- ✓ Cyber-attacks
- ✓ Cyber-espionage
- ✓ Nouveaux règles UE
- ✓ NCC-BE
- ✓ NCCA
- ✓ Future?

## Personnel



—

02

# European Cybersecurity Competence Centre « ECCC »

# Introduction de l'ECCC

*L'ECCC est le moteur de la mise en œuvre de la stratégie européenne en matière de recherche, d'innovation et de politique industrielle dans le domaine de la cybersécurité.*

Officiellement fondé en 2021. Sa création repose sur le Règlement (UE) 2021/887, adopté par le Parlement européen et le Conseil le 20 mai 2021.



# Sources de financement européen (2021-2027)



Digital Europe Programme

Horizon Europe

European Cybersecurity Competence Center

Réseau de centres de  
coordination nationaux  
(NCC)

Projets de renforcement des  
capacités

Projets de R&D collaboratifs

Co-investissement par l'industrie sur  
une base projet

Co-investissement par les États  
membres (volontaire)

# National Coordination Centres (NCCs)




Nominated by Member States as the national contact point, and notified to the Commission (One NCC per Member State)



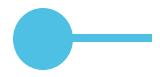
National capacity building: NCCs can effectively engage and coordinate with industry, academia and research community, citizens, and the public sector and authorities under NIS



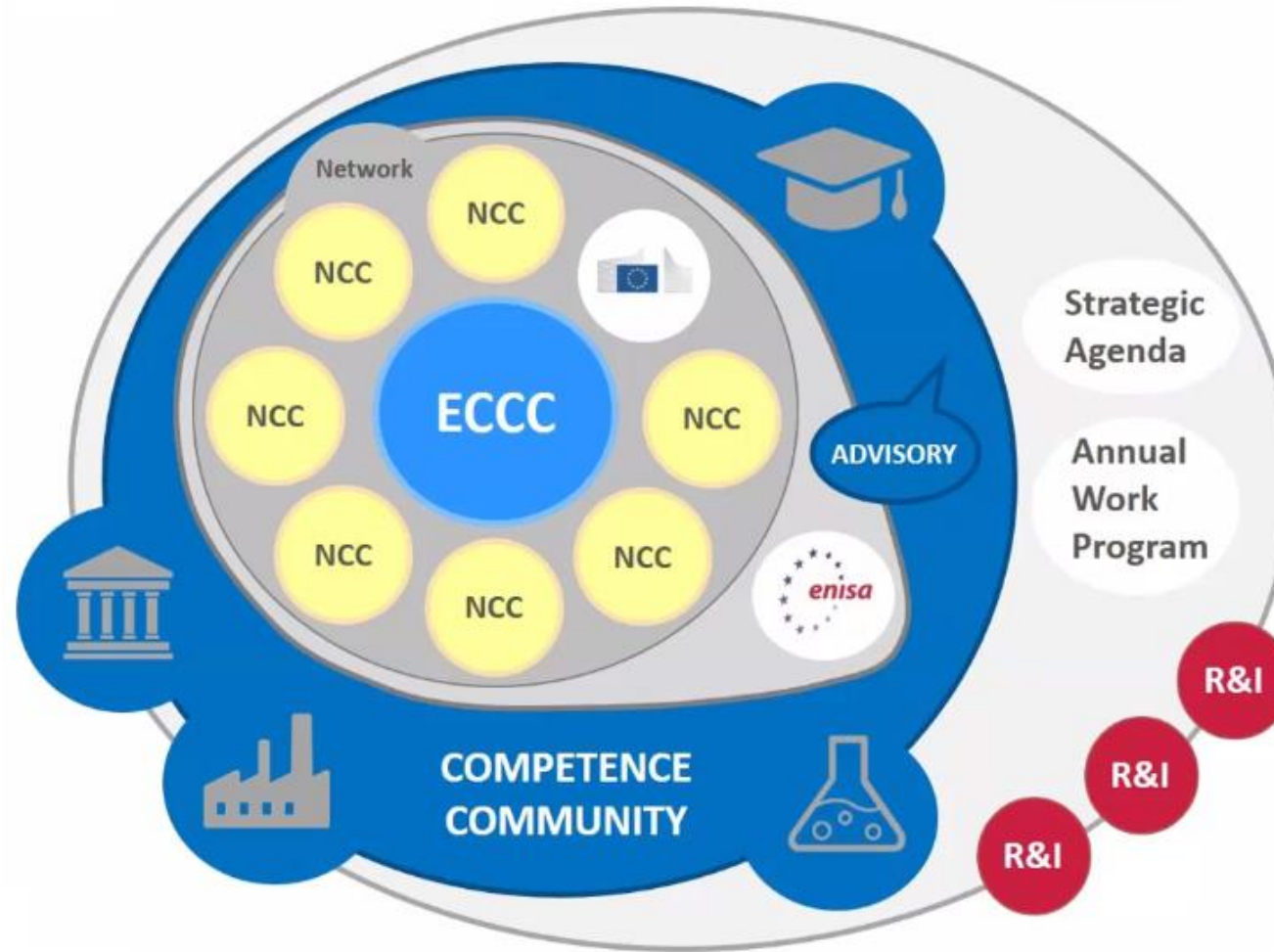
NCCs may receive funding, may pass on financial support

- 
- *Provides technical assistance*
  - *Coordinates the national, regional and local levels*
  - *Promotes cybersecurity educational programmes*
  - *Advocates involvement of relevant entities*





# Un nouveau cadre européen



Source: ENISA

# Objectifs du nouveau cadre européen



Renforcer le 'leadership' global de l'UE en matière de cybersécurité et **son autonomie stratégique**

Préserver et développer **les capacités technologiques et industrielles** dans le domaine de la recherche sur la cybersécurité

Renforcer la **compétitivité de l'industrie** de la cybersécurité

Faire de la cybersécurité **un avantage concurrentiel** pour les autres secteurs



**ECCC**   
EUROPEAN CYBERSECURITY  
COMPETENCE CENTRE

—

03

# Le NCC-BE en pratique

En 2022, le CCB a été désigné comme le centre national de coordination pour la Belgique (NCC-BE)



Ses missions légales sont les suivantes :

1. Coordonner **les investissements de l'UE** (DEP et HE) – y compris le FSTP ;
2. Soutenir **les missions stratégiques du Centre de compétence européen** – renforcement des capacités nationales ;
3. Agir en tant que **point de contact national** pour le cadre de l'ECDC.



De plus, le NCC-BE devrait servir de **plateforme pour la coordination et la collaboration entre les parties prenantes belges** des secteurs industriel, académique et de la recherche, ainsi que les citoyens, le secteur public et les autorités dans le cadre de la NIS.

## Comment demander un financement de l'UE?

Le NCC-BE en tant que 'navigateur avisé' pour aider et soutenir les candidats belges, y compris *les chercheurs*

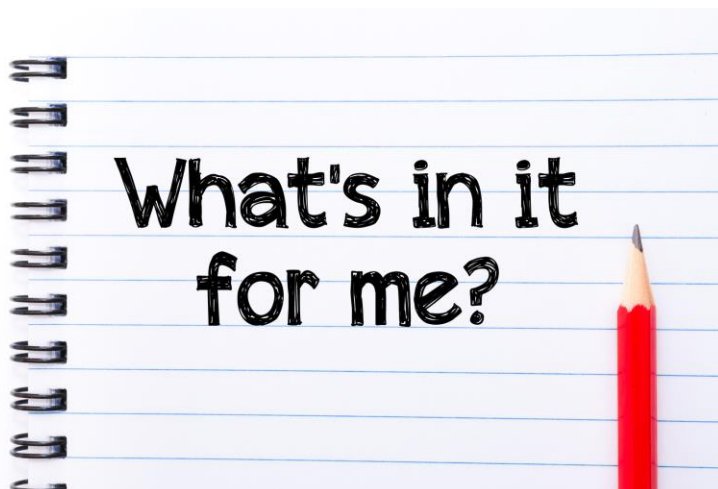




# Les possibilités de financement sont multiples



# Les avantages



- Une **approche plus structurée des investissements** dans la cybersécurité au sein de la BE ;
- Connaître **les prochaines possibilités de financement** de l'UE dans le domaine de la cybersécurité ;
- Possibilité **d'influencer les programmes de travail de l'UE** sur la cybersécurité ;
- Établir et renforcer les relations et la **collaboration intersectorielles et transfrontalières.**

# En pratique: comment?

## Co-design Belgium's Cybersecurity Future

Event - 19/09/2024

—

04

# Current Cybersecurity calls under DEP and HE

2021 - 2027

Digital Europe Programme (DIGITAL)

Call

Submission status

All filters

- Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2024)**  
DIGITAL-ECCC-2024-DEPLOY-CYBER-07-CYBERSEC-02 | Call for proposal  
Opening date: 04 July 2024 | Next deadline: 21 January 2025 | Single-stage

Programme: Digital Europe Programme (DIGITAL) | Type of action: DIGITAL JU Simple Grants
- Deploying The Network of National Coordination Centres with Member States**  
DIGITAL-ECCC-2024-DEPLOY-NCC-06-MS-COORDINATION | Call for proposal  
Opening date: 29 February 2024 | Next deadline: 28 November 2024 | Multiple Cut-off

Programme: Digital Europe Programme (DIGITAL) | Type of action: DIGITAL Simple Grants
- Preparedness Support and Mutual Assistance, Targeting Larger Industrial Operations and Installations**  
DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER | Call for proposal  
Opening date: 04 July 2024 | Next deadline: 21 January 2025 | Single-stage

Programme: Digital Europe Programme (DIGITAL) | Type of action: DIGITAL JU Grants for Financial Support
- National SOCs**  
DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOC | Call for proposal  
Opening date: 04 July 2024 | Next deadline: 21 January 2025 | Single-stage

Programme: Digital Europe Programme (DIGITAL) | Type of action: DIGITAL JU Simple Grants
- Enlarging existing or Launching New Cross-Border SOC Platforms**  
DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCPLAT | Call for proposal  
Opening date: 04 July 2024 | Next deadline: 21 January 2025 | Single-stage

Programme: Digital Europe Programme (DIGITAL) | Type of action: DIGITAL JU Simple Grants
- Strengthening the SOC Ecosystem**  
DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCSYS | Call for proposal  
Opening date: 04 July 2024 | Next deadline: 21 January 2025 | Single-stage

Programme: Digital Europe Programme (DIGITAL) | Type of action: DIGITAL JU Coordination and Support Actions
- Development and Deployment of Advanced Key Technologies**  
DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH | Call for proposal



Full list of current available calls under DEP [here](#).



# Horizon Europe

**Current calls – open since 27 June  
and deadline on 20 November 2024 :**



**HORIZON EUROPE**

- Approaches and tools for security in software and hardware development and assessment;
- Post-quantum cryptography transition ;
- Mitigating new threats and adapting investigation strategies in the era of Internet of Things ;
- Interoperability for border and maritime surveillance and situational awareness;
- Advanced real-time data analysis used for infrastructure resilience.

Quick search

Cybersecurity

2021 - 2027

Horizon Europe (HORIZON)

Call

Submission status

All filters

Programme: Horizon Europe (HORIZON)

<p><a href="#">Post-quantum cryptography transition</a></p> <p>HORIZON-CL3-2024-CS-01-02   Call for proposal</p> <p>Opening date: 27 June 2024   Next deadline: 20 November 2024   Single-stage</p> <p>Programme: <b>Horizon Europe (HORIZON)</b>   Type of action: <b>HORIZON Research and Innovation Actions</b></p>	<p>Open For Submission</p>
<p><a href="#">Approaches and tools for security in software and hardware development and assessment</a></p> <p>HORIZON-CL3-2024-CS-01-01   Call for proposal</p> <p>Opening date: 27 June 2024   Next deadline: 20 November 2024   Single-stage</p> <p>Programme: <b>Horizon Europe (HORIZON)</b>   Type of action: <b>HORIZON Innovation Actions</b></p>	<p>Open For Submission</p>
<p><a href="#">Mitigating new threats and adapting investigation strategies in the era of Internet of Things</a></p> <p>HORIZON-CL3-2024-FCT-01-01   Call for proposal</p> <p>Opening date: 27 June 2024   Next deadline: 20 November 2024   Single-stage</p> <p>Programme: <b>Horizon Europe (HORIZON)</b>   Type of action: <b>HORIZON Research and Innovation Actions</b></p>	<p>Open For Submission</p>
<p><a href="#">Interoperability for border and maritime surveillance and situational awareness</a></p> <p>HORIZON-CL3-2024-BM-01-02   Call for proposal</p> <p>Opening date: 27 June 2024   Next deadline: 20 November 2024   Single-stage</p> <p>Programme: <b>Horizon Europe (HORIZON)</b>   Type of action: <b>HORIZON Innovation Actions</b></p>	<p>Open For Submission</p>

https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/HORIZON-CL3-2024-CS-01-02?ord...ance&keywords=Cybersecurity&isExactMatch=true&status=31094501,31094502&programmePeriod=2021 - 2027&frameworkProgramme=43108390

Full list of current available calls under HE [here](#).



Soutien aux candidats au financement du DEP

→ bientôt disponible en ligne!

—

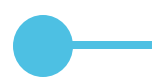
# 05 Points à retenir

# Principaux points à retenir et prochaines étapes

1. Le CCB est le **NCC de la Belgique**
2. Le NCC-BE sert de plaque tournante pour la **coordination et la collaboration entre tous les acteurs belges** en cybersécurité
3. Le NCC-BE est là pour **soutenir les universités et les centres de recherche et d'innovation**







# Quels sont les avantages pour vous?

1

Faites entendre  
votre voix sur la  
scène européenne



*Rejoignez la  
Communauté de  
Compétence en  
Cybersécurité belge !*

2

Soyez au courant  
des possibilités de  
financement de l'UE  
en avant-première



*Participez à nos  
événements de  
networking !*

3

Recevez du soutien



*Inscrivez-vous à notre  
newsletter*

Vous pouvez suivre les mises à jour NCC-BE sur notre site web → [website](#)

- le financement,
- les événements,
- les trucs et astuces sur le financement de l'UE... et plus!

Adresse mail: [ncc@ccb.belgium.be](mailto:ncc@ccb.belgium.be)





*Rejoignez notre groupe LinkedIn pour rester informés de toutes les dernières nouvelles du NCC-BE*

You can follow the NCC-BE  
LinkedIn group via [this link](#) or QR



—

06

# Questions & réponses

## Session interactive





# Avez-vous des questions?

---



# Session interactive

---

# Session interactive à l'écoute

NCC-BE

BELGIUM CYBERSECURITY  
COORDINATION CENTRE



1. Quels sont **vos plus grands défis** en matière de cybersécurité ?
2. Où trouvez-vous **votre financement principal** pour vos projets de cybersécurité ?
3. Envisagez-vous de postuler à un **financement européen** afin de relever les défis de cybersécurité ?

# Session interactive à l'écoute

NCC-BE

BELGIUM CYBERSECURITY  
COORDINATION CENTRE



1. De **quoi auriez-vous besoin** pour postuler à un financement de l'UE
  - ✓ capacité?(rédaction de projet),
  - ✓ expertise?,
  - ✓ approbation de l'université?,
  - ✓ autres ?
2. Où voudriez-vous que **l'Europe investisse** dans la cybersécurité dans un avenir prévisible ?
3. Le financement de l'UE peut nécessiter un **cofinancement**. Quelles sont vos possibilités de co-investissement ?



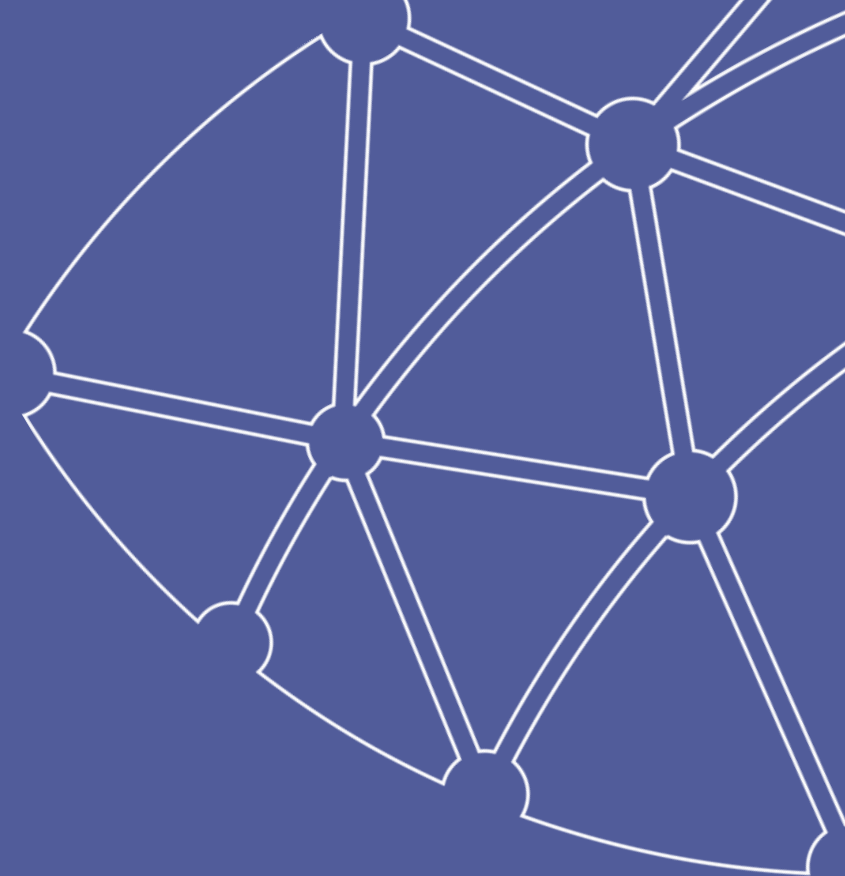
CENTRE FOR  
**CYBERSECURITY**  
BELGIUM



Centre for Cybersecurity Belgium  
*Under the authority of the Prime Minister*

Rue de la Loi / Wetstraat 18 - 1000 Brussels

[www.ccb.belgium.be](http://www.ccb.belgium.be)





# Conclusion



# Plus d'infos sur

[digitalwallonia.be/cyber](https://digitalwallonia.be/cyber)

