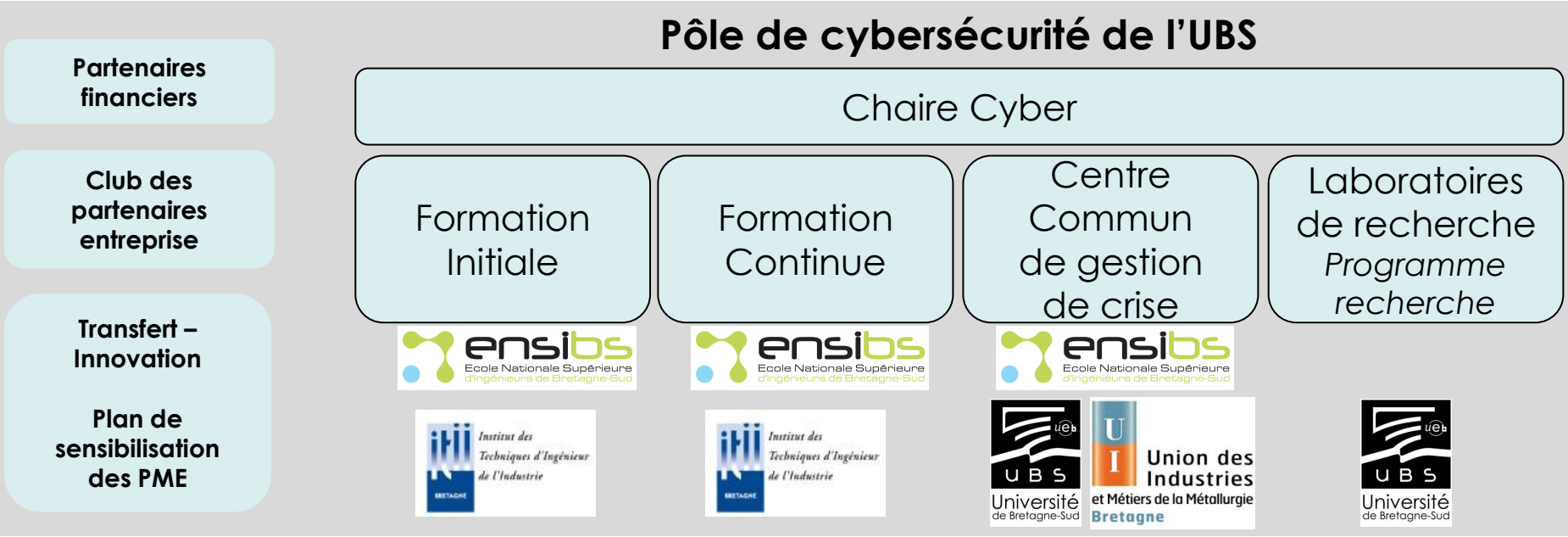
Projet de l'UBS en cybersécurité

22 janvier 2015
Guy GOGNIAT

Pôle de cybersécurité de l'UBS – Chaire cyberdéfense

- **Plusieurs projets se nourrissent au sein d'un même pôle**

1. Des formations d'ingénieurs en cyberdéfense et informatique de confiance
2. Des DU en cybersécurité
3. Une plateforme technologique
   - *Le Centre Commun de gestion de Crise Cybernétique*
4. Une plateforme méthodologique
   - *Programme de recherche (avec 6 axes) (2015-2017)*



Formation d'ingénieurs en cyberdéfense

1

Compétences transverses	Année N 2	Année N 3
	Cyber droit *Cyber éthique* *Facteurs humain* *SHS* *Méthodologie cyber sécurité* *Projets de produits de sécurité*	*Cyber crise*  *Analyse géostratégie internationale* *Doctrine et organisation en cyberdéfense* *Projets complexes de sécurité des systèmes*
Compétences scientifiques	***Maitriser les maillons de la chaine de confiance du numérique*** *du composant matériel aux systèmes d'information et systèmes industriels (ICS/SCADA)* ***Analyser le risque cybernétique***	***Maitriser la sécurité dynamique des infrastructures vitales dans une approche système*** ***Gérer des crises cyberdéfense***

Années

Formation d'ingénieurs en cyberdéfense : Seconde année

Maitriser la chaine de confiance du numérique

- Sécurisation des systèmes d'exploitation et des systèmes embarqués
- Sécurisation des réseaux de communication et des réseaux industriels (SCADA)
- Sécurisation des solutions de base par approche cryptographique et gestion de clefs
- Sécurisation des solutions middleware (annuaires, messageries, bases de données)
- Sécurisation des infrastructures (contrôle d'accès, gestion des identités numériques, cloud, virtualisation, bigdata, …)
- Analyser les vulnérabilités matérielles et logicielles (analyses de sécurité)
- Maitriser la protection numérique des développements et des contenus numériques
- Maitriser les architectures de sécurité
- Concevoir, réaliser et mettre en œuvre un ensemble de solutions de sécurité

Analyser le risque cybernétique

- Analyse géostratégique internationale
- Comprendre l'interconnexion et l'évolutivité à grande échelle des systèmes dans le cyberespace
- Analyser la menace et diagnostiquer le mode opératoire des attaquants
- analyser les attaques sur les infrastructures
- Maitriser les politiques de sécurité
- Maitriser la méthodologie d'analyse de risque et bonnes pratiques
- Maitriser la méthodologie d'évaluation et de certification d'une solution de sécurité
- Maitriser le droit et réglementation en cyber sécurité

Formation d'ingénieurs en cyberdéfense : Troisième année

Construire la sécurité dynamique des infrastructures vitales dans une approche système

- Résoudre des problèmes complexes de niveau système (de nature technologique) par un panel de solutions à la fois méthodologiques, technologiques, organisationnelles, humaines, juridiques et déontologiques
- Concevoir, réaliser et mettre en œuvre un ensemble de solutions de sécurité
- Concevoir, réaliser et mettre en œuvre la protection des systèmes des Opérateurs d'Infrastructures Vitales (OIV)
- Conduire une approche systémique de la sécurité pour sécuriser des systèmes industriels, des systèmes d'information, des systèmes financiers, des systèmes d'armes…

Gérer des crises cybernétiques

- Concevoir, développer et exploiter un centre opérationnel de cybersécurité
- Savoir détecter dynamiquement les attaques
- Savoir réagir en situation de gestion de crise en conformité avec le cadre juridique, les doctrines d'emploi et les règles d'engagement de la cyberdéfense
- Expertiser, auditer et évaluer les résistances des configurations techniques des systèmes
- Savoir adopter un comportement éthique et déontologique en situation de gestion de crise
- Savoir communiquer pendant une crise

Manager des projets complexes de sécurité des systèmes

Formation d'ingénieurs en cyberdéfense

- **Quelques terrains d'apprentissage chez les partenaires :**
  - **Orange,**
  - **Alcatel,**
  - **Thales,**
  - **Airbus,**
  - **SAB,**
  - **Bull,**
  - **Atos,**
  - **Cap gemini,**
  - **SOPRA,**
  - **Schneider,**
  - **Nestlé,**
  - **EFS,**
  - **Clararet,**
  - **Amossys,**
  - **Bertin,**
  - **Areva,**
  - **Nextiraone,**
  - **SII,**
  - **Isatech,**
  - **IMS Network …**

Autres formations cybersécurité

Diplômes universitaires en cyber sécurité pour la formation continue à la demande des entreprises

- 2013 : Ingénierie de solutions en sécurité
- 2013 : Management et Ingénierie de sécurité des systèmes
- 2014 : Management de cyber crise (cadre partenariat IEP)

Transformation de la spécialité informatique de l'ENSIBS (statut étudiant)

- 09 2013 : habilitation CTI en ingénierie des systèmes logiciels de confiance

Centre commun de gestion de crise cybernétique

Salle N 2 :
cellule de planification de la réaction à la crise en temps différé et communication de crise
8 POSTES DE TRAVAIL (24m²)

Défenseurs

Salle N 1 :
cellule d'analyse et de conduire en temps réel de la crise
16 POSTES DE TRAVAIL en U (50M²)

Salle N 3 :
cellule d'animation de la crise (génération d'évènements d'attaque en temps réel, analyse de la situation et analyse après action)
6 POSTES DE TRAVAIL (24m²)

Attaquants - Animateur

Salle N 4:
cellule de préparation et de création des scénarii de crise et de gestion des configurations techniques du centre (+ interopérabilité avec d'autres centres potentiels
2 POSTES DE TRAVAIL (18m²)

Préparateur

Salle N°5 :
cellule de débriefing, de cours, workshop avec visioconférence connectée à l'Internet
25/30 PLACES

Débriefing

Salle N°6 :
cellule « vie » (accueil/ détente/ repos)
15 PLACES (30m²)

Vie

Centre commun de gestion de crise cybernétique

Plan de sensibilisation des PME : 5 offres ciblées pour les PME : Scyforpro

1. **Cyforpro- Sensibilisation des cadres** pour apprendre à identifier vos actifs informationnels vitaux, à comprendre et à mitiger les cybers risques puis mettre en oeuvre un plan ou chartre de sécurité.

2. **Cyforpro – Pour tous**. Que ce soit à la maison, au bureau ou en déplacement, nous vous présenterons - à partir de vos activités quotidiennes telles qu'échanges d'Emails ou de données, utilisation d'internet, des réseaux sociaux, téléchargements visionnage de vidéos, sauvegarde des données - les risques auxquels vous êtes confrontés et les réflexes simples à acquérir pour vous protéger.

3. **Cyforpro – Logiciels libres.** Gérer ses mots de passe, protéger ses échanges de données, stocker ses informations sur le cloud renforcer la sécurité de votre navigateur sont facilités par l'utilisation de logiciels gratuits aussi bien pour vos ordinateurs, tablettes que vos smartphones. Vous apprendrez à installer, configurer et utiliser ces logiciels pour votre environnement de travail. Ex : gestion mots de passe (Keepass :coffre fort de mots de passe)

4. **Cyforpro –Cyber renseignement .** La recherche et l'exploitation de l'information à travers l'analyse des réseaux sociaux et des informations publiées sur Internet permettent de renforcer votre stratégie de cyber défense ou tout simplement d'affiner votre stratégie de développement. Vous apprendrez à détecter les indices, à utiliser différents outils pour collecter, croiser et synthétiser l'information.

5. **Formation et entrainement à la gestion de crise et reprise d'activité sur le C4 de l'UBS**

Programme de recherche en cyberdéfense

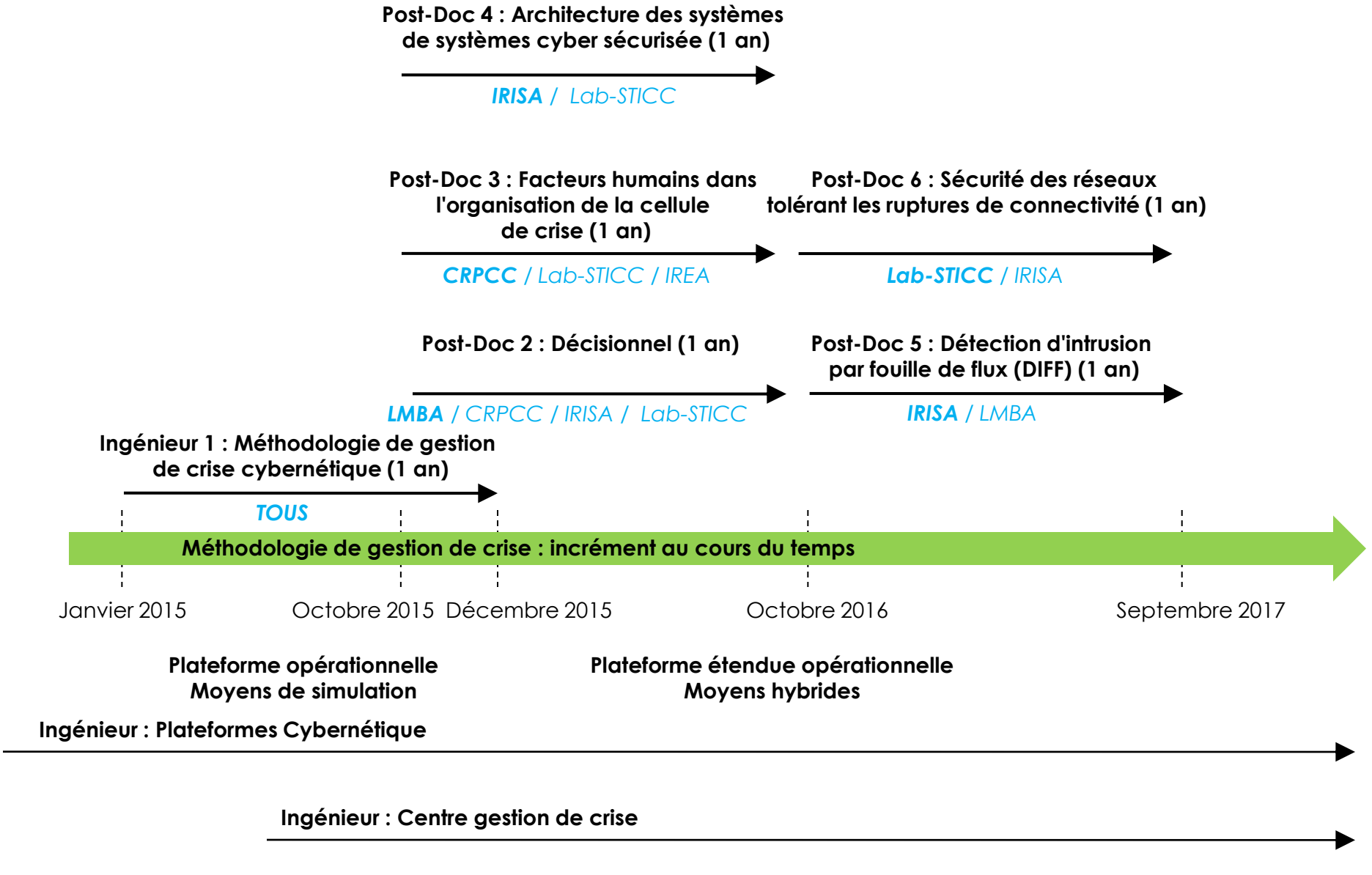
Un programme de recherche et d'innovation stratégique pour l'UBS associé à un financement de 273k€/3 ans

5 laboratoires participent à se programme de recherche

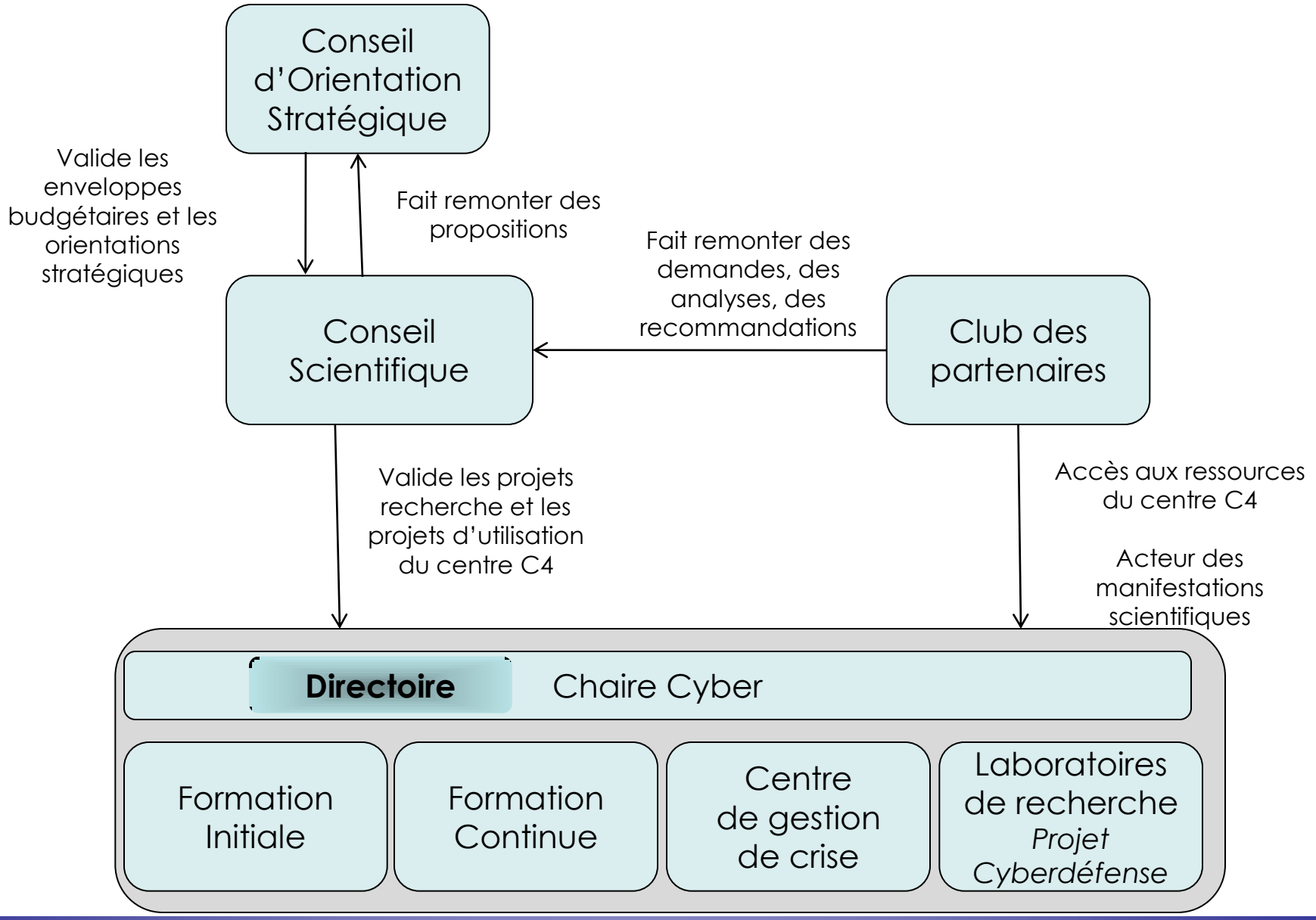
Ce programme s'articule autour du centre commun de gestion de crise cybernétique et se décline en 6 axes de recherche :

- Axe 1 : Méthodologie de gestion de crise cybernétique
- Axe 2 : Décisionnel
- Axe 3 : Facteurs humains dans l'organisation de la cellule de crise
- Axe 4 : Architecture des systèmes de systèmes cybersécurisés
- Axe 5 : Détection d'intrusion par fouille de flux (DIFF)
- Axe 6 : Sécurité des réseaux tolérant les ruptures de connectivité

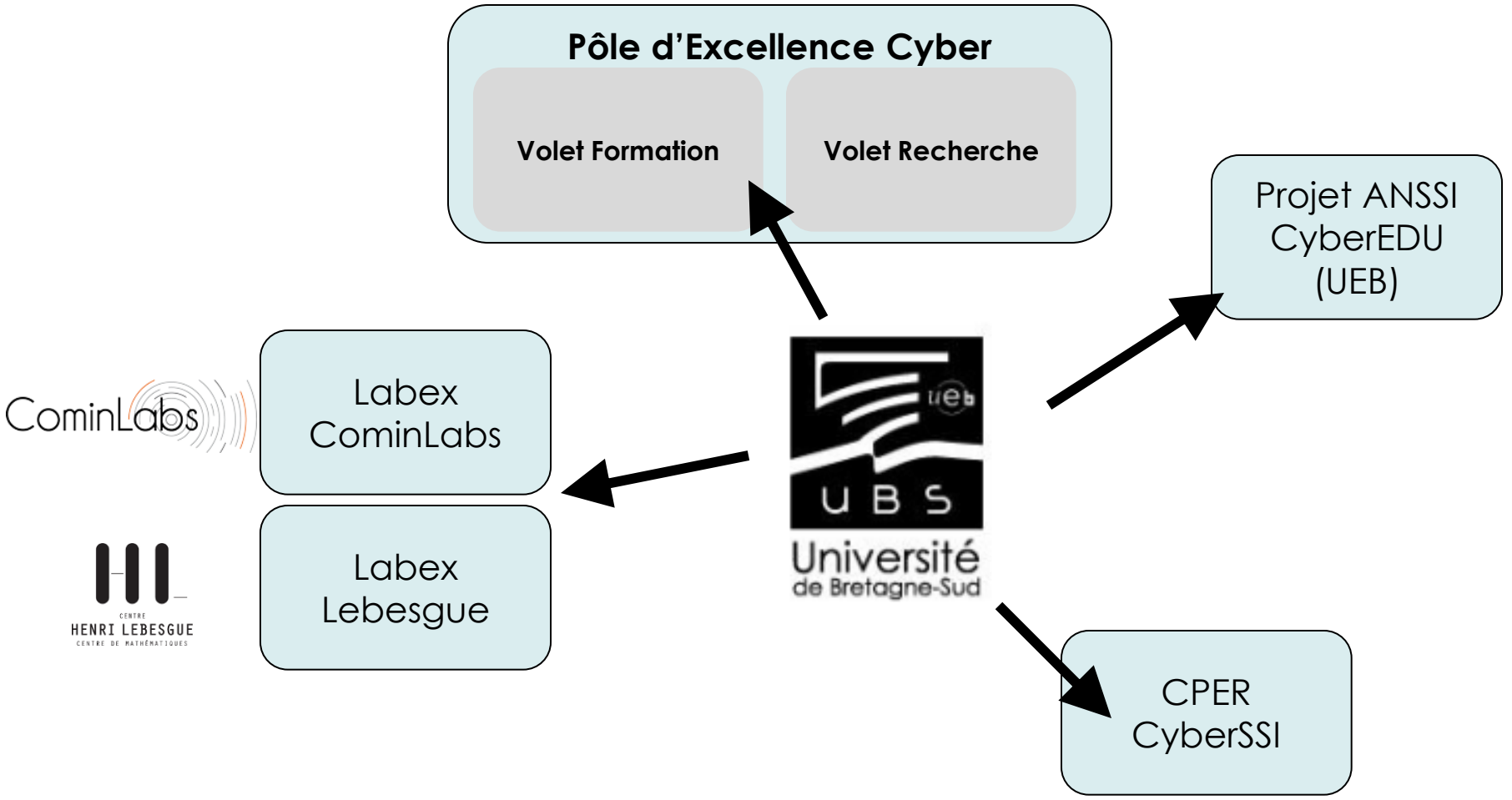
Organisation des travaux du programme de recherche



Gouvernance du projet d'ensemble avec les partenaires



L'UBS dans l'écosystème régional



L'UBS un acteur régional dans les domaines de la formation, de la recherche et de l'innovation

Projet de l'UBS en cybersécurité

22 janvier 2015
Guy GOGNIAT