PÔLE D'EXCELLENCE CYBER

Rapport d'activité 2025

Janvier 2026

Région Bretagne

MINISTÈRE DES ARMÉES ET DES ANCIENS COMBATTANTS
Liberté
Égalité
Fraternité

Préface Chiffres

Structuration de l'écosystème cyber : un engagement stratégique du Pôle

Les programmes phares du Pôle

LES CHIFFRES CLÉS EN 2025

PÔLE D'EXCELLENCE CYBER

132 membres	**31** partenaires	**5** ambassadeurs
3 évènements majeurs à l'étranger	**8 500** participants à l'ECW	**5** nouvelles conventions signées
19 500 Followers sur Linkedin	**376 297** Impressions	**5** Ouvrages
1 site Internet avec 1 partie dédiée aux membres	**26 868** visites	**1 890** téléchargements

LE MOT DU PRÉSIDENT

Chers membres, partenaires et amis du Pôle d'Excellence Cyber,

L'année 2025 a marqué une nouvelle étape décisive pour le Pôle d'Excellence Cyber, confirmant notre position dans l'écosystème de la cybersécurité en France et à l'international. Parmi nos temps forts, l'European Cyber Week 2025 s'est révélée une très belle édition et a encore une fois dépassé nos attentes, s'affirmant comme le rendez-vous incontournable des experts, décideurs et innovateurs du secteur. Cet événement a permis de fédérer une communauté toujours plus large autour des enjeux critiques de la cyber souveraine et de l'IA, tout en renforçant notre visibilité à l'échelle nationale et européenne.

Cette année a également été marquée par une dynamique collective sans précédent : la production de plusieurs ouvrages collectifs issus de nos groupes de travail (GT) a concrétisé notre engagement en faveur d'une IA de confiance dans la défense, de l'innovation, de la prise en compte de la dimension cyber dans les plans communaux de sauvegarde, et une réflexion autour des hackers éthiques. Ces publications, fruit d'une collaboration étroite entre acteurs publics, privés et académiques, illustrent notre capacité à fédérer notre écosystème autour de thématiques d'actualité.

Dans le domaine sociétal, nous avons poursuivis notre engagement avec le lancement d'un programme innovant et ambitieux, les Cyber Singuliers, afin de promouvoir l'insertion des profils neurotaypiques dans le monde de la cyber.

Ces initiatives positionnent le Pôle d'Excellence Cyber comme un acteur de structuration de l'écosystème de la cyber et de l'IA souveraine afin de répondre aux défis technologiques et éthiques posés par un paysage numérique en constante évolution. Ces réalisations s'inscrivent dans une vision ambitieuse : construire un écosystème résilient, innovant et inclusif, capable de relever les défis croissants de la cybersécurité.

En 2026, nous renforcerons nos priorités stratégiques :

- Approfondir nos partenariats avec les acteurs majeurs en Europe et à l'international,
- Développer les talents et compétences pour répondre aux besoins du secteur,
- Amplifier l'impact de nos actions, notamment à travers des projets concrets et des collaborations renforcées.

Ce rapport d'activité témoigne de la richesse de nos initiatives et de l'ampleur de nos réalisations. Ensemble, nous avons fait avancer la cybersécurité en France et au-delà, et c'est grâce à l'engagement de chacun d'entre vous que nous continuerons à bâtir un numérique sûr, résilient et porteur d'innovation.

Je tiens à remercier chaleureusement toutes et tous pour votre contribution essentielle. Continuons à œuvrer ensemble, avec détermination et vision, pour relever les défis de demain et façonner l'avenir de la cybersécurité.

Le vice amiral d'escadre (2S) Arnaud Coustillière
Président du Pôle d'excellence cyber

INTRODUCTION

L'année 2025 a confirmé la mobilisation sans précédent et la structuration renforcée du Pôle d'Excellence Cyber (PEC). Ce rapport d'activité reflète le rôle central joué par nos membres, en particulier les membres fondateurs – le ministère des Armées et la région Bretagne – dont l'engagement a été déterminant pour dynamiser notre association. Leur soutien aux projets ambitieux et leur participation active aux groupes de travail ont permis de produire des publications de inspirantes, consolidant ainsi le positionnement du PEC comme un acteur incontournable de l'écosystème cyber national.

Nous saluons également l'action décisive de nos instances dirigeantes – conseil d'administration, Advisory Board et présidence – dont la vision stratégique a permis de lancer de nouvelles initiatives. L'équipe opérationnelle, par son expertise, son engagement et sa réactivité, a assuré la mise en œuvre de ces projets et accompagné nos membres dans leurs travaux, renforçant ainsi notre capacité collective à innover et à agir.

L'European Cyber Week 2025 a une nouvelle fois marqué les esprits, s'imposant comme l'un des grands événement de la cybersécurité sur la carte de France. Ce succès a fédéré les acteurs nationaux, européens et internationaux autour des enjeux critiques du secteur, tout en mettant en lumière l'écosystème breton et notre rôle de catalyseur dans la structuration d'un environnement dynamique et innovant.

Autre réalisation forte de l'année, notre réorganisation afin de relever le défi du programme EDIH Bretagne, co-piloté par Images et Réseaux et Bretagne Cyber Alliance, au profit de la maturité cyber des entreprises et collectivités en Bretagne.

Malgré ces avancées, des enjeux majeurs restent à relever. La sécurisation financière demeure une priorité pour garantir la pérennité de notre modèle. Par ailleurs, l'intégration de l'intelligence artificielle (IA) dans nos actions et réflexions représente un défi stratégique, alors que cette technologie redéfinit les contours de la cybersécurité. Enfin, notre capacité à anticiper les évolutions technologiques, à attirer de nouveaux membres et à consolider notre rôle d'association de la cybersécurité souveraine sera au cœur de nos priorités pour 2026.

J'adresse mes remerciements les plus sincères à l'ensemble des membres, partenaires et collaborateurs du Pôle pour leur engagement et leur contribution à ces succès. Nous continuerons à renforcer notre écosystème et à être un moteur de projets innovants dans le domaine de la cybersécurité.

Loïc ROIGNAN
Délégué général du Pôle d'excellence cyber

PÔLE D'EXCELLENCE CYBER

GOUVERNANCE
LE CONSEIL D'ADMINISTRATION/ ÉLUS

STÉPHANIE LEDOUX

ALCYCONIE

TRÉSORIÈRE

PIERRE JEANNE

THALES

VP EUROPE

Axe soutenu par

JEAN-LUC GIBERNON

SOPRA STERIA

VP DÉVELOPPEMENT INDUSTRIEL

Axe soutenu par

ANTOINE HAUTIN

ALMOND

VP CERTIFICATION

Axe soutenu par

NOBERT CHASSANG

AIRBUS

SECRÉTAIRE

DAVID MENIER

UBS

VP FORMATION

Axe soutenu par

PATRICK GROS

INRIA

VP RECHERCHE

Axe soutenu par

DAVID ALIS

UNIVERSITÉ DE RENNES

VP RECHERCHE

Axe soutenu par

HÉLÈNE CHINAL

CAPGEMINI

VP ENJEUX SOCIÉTAUX & AXES TRANSVERSES

Axe soutenu par

PÔLE D'EXCELLENCE CYBER

GOUVERNANCE
LE BUREAU

VAE (2S)
ARNAUD COUSTILLIÈRE

PÔLE D'EXCELLENCE CYBER

PRÉSIDENT
(NOMMÉ)

LOÏC ROIGNAN

PÔLE D'EXCELLENCE CYBER

DÉLÉGUÉ GÉNÉRAL

STÉPHANIE LEDOUX

ALCYCONIE

TRÉSORIÈRE

JEAN-LUC GIBERNON

SOPRA STERIA

TRÉSORIER ADJOINT

NOBERT CHASSANG

AIRBUS

SECRÉTAIRE

PIERRE JEANNE

THALES

SECRÉTAIRE ADJOINT

Vie d'association

Nouveaux représentants

Un renouvellement partiel des administrateurs et membres du bureau s'est tenu cette année du fait du changement d'activité professionnelle ou du départ en retraite de certains de nos administrateurs. Ainsi, Norbert CHASSANG a succédé pour la société Airbus à Serge MAURICE au poste d'administrateur et de trésorier. Pour sa part, David MENIER a succédé à Virginie DUPONT en qualité de vice-président formation au sein du conseil d'administration.

En outre, le pôle a le plaisir d'accueillir Matthieu BLONDEAU qui succède à Annie AUDIC en qualité d'Ambassadeur Europe du PEC.

Enfin, afin de l'appuyer dans ses missions, le président s'est adjoint des chargés de mission :

- Jonathan FUSSNER (Systancia) : chargé de mission "Accompagnement start-ups, PME, ETI"
- Antoine HAUTIN (Almond) : Vice-président du PEC et chargé de mission "Affaires publiques"
- Estelle Franz : bénévole du PEC, chargée de mission développement des relations avec l'Allemagne

Les nouveaux membres du Pôle

18 nouveaux membres ont rejoint le pôle cette année.
Il s'agit majoritairement de start-ups, PME et ETI mais également d'acteurs de la formation qui viennent tous enrichir l'écosystème à travers leurs contributions essentielles sur les groupes de travail et divers projets et programmes en cours.

Les nouveaux partenariats

Groupement Régional e-Santé Bretagne :
Une convention de partenariat a été signée à l'occasion de l'European Cyber Week 2025 afin de renforcer la cybersécurité du secteur de la santé en Bretagne. Ce partenariat vise à sensibiliser les professionnels, accompagner les structures dans leurs démarches de cybersécurité, encourager l'innovation et identifier des projets d'intérêt commun, dans un contexte de menaces croissantes pesant sur les systèmes d'information de santé.

Union Nationale de l'Aide, des Soins et des Services aux Domiciles
Une convention de partenariat a été signée à l'occasion de l'European Cyber Week 2025 afin d'accompagner les structures de l'aide, des soins et des services à domicile face aux enjeux de cybersécurité. Ce partenariat vise notamment à renforcer la maturité en sécurité numérique du secteur, sensibiliser les professionnels aux cybermenaces, favoriser l'acculturation mutuelle entre cybersécurité et médico-social, et co-construire des actions communes au bénéfice des adhérents des deux organisations.

ECW 2025, signature de deux protocoles d'entente avec des organismes de recherche canadiens :

- **Institut Multidisciplinaire en Cybersécurité et Cyberrésilience (IMC2)**

Cette entente cadre vise à la création de l'IMC2, qui fédère des institutions prestigieuses telles que l'Université de Montréal, Polytechnique Montréal, l'UQAM, l'Université de Laval et l'UQO.

- **Université de Sherbrooke**

Une entente cadre a également été signée le Pôle d'Expertise en cybersécurité Intact de l'université de Sherbrooke.

Ces initiatives s'inscrivent dans une volonté de renforcer les échanges académiques et de favoriser la mobilité des étudiants et des chercheurs entre les deux régions.

Cyber'Occ
Un partenariat stratégique a été officialisé en 2025 à l'occasion du Forum INCYBER afin de croiser les écosystèmes breton et occitan de la cybersécurité. Cette collaboration vise à favoriser le partage d'expertises, le développement d'actions communes et le renforcement de l'innovation, de la résilience et de la compétitivité des territoires, en s'appuyant sur les dynamiques respectives des deux réseaux.

Vie d’association

Les nouveaux membres de l’équipe opérationnelle

Thomas GUILLAUDEUX est alternant en première année de Master Cybersécurité. Il est venu renforcer l’équipe Sec.Ops dans le cadre du programme européen EDIH Bretagne.
Intégré aux activités de la Red Team, Thomas intervient principalement sur les aspects techniques de la cybersécurité. Il mobilise ses compétences pour contribuer à l’évaluation des systèmes d’information, à l’identification des vulnérabilités et à la mise en œuvre de recommandations visant à améliorer le niveau de protection et la maturité cybersécurité des organisations accompagnées.

Chloé CHEMIN a rejoint le Pôle d’Excellence Cyber en septembre au sein de l’équipe Sec.Ops en tant que Cheffe de projet cybersécurité, afin de renforcer la dimension opérationnelle de ce programme européen.
Elle intervient principalement sur la réalisation de diagnostics de cybersécurité auprès des entreprises, associations et collectivités bretonnes. Grâce à une approche Purple Team, Chloé assure un rôle de passerelle entre la prévention des risques cyber, l’analyse des menaces et la mise en œuvre de recommandations techniques adaptées aux contextes des structures accompagnées.
Son objectif est de participer, à son niveau, au renforcement de la résilience cyber des petites et moyennes structures bretonnes, en privilégiant une écoute attentive des besoins, une pédagogie adaptée et la proposition de solutions concrètes, pragmatiques et proportionnées à leurs enjeux.

Nathan ROLLAND, est alternant au sein du service communication du Pôle d’excellence cyber. Il suit actuellement un Bachelor 3 à l’ISCOM Rennes.
Il a rejoint l’équipe à l’occasion de l’European Cyber Week 2024,
dans le cadre d’un stage de trois mois. À l’issue de cette première expérience, il a choisi de poursuivre son engagement en alternance au sein du Pôle.
Ses compétences lui permettent de prendre en charge, entre autres, la couverture photographique des évènements du Pôle, le traitement et l’archivage des fichiers, la communication digitale, participer à la création de designs etc...

Diarra BOHM-MBAYE, alternante en deuxième année de Master de géopolitique – parcours Territoires et enjeux de pouvoir, spécialité Cyberstratégie et terrains numériques à l'Institut Français de Géopolitique, apporte depuis septembre un appui direct au Président sur certains dossiers. Elle contribue notamment aux Groupes de Travail internationaux, parmi lesquels le GT Canada, AFMO, ASEAN ainsi que Ukraine/Estonie, et co-pilote également les travaux du GT Autonomie stratégique. Par ailleurs, elle prend en charge une partie des missions liées au processus d'adhésion des nouveaux membres.

Flavie MIRVENARD, est alternante en deuxième année de Master géopolitique, parcours territoires et enjeux de pouvoir, spécialité cyberstratégie et terrain numérique à l'Institut Français de Géopolitique, est, depuis octobre, en appui du Président sur de nombreux sujets. Parmi eux, le co-pilotage du GT enjeux sociétaux, et du GT Autonomie Stratégique. A cela s'ajoute l'appui au programme des Cadettes de la cyber, celui du programme CyberSinguliers et au au GT Cyberdéfense du domaine spatial. L'étude sur des sujets internationaux actuels est aussi une des missions réalisées.

Structuration de l'écosystème cyber : un engagement stratégique du Pôle

Axe formation / Engagement du PEC dans des projets AMI-CMA

Deux programmes structurent les actions menées dans le domaine de la formation : deux AMI CMA (Appel à Manifestation d'Intérêt, Compétences et Métiers d'Avenir) remportés par des consortiums dont le Pôle est partenaire : le projet CyberSkills4All et le projet IFALP (Institut Français des Achats et de la Logistique Publics).

À travers son Consortium (Université de Rennes, UBS, ENSTA, Rennes School of Business, GIP-FAR, GIP-FUN, ENIB, Campus des métiers et des qualifications d'excellence Numérique Photonique de Bretagne, Groupe Orange, PEC), création de 12 nouveaux diplômes pour spécialistes en cybersécurité (du Baccalauréat au Master), 15 sujets de thèses et formations doctorales et plus de 150 formations de non spécialistes, sous la forme de « mineures » dans tous les domaines (droit, santé, sciences, lettres) répondant aux besoins identifiés notamment via l'observatoire Emploi-Formation Cela représentera plus de 3600 spécialistes formés, dont un millier dans le cadre de la formation continue, 15 000 apprenants formés au juste niveau de leur domaine de compétence, 80 000 élèves seront sensibilisés.

Pour cet AMI, le PEC est chargé de piloter les travaux du Comité d'Orientation Stratégique. Ces travaux sont animés par Solène Chevreau, en collaboration étroite avec Jean Peeters (le nouveau Directeur scientifique du projet). Un certain nombre de travaux alimentent la réflexion de ce comité d'orientation stratégique dont voici quelques avancées :

- Les travaux de l'observatoire Emploi/Formation piloté par le GREF Bretagne a produit un document recensant toutes les formations cyber en Bretagne. Ce document permet de mettre en lumière le niveau d'expertise de ces formations qui prend en compte le nombre d'heures d'enseignements en cyber. Après plusieurs réunions de travail, le groupe de travail évolue vers des GT "bénéficiaires" qui prendra en compte les besoins des utilisateurs pour retravailler le fichier de manière idoine (en fonction des besoins des étudiants, des professionnels de l'orientation)
- De plus, le projet Cyberskills4all a décidé d'arrêter la collaboration avec le GREF Bretagne et de confier la suite des travaux au Pôle d'Excellence Cyber. En effet, le PEC a déjà produit un certain nombre d'enquêtes qualitatives et quantitatives, et se révèle être l'acteur le mieux positionné pour effectuer ces travaux d'études prospectives sur les compétences en tension en cyber et repérer celles qui vont devenir essentielles d'ici 2 à 4 ans. Cet observatoire sera mis en place au premier trimestre 2026. Le premier livrable portera sur un recensement des enquêtes existantes sur le thème de l'emploi et des compétences en cyber en France.

Dans la continuité de 2024, les principales réalisations de 2025 concernent la sensibilisation des collégiens et lycéens, la création d'une nouvelle formation à l'ENSSAT dont l'ouverture est prévue en 2026, et la passation d'un appel d'offre de formation par l'Université de Rennes pour la création de 6 micro-certifications en sous-traitance. Parmi les lauréats de cet appel d'offre, 3 des 5 lauréats sont des membres du Pôle d'Excellence Cyber. Ainsi une dizaine de micro-certifications devraient être finalisées au début de l'année 2026 et commercialisées par France Université Numérique (FUN).

IFALP

Présentation du projet : à travers son Consortium (qui regroupe notamment le ministère de l'Intérieur, ministère des Armées, ministère de la Justice, ministère de l'Enseignement Supérieur et de la Recherche, MTES, UGAP, CNRS, des collectivités locales, des agences de l'Etat, CCI, PEC) l'IFALP a pour objectif de créer un institut à vocation nationale dédié à l'achat public et à la chaîne d'approvisionnement (de bout en bout), afin de répondre au besoin de la sphère publique, en termes de formation, de recherche (sa valorisation et promotion), de documentation, d'intelligence économique, d'influence de la doctrine, d'animation d'un think-tank, d'échanges dédiés au domaine, surtout autour de 2 axes : souveraineté / sécurité (dont cyber) et décarbonation / logistique.

Dans le cadre d'IFALP, le rôle du Pôle est d'aider le GIP ESPRIT à développer une nouvelle formation localisée à Redon : le Bachelor ARSIS (« Administrateur Réseaux, Systèmes et Infrastructures Sécurisées »), une formation en alternance au carrefour de l'informatique, des réseaux et de la cybersécurité, conçue pour répondre aux besoins croissants de sécurité et de performance des systèmes numériques dans les environnements industriels et logistiques. Cette formation qui délivre un titre RNCP de niveau Bac+3 représente le niveau de formation manquant sur le territoire de Redon pour permettre aux étudiants de continuer de monter en compétences en cybersécurité et de pouvoir accéder aux masters existants déjà au GIP ESPRIT. L'ouverture de la première promotion est prévue pour septembre 2026.

Le Pôle contribue ainsi à la mise en contact du GIP CEI avec les acteurs professionnels du milieu industriel qui expriment un besoin de compétences dans ce secteur. Une étude approfondie a permis d'identifier les lycées et entreprises potentiellement intéressés par cette nouvelle formation. Des présentations du Bachelor ARSIS sont programmées avec des lycées partenaires auprès des étudiants de BTS SIO et CIEL comme poursuite d'étude potentielle.

Axe formation / Animation des groupes de travail dédiés à la formation

Plusieurs groupes de travail du Pôle sont actifs dans le cadre de cet axe :

GT GPEC (Gestion Prévisionnelle des Emplois et des Compétences) : débuté en mai 2024, ce GT vise à réfléchir et à anticiper les besoins en emplois et compétences en cyber. L'objectif est de promouvoir l'utilisation d'un référentiel commun aux employeurs, salariés et acteurs de la formation (enseignants, étudiants, RH), et ce, quel que soit leur secteur d'activité (public ou privé, start-up ou grande entreprise). Un premier croisement entre les référentiels ANSSI et NICE a été effectué sur deux métiers différents. Ce travail extrêmement chronophage doit aujourd'hui se réorienter pour permettre une production plus rapide des référentiels. Un niveau de granularité fin de description des compétences est essentiel au projet Cyberskills4all afin identifier les micro compétences à proposer, mais également pour les professionnels du secteur et les organismes de formation pour exprimer et ajuster les programmes de formation au regard des profils recherchés.

GT Formateurs : Ce GT vise à disposer de professionnels formés en cohérence avec les besoins en compétences de la filière, mais également à créer une communauté de formateurs selon leur domaine de compétence. En 2025, les travaux ont permis d'identifier les difficultés actuelles des apprenants pour trouver des terrains d'alternance ou de stage ; les difficultés qu'ont les écoles et universités à trouver des formateurs en cybersécurité ; et partager des pratiques d'innovation pédagogiques entre enseignants. Tous ces travaux, en collaboration avec la région Bretagne, vont se poursuivre en 2026.

Axe formation / Actions dédiées lors de l'European Cyber Week (ECW)

Journée formation ECW & CTF lycéens

La journée formation de l'ECW a proposé quatre tables rondes :

- Se reconvertir en cybersécurité
- Travailler en cyber au service de nos institutions
- Les métiers de la cybersécurité
- Les formations existantes pur accéder aux métiers de la cyber

Ces tables rondes ont mis en avant l'inclusion, la diversité des métiers et des parcours tant au service des institutions publiques que des entreprises privées. Comme l'an dernier, ces tables rondes ont été préparées et animées par des Cadettes de la cyber, permettant à ces étudiantes de montrer l'étendue de leurs compétences, et de travailler en transversalité entre programmes du Pôle d'Excellence Cyber. De plus, leur participation contribue à faire naitre des vocations auprès des jeunes filles en incarnant un "role modèle".

Parallèlement, des ateliers pratiques ont été proposés :

- Test de jeu numérique développé par les Cadettes de la cyber auprès d'une classe de 2nde qui a permis aux lycéens de découvrir et de s'initier à la cybersécurité de manière ludique.
- Escape game Great Anonymous animé par le Greta auprès des lycéens mais également des publics en reconversion. Ce jeu immersif permet de découvrir les métiers du numérique et plus particulièrement ceux de la cybersécurité.

La finale du challenge lycéens a réuni 30 jeunes de toute la France. Cet événement était organisé par NoBrackets CTF, une association d'étudiants en cybersécurité. Les qualifications ont permis à 230 lycéens de s'essayer à la cybersécurité de manière ludique et pédagogique.
La remise des prix du challenge lycéen s'est déroulée en présence de la Rectrice de l'Académie de Rennes Madame Hélène INSEL, ainsi que du Général AUGUSTIN, commandant de l'École des Transmissions, du Numérique et du Cyber (ETNC).
Cette journée a également été l'occasion de remettre les diplômes des deux premières promotions de "Technicien veilleur en cybersécurité".

CTF ingénieurs de l'ECW : une dimension européenne affirmée

En 2025, le CTF ingénieurs, événement historique de l'ECW, s'est ouvert à l'Europe, avec la participation de deux équipes européennes en finale.
Le projet global a été porté par France Cyber Maritime, avec une phase de qualification coordonnée par Astek et une finale aux Jacobins soutenue par Airbus.

- 1111 inscrits en provenance de plusieurs pays européens
- + de 30 challenges organisés sur 10 jours en 24h/24 pour la partie qualification
- 15 équipes de 4 personnes présentes en salle pour la partie finale
- 3 écoles bretonnes dans le trio gagnant : ESNA, ENSIBS et Université de Rennes

Axe Recherche

1. Renforcement des coopérations bilatérales avec le Québec

Un événement structurant à l'ECW

L'année a été marquée par un événement d'envergure à l'ECW, couronnant quatre années d'efforts visant à renforcer les liens entre la France et le Québec en matière de cybersécurité. Deux ententes-cadres majeures ont été signées, regroupant l'ensemble des acteurs académiques québécois dans ce domaine. La première concerne le Pôle d'Expertise en cybersécurité Intact de Sherbrooke, tandis que la seconde porte sur la création d'un Institut multidisciplinaire en cybersécurité et cyberrésilience (IMC2), qui fédère des institutions prestigieuses telles que l'Université de Montréal, Polytechnique Montréal, l'UQAM, l'Université de Laval et l'UQO.

Par ailleurs, deux avenants à ces ententes-cadres sont en cours de finalisation. Ils visent à établir des parcours de co-diplomation entre l'Université de Rennes et l'Université de Sherbrooke, ainsi qu'entre l'Université de Brest et l'UQO. Ces initiatives s'inscrivent dans une volonté de renforcer les échanges académiques et de favoriser la mobilité des étudiants et des chercheurs entre les deux régions.
Un événement mixte, associant recherche et industrie, a également été organisé sur une journée complète. Trois tables rondes ont permis de réunir des représentants académiques, membres des institutions signataires, et des acteurs industriels, notamment issus d'INSECM et du PEC. Ces échanges ont mis en lumière les enjeux communs et les opportunités de collaboration entre les milieux universitaire et professionnel.

Vers la création d'un dispositif de thèses CIFRE franco-canadiennes

Un projet pilote est en cours pour établir un dispositif de thèses CIFRE franco-canadiennes, financé à parts égales par la France, via l'ANRT, et le Canada, via MITACS. Ce dispositif innovant vise à soutenir des projets de recherche collaboratifs entre les deux pays. Une condition essentielle est que le partenaire industriel impliqué possède des sites à la fois en France et au Canada. Actuellement, des recherches sont menées pour identifier deux partenaires industriels répondant à ce critère, afin de lancer ce projet pilote ambitieux.

Cette dynamique d'échange a été largement appuyée et accompagnée par le Délégué Général du Québec à Paris avec qui les représentants du Pôle. Ainsi, lors d'une rencontre avec le Délégué général, la création d'un centre franco-québécois de recherche en cybersécurité, inspiré du modèle de l'IFQM a été évoqué. Ce centre aurait pour vocation de renforcer les synergies entre les chercheurs des deux pays et de stimuler l'innovation dans ce domaine stratégique.

Participation au Forum industriel de Gatineau

Le PEC a participé activement au Forum industriel de Gatineau (Canada), organisé en marge de la conférence scientifique CRISiS, co-organisée par le PEC, l'UQO et l'Université d'Ottawa. Lors de ce forum, une attention particulière a été portée à la thématique de la souveraineté et des chaînes d'approvisionnement en cybersécurité.

2. Poursuite des échanges avec Eurobits

L'objectif principal de cette année a été de maintenir la dynamique engagée avec le cluster Eurobits, en préparation d'un événement plus structurant prévu en 2026. À cet effet, une délégation de chercheurs de l'écosystème du PEC s'est rendue à Bochum en mai 2025 pour renforcer les liens avec ce partenaire. Avec Eurobits, une journée de recherche a été organisée à l'ECW, dans le cadre de l'European Day Recherche. Des représentants d'Eurobits ont participé activement à cette journée, notamment par leur participation à des tables rondes.
Les premiers échanges ont également permis d'envisager des actions communes pour 2026, notamment la possibilité de monter des projets européens conjoints. Ces initiatives visent à renforcer la collaboration entre les acteurs français et européens dans le domaine de la cybersécurité.

3. Lancement d'un groupe de travail sur la cyber sécurité du domaine spatial

Une volonté forte s'est exprimée cette année pour définir un groupe de travail Recherche et Innovation autour de la thématique de la cyber sécurité appliquée au domaine spatial. Ce groupe a pour ambition de fédérer la communauté scientifique autour de cette problématique émergente et stratégique.
Le portage de ce groupe de travail est assuré conjointement par le PEC et IRISPACE, afin d'éviter une multiplication des initiatives à l'échelle régionale et d'offrir une meilleure visibilité aux acteurs locaux. Les actions principales envisagées incluent l'identification des synergies entre les différents acteurs, qu'ils soient académiques ou industriels, ainsi que le montage de projets collaboratifs.
Un événement préparatoire a été organisé sous la forme d'une matinée dédiée à cette thématique, dans le cadre de l'European Day à l'ECW. Deux tables rondes ont structuré les échanges : la première portait sur les technologies quantiques pour des communications sécurisées, tandis que la seconde abordait la sécurité de la chaîne d'approvisionnement.

Axe Développement industriel

Sous l'impulsion de Jean-Luc Gibernon (Sopra Steria), vice-président en charge du Développement industriel, trois priorités ont structuré les actions de l'axe Développement Industriel pour l'année 2025 :

- L'animation des groupes de travail (GT) liés au développement industriel,
- La participation à des projets stratégiques dans certaines verticales métiers,
- L'accueil et l'intégration des nouveaux adhérents au sein du PEC.

Animation du collectif du PEC dans le domaine industriel

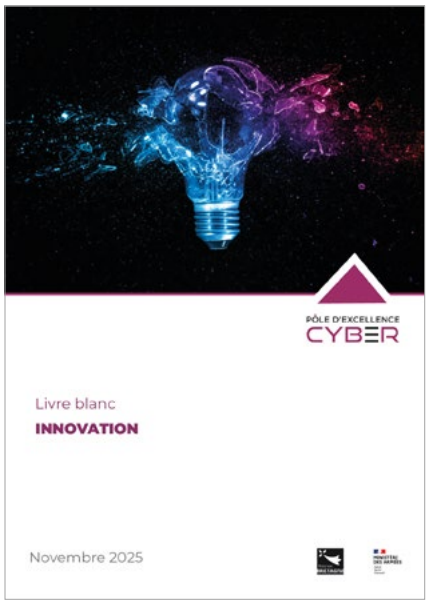
L'animation du collectif s'est articulée autour du « Forum développement industriel » mensuel, piloté par Jean-Luc Gibernon.

Ce rendez-vous régulier offre un espace dynamique pour présenter des entreprises, des services, des technologies ou des produits, et encourage les synergies entre membres pour initier de nouveaux groupes de travail. Ce Forum, véritable point de ralliement, joue un rôle clé dans la vie du PEC en intégrant activement les nouveaux adhérents aux travaux du Pôle.

Parmi les initiatives phares, un travail collectif sur l'Innovation, co-piloté par Jean-Luc Gibernon, Nadine Priam (DGA MI) et Benoit Wintrebert (INRIA) a conduit à la réalisation puis la publication (en novembre 2025 à l'occasion de l'ECW) d'un Livre Blanc sur l'Innovation. Ce travail collaboratif a fait intervenir plus de 20 personnes impliquées dans les travaux du PEC. Largement salué, il fera l'objet de différentes actions de communication et de suites, destinées à favoriser la création de projets innovants collaboratifs entre membres du Pôle.

Différents GT ont notablement progressé, entre autres le GT « Cryptographie post-quantique », animé par Jean-Picco (Thales) et Samih Souissi (ANSSI).

D'autres GT ont été créés ou initiés en 2025, dont en particulier le Comité « Souveraineté numérique » piloté par le président, ou encore le GT « Cyber & Spatial » co-piloté par Antoine Hautin (Almond) et David Espes (UBO).



Axe Développement industriel

Appui aux collectivités

Un travail collectif, co-piloté par Paul-André Pincemin (Rennes métropole) et Jean Godot (ALL4TEC), a permis la réalisation d'un document intitulé « Intégration du risque cyber au plan communal de sauvegarde des petites communes » qui a été diffusé à destination des collectivités territoriales.

Ce document offre des repères opérationnels, des bonnes pratiques et des outils concrets pour renforcer la résilience des territoires face aux cyberattaques. Destiné essentiellement aux petites communes typiquement de moins de 3500 habitants, il a vocation à les aider à inclure ce risque dans leur Plan Communal de Sauvegarde (PCS) afin de gérer efficacement une crise cyber au regard des ressources dont elles disposent.

D'autres initiatives, dont en particulier le GT « Hacker éthique », ainsi que les groupes de travail « Cyber & Santé », ont poursuivi leurs activités tout au long de l'année.

Participation à des projets stratégiques

En 2025, le PEC s'est impliqué dans plusieurs projets d'envergure, dont :

- Le projet EDIH, développé autour de trois verticales métiers : Santé, BITD, et Maritime, en partenariat avec France Cyber Maritime. L'année 2025 est l'année du renouvellement du projet, dans lequel le Pôle continuera de s'investir activement, avec le démarrage de l'EDIH V2.

- Bretagne Cyber Alliance, dans le cadre duquel le PEC a participé aux réunions et événements clés.

Perspectives pour l'année 2026

L'année 2026 s'annonce prometteuse avec le lancement ou la poursuite de plusieurs groupes de travail stratégiques. Parmi ces initiatives :

- Un GT Cyber & Espace, dont les travaux s'orienteront en réponse aux enjeux croissants liés à la sécurisation des infrastructures spatiales et à la protection des données dans ce secteur.

- Un GT Innovation, destiné à explorer les technologies émergentes et à encourager l'expérimentation pour anticiper les défis industriels et technologiques à venir. Ce GT est une suite donnée au livre blanc du PEC qui a été rendu public en 11/2025.

- Dans le cadre du renforcement de la collaboration avec Eurobits, des actions internationales seront lancées autour, en particulier, des thèmes des montages de projets collaboratifs et européens.

Ces nouveaux GT s'inscrivent dans une dynamique de renforcement des efforts de développement industriel et de recherche, tout en consolidant les collaborations au sein du Pôle et avec ses partenaires internationaux.

Axe Enjeux sociétaux

Inclusion et diversité - impacts de l'IA : des actions au cœur de la stratégie du Pôle d'excellence cyber

Le Pôle d'excellence cyber porte des programmes sur ces thèmes depuis plusieurs années :

- attirer plus de femmes dans les métiers cyber avec le programme des Cadettes de la Cyber et la prise de parole de femmes leaders et inspirantes lors de chaque ECW,
- intégrer dans les métiers cyber des talents neuroatypiques dont les différences sont des atouts si on sait les prendre en compte. Sur ce dernier sujet, un programme spécifique appelé Cyber Singuliers a été lancé cette année pour rendre très concrètes les actions conduites les années précédentes,
- concilier IA et éthique dans la défense et la sécurité avec un groupe de travail lancé en 2024 qui a produit un livre blanc sur l'IA de confiance dans la défense en 2025.

Le programme des Cadettes de la cyber

Ce programme a été proposé par Charlotte Wojcik (Capgemini) et elle le pilote avec une équipe constituée de membres du PEC et de cadettes de différentes promotions depuis sa création.
La 5ème promotion a été lancée pendant l'ECW avec comme parrain le directeur du Campus Cyber, Joffrey Célestin Urbain. Les cadettes des différentes promotions ont activement participé aux ateliers et panels de l'ECW 2025.
L'ouvrage des cadettes "Cybersécurité : un défi citoyen et stratégique" a été aussi dévoilé lors de l'ECW 2025. Cet ouvrage est le symbole des projets que développent les cadettes de la Cyber en contrepartie de l'accompagnement que leur est offert. D'autres projets ont vu le jour comme la BD des cadettes, le jeu numérique (CyberChall), la Fresque du cyber citoyen, le podcast "la Matrice a buggée", ou encore les news bimensuelles.



Le programme Cyber Singuliers

Un guide pour l'inclusion a été présenté lors de l'ECW 2023 : il propose des recommandations pratiques et des témoignages inspirants pour accompagner ces profils, de la formation à l'emploi. En 2024, la diffusion élargie de ce guide et des témoignages inspirants ont renforcé la sensibilisation des acteurs du secteur. Le programme Cyber Singuliers, piloté par Hélène Chinal (Capgemini), Vice-présidente du PEC, a été lancé officiellement pendant l'ECW 2025 et a pour objectif de mettre en pratique ce guide.

Le 18 novembre 2025 a été la journée pour la mise en valeur des profils neuroatypiques. Entre le programme des Cyber Singuliers et la mise en avant de ses profils dans les entreprises, la thématique a su trouver son public. Tables rondes et expériences ont permis d'informer les employeurs sur les approches inclusives tout en donnant la parole à des talents neuroatypiques, qui ont partagé leurs expériences et proposé des pistes pour leur meilleure intégration professionnelle.

Axe Enjeux sociétaux

Le programme Cyber Singuliers a pour objectif d'accompagner des étudiants dans leurs dernières années d'études vers l'insertion professionnelle. Il repose sur 4 piliers :

- Les écoles qui proposent des étudiants volontaires pour être accompagnés
- Les employeurs qui proposent des immersions professionnelles sous différents formats pour préparer à l'emploi.
- Les « accompagnants » qui sont des personnes issues des employeurs partenaires du programme volontaires pour passer du temps avec les jeunes afin de les aider à aborder le monde du travail avec ses codes tout en les soutenant dans leurs actions de préparation puis d'intégration dans l'emploi.
- Des personnes neuroatypiques déjà insérées dans le milieu professionnel, qui peuvent éclairer les étudiants sur leur parcours en leur permettant d'éviter des écueils et montrer que le succès est possible.

Il s'appuie sur un partenariat avec Singularity et un conseil scientifique permettant d'orienter le programme grâce à l'expertise de sachants.

Le Groupe de travail sur l'IA de défense

Parmi les thématiques sociétales du PEC, l'éthique de l'intelligence artificielle occupe une place centrale.

Une table ronde a permis d'aborder ces sujets et de planter le décor pendant l'ECW 2024 puis un livre blanc sur l'IA de confiance dans la Défense a été produit et mis à l'honneur au cours de plusieurs évènements pendant l'année 2025 avec une matinée dédiée à ce sujet pendant l'ECW. Ce livre blanc propose les regards croisés entre industriels, chercheurs, universitaires et acteurs publics sur cette thématique. L'usage de l'IA dans les conflits visibles ou invisibles est déjà là ! C'est pourquoi, développer une IA de confiance exige de concilier analyse stratégique, mesure de la valeur et coopération entre de multiples acteurs.

Axe Europe / Éléments de contexte : la stratégie Europe du PEC

Le Pôle porte une vision stratégique visant au développement d'une filière souveraine de cybersécurité aux niveaux local, national et européen. Cette ambition se décline autour de cinq lignes d'action prioritaires :

- appuyer ou structurer des partenariats stratégiques aux niveaux local, régional et national, en articulation avec les dynamiques européennes ;
- renforcer la visibilité et le positionnement du Pôle auprès des institutions de l'Union européenne (Commission européenne, Parlement européen, Représentation permanente de la France auprès de l'UE), des agences spécialisées (ENISA, CERT-EU, Centre européen de compétences en cybersécurité – ECCC) et des acteurs industriels européens, notamment au sein de l'ECSO ;
- contribuer à la construction des trajectoires technologiques de la filière ;
- participer à la formation et à la montée en compétences des jeunes publics européens ;
- développer des outils et des procédures favorisant l'émergence d'une offre collective structurée à l'échelle européenne.

Mise en œuvre de la dimension européenne

La stratégie européenne du Pôle repose sur un ensemble d'actions structurantes :

- l'European Cyber Week (ECW), événement de référence dont le rayonnement international permet l'implication d'acteurs et de décideurs européens à travers des formats dédiés ;
- l'adhésion à l'European Cyber Security Organisation (ECSO), facilitant l'intégration du Pôle dans les réseaux européens de coopération industrielle et institutionnelle (label Cybersecurity Made in Europe, journées investisseurs, initiatives en faveur de la diversité dans la filière) ;
- la contribution à la Smart Specialisation Strategy (S3) portée par Bretagne Cyber Alliance, au bénéfice de la Région Bretagne, sur l'axe prioritaire de la cybersécurité ;
- l'animation d'un Groupe de travail Europe, ouvert à l'ensemble des membres du Pôle et réuni deux fois par an (février et juillet).

Les travaux du GT Europe couvrent les axes formation, recherche, développement industriel et économique, ainsi que des thématiques transversales telles que la certification et les enjeux sociétaux. Ils s'inscrivent dans une trajectoire progressive articulée autour de trois niveaux d'ambition :

- assurer une veille stratégique afin d'informer les membres, en amont, des évolutions législatives, réglementaires et financières au niveau européen ;
- conduire des actions d'influence ciblées, fondées sur l'identification des groupes de travail pertinents, la cartographie des parties prenantes et la mobilisation des réseaux du Pôle ;
- positionner le Pôle et ses membres comme force de proposition, en facilitant l'accès aux appels à projets, appels d'offres et partenariats européens.

Gouvernance et moyens mobilisés en 2025

En 2025, dans un contexte marqué par l'évolution rapide des politiques européennes de cybersécurité et des cadres réglementaires internationaux, le Pôle a maintenu les moyens dédiés à son action européenne afin d'en consolider les résultats. À ce titre :

- la fonction d'ambassadeur Europe a été reconduite ;
- le poste d'alternant dédié au volet Europe a été pérennisé au sein de l'équipe opérationnelle.

Par ailleurs, l'équipe Europe et les membres actifs du GT contribuent aux travaux du comité de niveau politique « Enjeux stratégiques », mis en place en 2025.

Réunions stratégiques et coordination européenne

Deux réunions du GT Europe se sont tenues en février et juin 2025. Elles ont notamment permis :

- La présentation du projet Cyberhive par l'ECSO ;
- Un échange sur le rôle et les missions du NCC-FR ;
- La présentation du plan d'action 2025 de Bretagne Cyber Alliance ;
- L'examen des feuilles de route 2025-2026 de Bretagne Commerce International et du GT Certification ;
- Un point d'actualité sur les enjeux européens croisant cybersécurité et santé ;
- La présentation du guide relatif au Fonds européen de défense (FED).

Coopération avec Bretagne Cyber Alliance

Une task force conjointe (PEC, Région Bretagne, Bretagne Cyber Alliance) a été constituée afin de renforcer la coordination européenne. Ses travaux visent notamment à :

- Partager et actualiser une cartographie des contacts institutionnels européens, en particulier dans la perspective de l'ECW ;
- Assurer un échange régulier d'informations sur les actions et projets européens en cours, dans une logique de complémentarité et d'appui mutuel.

Veille stratégique et participation aux événements européens

Dans le cadre de son action européenne, le Pôle a assuré une veille régulière sur les principales évolutions politiques, réglementaires et programmatiques en matière de cybersécurité. À ce titre, plusieurs publications et événements structurants ont été identifiés et relayés auprès des membres :

- Évolutions du cadre européen en cybersécurité, notamment dans les domaines de la santé, de la directive NIS 2 et du Cyber Solidarity Act ;
- Lancement d'un programme d'accélération à l'export franco-allemand ;
- Cyber Info Day ;
- Publication et diffusion du guide relatif au Fonds européen de défense (FED) au bénéfice des membres du Pôle ;
- Lancement par le NCC-FR d'un appel à manifestation d'intérêt « IA et cybersécurité » dans le cadre du programme Digital Europe 2025–2027 ;
- Travaux relatifs à la transition vers la cryptographie post-quantique (PQC), incluant des actions menées dans le cadre du GT PEC dédié et un événement organisé lors de l'ECW 2025 ;
- Informations relatives à la réserve de cybersécurité de l'Union européenne ;
- Suivi du dispositif du Tallinn Mechanism.

Axe Europe / Éléments de contexte : la stratégie Europe du PEC

Déplacements et représentation du Pôle

Le Pôle a participé à plusieurs événements importants pour la filière :

- Mission « VP Recherche » à Bochum, organisée dans le cadre de l'accord de coopération entre le PEC et eurobits ;
- Participation aux Infodays du Fonds européen de défense (FED), à Bruxelles ;
- Participation aux Infodays du programme Digital Europe, à Paris, en lien avec le NCC-FR ;
- Participation aux ECSO Days et à l'assemblée générale de l'ECSO, à Bruxelles ;
- Participation aux ECSO Awards et à des rencontres CISO, à Bochum ;
- Participation aux travaux de l'EU DisinfoLab, à Ljubljana.

Guide relatif au Fonds européen de défense

En avril 2025, le Pôle a publié un guide explicatif consacré au Fonds européen de défense (FED), présenté aux membres lors de la réunion du GT Europe de juin. Ce document a été conçu comme un outil d'aide à la décision, visant à accompagner les acteurs de la filière dans l'appréhension du dispositif.
Le guide poursuit les objectifs suivants :

- proposer une lecture claire, synthétique et juridiquement fondée du fonctionnement du FED ;
- présenter les opportunités de financement et les modalités de participation aux appels à projets ouverts en 2025 ;
- formuler des recommandations opérationnelles destinées à améliorer la qualité et la compétitivité des candidatures.

Suite à l'intérêt exprimé par les acteurs institutionnels concernés et au soutien du responsable FED de la direction générale de l'armement (DGA), ce travail a vocation à être prolongé par l'élaboration d'une feuille de route conjointe PEC–DGA.
Une première séquence de cadrage s'est tenue au second semestre 2025, dans la perspective de la refonte du programme FED pour la période 2028–2034 qui vise notamment:

- le renforcement des capacités budgétaires ;
- l'évolution des modalités de gouvernance ;
- l'accélération des calendriers de mise en œuvre.

Cette refonte s'inscrit dans un contexte caractérisé par :

- un déficit de leadership européen sur les volets numérique et cybersécurité du Fonds ;
- une approche « dual use » croissante au sein des différents programmes européens ;
- la nécessité de faciliter un accès plus autonome des PME au FED, en allégeant les charges administratives et en réduisant la dépendance aux prime contractors.

Consolidation du partenariat avec eurobits

La mise en oeuvre de l'accord de coopération avec le Pôle d'excellence cyber de fin 2024 a amené les actions suivantes:

- mission " VP Recherche" à Bochum en avril, incluant des échanges avec la "Cyber Agency Germany" et la visite de la société Eleqtron qui adresse l'informatique quantique ;
- implication et intervention de Eurobits dans deux événements "European Day" de l'ECW 2025 ;
- première structuration d'une feuille de route précisant des actions de coopération ciblées sur les trois axes du Pôle, en vue d'une mise en œuvre opérationnelle dès 2026.

Candidature à un groupe consultatif auprès de l'ECCC

L'European Cybersecurity Competence Centre (ECCC), en lien avec le réseau des Centres nationaux de coordination (NCC), a pour mission de renforcer la compétitivité, l'autonomie stratégique et la capacité d'innovation de la filière européenne de cybersécurité. À ce titre, l'ECCC assure notamment la gestion des financements dédiés dans le cadre des programmes Digital Europe et Horizon Europe.
Afin d'appuyer ses travaux, l'ECCC a engagé la constitution d'un Groupe consultatif stratégique (Strategic Advisory Group – SAG), composé de 20 experts indépendants, via un appel à manifestation d'intérêt.

Le Pôle a présenté sa candidature, qui a été acceptée, pour rejoindre ce groupe consultatif, dont les missions consistent à :

- suivre la performance et l'impact des programmes Digital Europe et Horizon Europe au regard des priorités définies dans la feuille de route stratégique européenne ;
- contribuer à l'analyse de l'offre capacitaire européenne en cybersécurité, des besoins et priorités associés, ainsi que de l'environnement technologique, industriel et réglementaire, en lien avec le réseau des NCC et la communauté des entités cyber de confiance, notamment à travers l'organisation de consultations publiques ;
- formuler des recommandations stratégiques à destination de la direction de l'ECCC et contribuer à l'élaboration des programmes de travail annuels et pluriannuels.

Axe International (hors Europe)

L'Axe International du Pôle d'Excellence Cyber, articulé autour de plusieurs groupes de travail, a pour ambition d'accompagner nos membres dans leur développement à l'export, en particulier les plus petites structures, de renforcer la visibilité du Pôle et de promouvoir à l'international l'image d'une cybersécurité française d'excellence et de confiance. Cet axe mène diverses actions telles que mise en relation avec les ambassades et représentations nationales, mobilisation des réseaux de personnalités et de membres lors d'échanges ou de visites à l'occasion d'événements, création de synergies entre les membres, identification de partenaires et d'homologues étrangers. Ces actions s'effectuent en coordination étroite avec le ministère des Armées et, plus largement, les institutions de l'État.

Le Groupe de Travail Canada

Ce groupe, piloté par NeverHack, rassemble une dizaine d'entreprises déjà implantées au Canada et y développant des activités significatives, ou souhaitant s'y établir pour y ouvrir de nouveaux marchés. Il bénéficie également de l'appui d'In-Sec-M, association avec laquelle le PEC avait conclu une convention de partenariat lors de l'ECW 2023.

Cette coopération se poursuit en 2025 avec une journée dédiée au Canada-Québec lors de l'European Cyber Week. Cette journée a été montée en partenariat avec NeverHack, In-Sec-M, et l'Université de Bretagne et a notamment abordé les sujets du post-quantique et de l'IA générative. A l'issue de cette journée, des conventions ont été signées entre le PEC et les instituts de recherche IMC2 et Pôle d'Expertise en Cybersécurité Intact.

Le Groupe de Travail Asie - Singapour

Ce groupe, piloté par Charles Thooris de Secure-IC, réunit une petite dizaine d'entreprises qui sont soit déjà implantées à Singapour et y ont des activités significatives, soit qui souhaitent s'y implanter et y développer un marché.

- Présence d'une délégation pour le salon GovWare en octobre 2025 en collaboration avec la chambre de commerce française à Singapour. Pour la seconde fois, sept de nos entreprises se sont retrouvées sur un pavillon France, soit deux de plus que l'année précedente : BreacHunt, Filigran, Hackuity, Secure-IC, Sekoia.io, Bactech, iDakto.
- Des réunions de travail ont été organisées avec CapVista, un investisseur singapourien tourné vers l'écosystème deep-tech, avec un fort ancrage dans les domaines de la défense et de la sécurité. Bras d'investissement de la DSTA, elle identifie et accompagne des technologies émergentes à double usage, en offrant non seulement des financements, mais aussi un soutien technique et stratégique pour leur intégration dans les politiques nationales de sécurité et d'innovation.
- Organisation de Webinaires :
  - > « Explorer les opportunités Cyber en Corée du Sud, un guide pour les acteurs français » avec Julien Provenzano (FKCA)
  - > « Explorer les opportunités numériques en Inde » avec Thierry Berthelot (Préfecture de la région Bretagne)

Le Groupe de Travail AFMO - Maroc

Ce groupe, piloté par Yassir Kazar de Yogosha, réunit une petite dizaine d'entreprises qui sont soit déjà implantées au Maroc et y ont des activités significatives, soit qui souhaitent s'y implanter. Il s'articule autour de quatre axes différents : commercial, universitaire, diplomatique et militaire.

- Participation au SIT AFRICA
- Participation au GITEX Africa à Marrakech avec une soirée organisée par le PEC au sein du Consulat
- Participation au GISEC à Dubaï
- Présence de délégations marocaine, sénégalaise et émiratie lors de l'ECW

En perspective pour 2026, étude de l'opportunité d'un groupe de travail Ukraine suite à l'arrivée récente d'un nouveau chargé des affaires économiques à Paris.

Structuration du dispositif cybersécurité – EDIH Bretagne

Évolution du programme et nouvelle organisation

L'année écoulée marque une évolution structurante majeure dans la mise en œuvre des actions cybersécurité portées par le Pôle d'Excellence Cyber dans le cadre de l'EDIH Bretagne.
Le programme PACTE, tel qu'il avait été initialement conçu, a été progressivement arrêté au profit d'une organisation plus opérationnelle, transverse et pérenne, incarnée par la structuration de l'équipe Sec.Ops.

Cette évolution répond à plusieurs constats :

- un besoin accru de capacité opérationnelle face à la demande croissante des bénéficiaires,
- la nécessité d'une vision élargie des services cyber, allant au-delà du seul diagnostic,
- une volonté de mieux articuler prévention, accompagnement, mise en œuvre technique et sensibilisation.

Renforcement et structuration de l'équipe Sec.Ops

Dans ce contexte, l'équipe est passée de 2 à 4 personnes, permettant une montée en puissance significative du dispositif.
Cette nouvelle structuration repose sur une approche complémentaire des rôles, inspirée des logiques Red / Blue / Purple / White Team, afin de couvrir l'ensemble du cycle de maturité cybersécurité des organisations accompagnées.

Cette organisation permet :

- une meilleure répartition des charges,
- une montée en expertise collective,
- une capacité accrue à répondre simultanément à des diagnostics, des accompagnements et des actions de sensibilisation.

L'équipe Sec.Ops constitue désormais le socle opérationnel du volet cybersécurité de l'EDIH Bretagne, en lien étroit avec l'écosystème de prestataires référencés au sein du CYEC – Cyber Expert Catalogue.




Étoffement et structuration de l'offre de services

La nouvelle organisation a permis un élargissement et une structuration progressive du catalogue de services cyber, avec des objectifs opérationnels clairement définis jusqu'à la fin du programme EDIH (en avril 2026).

Objectifs opérationnels réévalués (EDIH V1)

- 90 diagnostics cybersécurité
- 25 accompagnements structurés
- 5 enveloppes de financement complémentaires mobilisées
- 20 scans de vulnérabilités externes
- 1 scan interne & externe avec logique de surveillance
- 4 analyses de risques approfondies
- Déploiement d'actions de sensibilisation et de montée en compétences

Ces objectifs s'inscrivent dans une logique de progression en maturité, permettant aux bénéficiaires de passer d'un état des lieux à une sécurisation effective de leur système d'information.

État d'avancement et résultats intermédiaires

À date, les résultats obtenus traduisent une dynamique positive et une appropriation forte du dispositif par les acteurs du territoire :

- 55 diagnostics cybersécurité réalisés sur les 90 prévus
- 12 accompagnements engagés et terminés, avec 8 en attente de démarrage
- Ces actions ont permis de mobiliser environ 100 000 euros d'aides européennes au bénéfice des entreprises accompagnées
- Les bénéficiaires ont pu mettre en œuvre des actions concrètes de sécurisation grâce aux prestataires référencés dans le CYEC
- 1 analyse de risques réalisée sur les 4 prévues
- Les offres de scans de vulnérabilités (externes) sont en cours de structuration, expliquant l'absence de réalisations à ce stade.

Les actions de sensibilisation (Hack & Learn, Tutos Cyber & IA) ont d'ores et déjà dépassé les objectifs initiaux.

Ces résultats démontrent l'impact direct du dispositif sur la montée en maturité cyber des structures accompagnées, en particulier les Établissements de Santé, PME, associations et collectivités, souvent peu dotées en ressources internes.

Diversification des formats et actions de sensibilisation

Au-delà des services strictement cyber, l'année a également été marquée par une diversification des formats d'accompagnement.

L'équipe Sec.Ops a ainsi contribué à :

- la conception et l'animation de sessions Hack & Learn, permettant une sensibilisation concrète et opérationnelle aux enjeux cyber,
- la production de tutoriels cybersécurité et IA, en collaboration avec l'équipe Images & Réseaux , afin de réaliser des contenus pédagogiques accessibles et adaptés aux publics accompagnés.

Ces actions renforcent l'impact du programme en agissant sur le facteur humain, identifié comme un levier majeur de réduction des risques.

Structuration du dispositif cybersécurité – EDIH Bretagne

Cadre temporel et perspectives

Le dispositif EDIH Bretagne, dans sa 1ère version, permet de proposer des services cybersécurité jusqu'à fin avril 2026, avec un cofinancement européen constituant un levier essentiel pour les bénéficiaires.
Les priorités pour la période à venir portent sur :

- la poursuite des diagnostics et accompagnements,
- la montée en charge des offres de scans de vulnérabilités,
- la structuration complète des analyses de risques,
- le renforcement du lien entre diagnostics, accompagnements et prestataires du CYEC,
- la préparation de la transition vers l'EDIH V2, avec une offre encore plus lisible, industrialisée et orientée résultats.

La transformation du programme PACTE vers une équipe Sec.Ops structurée et opérationnelle marque une étape clé dans la maturité du dispositif cybersécurité de l'EDIH Bretagne.

Cette évolution a permis de renforcer l'impact terrain, d'élargir l'offre de services et de mieux répondre aux besoins concrets des acteurs bretons, tout en optimisant l'utilisation des financements européens.

Transition vers EDIH V2 – Industrialisation et pérennisation

La dynamique engagée ouvre la voie à l'EDIH V2, avec une ambition renforcée :

Objectifs structurants EDIH V2 :

- passer d'un modèle "projet" à un modèle industrialisé et réplicable,
- renforcer la capacité de traitement (volume, complexité, sectorisation),
- intégrer davantage de services techniques avancés (scans, supervision, risques),
- consolider le rôle du CYEC comme catalogue de prestataires de confiance,
- renforcer la mesure d'impact (KPI, maturité, trajectoires de progrès).

Évolutions attendues :

- spécialisation accrue des rôles au sein de l'équipe Sec.Ops,
- meilleure articulation entre :
  - prévention,
  - détection,
  - réponse,
  - accompagnement stratégique,
- déploiement de parcours cyber sectoriels (santé, industrie, collectivités, ESMS).

European Cyber Week 2025

Une édition qui confirme le changement d'échelle du congrès

La 10ème édition de l'European Cyber Week, organisée du 17 au 20 novembre à Rennes, s'est achevée sur un bilan remarquable :

- Plus de **8 500 participants**,
- **130 partenaires** français et européens
- Plus de **100 événements**, tables rondes et ateliers organisés
- Un programme riche et complet,
- Des intervenants de haut niveau,
- Une présence internationale renforcée,
- Et un fort taux de participation aux conférences.

Cette édition anniversaire a mobilisé tous les acteurs de l'écosystème cyber régalien autour de l'objectif : établir **une souveraineté numérique durable,** face aux défis géopolitiques et technologiques actuels.

Au cours de ces **quatre jours de congrès**, les plus de **100 événements**, tables rondes et ateliers organisés ont à nouveau positionné Rennes comme le centre névralgique de la cybersécurité, de la cyberdéfense et de l'IA de défense.

Les grandes Thématiques 2025

SOUVERAINETÉ NUMÉRIQUE EUROPÉENNE : À l'heure où les infrastructures critiques, les données sensibles et les outils de défense reposent encore largement sur des technologies extra-européennes, la souveraineté numérique devient une condition de survie économique, politique et démocratique. L'ECW 2025 a mis en lumière les initiatives visant à mutualiser les investissements, développer des technologies souveraines (cloud, semi-conducteurs, cyber solutions) et bâtir une Europe plus résiliente face aux pressions géopolitiques et aux cyberattaques.

CYBERSÉCURITÉ ET INTELLIGENCE ARTIFICIELLE : L'IA transforme tous les domaines — défense, santé, finance, énergie — mais son adoption rapide ouvre aussi la porte à de nouvelles vulnérabilités. Les conférences de l'ECW 2025 ont exploré ce paradoxe : comment faire de l'IA un outil de résilience et de supériorité opérationnelle, tout en limitant les risques de manipulation, de dépendance et de compromission. La notion d'IA de confiance était au coeur des débats, avec un focus sur la robustesse, l'explicabilité et la qualification des systèmes.

CYBERDÉFENSE : Au coeur des missions régaliennes, la cyberdéfense vise à protéger les forces armées, les infrastructures critiques et les citoyens face à des menaces de plus en plus hybrides. Elle combine la lutte défensive (protection des systèmes d'armes et d'information), offensive (capacité de riposte dans le cyberespace) et l'influence (contrer la désinformation et les manipulations). L'ECW 2025 a mis en avant cette triple dimension à travers des conférences stratégiques, des wargames, et la grande finale du Capture The Flag – autant de terrains d'expérimentation et d'anticipation des conflits numériques de demain.

ENJEUX SOCIÉTAUX : La cybersécurité souffre d'un manque de talents, mais aussi d'un déficit de diversité. En 2025, seules 11 % des professionnels du secteur sont des femmes, et les profils neuroatypiques restent encore trop peu valorisés. L'ECW 2025 a mis à l'honneur deux initiatives inédites : la 5e promotion des Cadettes de la cyber, programme qui inspire et accompagne des étudiantes en filières cyber dans leur formation et insertion. Dans un autre axe, le lancement de Cyber Singuliers, un dispositif d'accompagnement pour l'intégration des profils neuroatypiques. L'objectif était clair : faire de la diversité une force stratégique pour l'innovation de notre secteur.

Les Points forts du Parcours européen

En 2025, ce parcours s'est renforcé à travers l'organisation de quatre European Days, en complément d'interventions d'acteurs européens au sein des conférences scientifiques :

INVESTOR DAY: dédié à l'accès au financement pour des start-ups françaises positionnées sur les marchés européens.

START-UPS ET PME DANS LA CONQUÊTE DU MARCHÉ EUROPÉEN : visant le partage de retours d'expérience et de bonnes pratiques industrielles et dialogue entre institutions et entreprises.

COOPÉRATIONS RÉGIONALES ET CYBER-RÉSILIENCE : consacré au rôle des coopérations territoriales dans le déploiement des politiques européennes de cybersécurité.

ESPACE ET INDUSTRIE DU FUTUR : portant sur les enjeux émergents de cybersécurité dans le domaine spatial.

Au total, près de quarante représentants européens, civils et militaires, ont été accueillis dans le cadre du congrès.

Les Points forts du Parcours AI in Defence

IA DE DÉFENSE BY AMIAD : Cet événement dédié à l'IA au service de la défense a rassemblé des experts, des décideurs et des opérationnels pour discuter des avancées technologiques, des besoins opérationnels et des implications stratégiques de l'IA militaire. Il s'est cloturée par la vision de Bertrand Rondepierre, Directeur de l'AMIAD – l'Agence ministérielle pour l'IA de défense, sur l'avenir de l'IA militaire.

CAID (CONFERENCE ON ARTIFICIAL INTELLIGENCE FOR DEFENCE) : Organisée par l'AMIAD, la 7ème édition de CAID était un rendez-vous majeur sur l'IA appliquée à la Défense. Elle a présenté les dernières applications Terre, Air, Mer, Cyber, Renseignement et Commandement, en mettant l'accent sur la robustesse, l'explicabilité, la frugalité et l'intégration embarquée. L'édition 2025 était particulièrement dédiée à l'autonomie, la robotique militaire et aux architectures frugales, illustrées par des cas d'usage concrets.

IA ET ROBOTIQUE : L'AMIAD a organisé une conférence scientifique dédiée à l'IA et la robotique. Cet événement a fait intervenir des chercheurs reconnus dans leur domaine, pour partager leurs travaux sur la perception temps-réel, la navigation tout-terrain, la collaboration multi-robots ou encore l'interaction homme-robot.

Les nouveautés 2025

PROGRAMME ET ÉQUIPEMENT PRIORITAIRE DE RECHERCHE (PEPR) CYBER DAY : Lancé en 2022 dans le cadre de la Stratégie Nationale pour la Cybersécurité (SNC) de France 2030, le PEPR Cybersécurité vise à renforcer les capacités nationales de protection de l'ensemble de la chaîne de cybersécurité. La conférence PEPR Cyber Day a déroulé en un tour d'horizon des grands défis en matière de sécurité au sens large (sécurité des applications de messagerie, des données personnelles et industrielles, de l'IA…) ainsi que les points durs spécifiques à chaque enjeu justifiant une recherche scientifique.

European Cyber Week 2025

DATA CENTRIC SECURITY (DCS) : La conférence Data Centric Security a exposé les principaux enjeux de sécurité centrée sur les données ayant cours en 2025 (confidentialité, intégrité, accessibilité, partage…), ainsi que les grands concepts de défense attenants (méthode du « Zero Trust », etc.). Etaient mis en lumières les présentations industrielles et processus d'accompagnement du ministère des Armées.

JE CHOISIS LA FRENCH TECH : Cet événement « showroom » porté par Le Poool et La French Tech Rennes St Malo était dédié avant tout aux acheteurs et aux décideurs. Des start-ups françaises et leurs acheteurs ont dévoilé le fruit de leur collaboration, avec dans chaque cas la problématique acheteur, la solution déployée, le résultat et des preuves tangibles que l'innovation peut répondre aux défis de cybersécurité et d'IA.

CRYPTOGRAPHIE POST-QUANTIQUE (PQC) : Cette conférence organisée par l'ANSSI était consacrée aux grands enjeux de la transition vers la cryptographie post quantique en France. Elle était également l'occasion de partager les premiers retours d'expérience des parties-prenantes (offreurs de solutions, utilisateurs et centres d'évaluation) sur leurs travaux en cours.


ACCEIS
ANOZR WAY
Nation Data Center
30
33
34
35
36


REMISE DES PRIX
19 novembre à 19h00
Salle NEF
CHALLENGE TAM
AIRBUS
YOGOSHA – SAHAR
PÔLE D'EXCELLENCE CYBER
COMCYBER
CHALLENGE CYBER INTERARMEES
TERRE
AIR
MER


European Cyber Week
10ème anniversaire
European Cyber Week
by CYBER


RENNES MÉTROPOLE
PÔLE D'EXCELLENCE CYBER


Anne Le Hénanff
Ministre déléguée chargée
de l'Intelligence artificielle
et du Numérique
European Cyber Week, jeudi 20 novembre 2025


Gamification
qu'il n'y a pas de droit de propriété ? Il n'y a pas de droits d'auteur sur ça.
Et le truc, c'est que vous pouvez
DGA ECW


10ème anniversaire

Les cadettes de la cyber

Les activités des Cadettes de la Cyber – 2025

En 2025, les actions de sensibilisation ont une nouvelle fois constitué un axe central du programme des Cadettes de la cyber, à travers des interventions menées au plus près des jeunes, dans les collèges et lycées, ainsi que lors de salons et événements organisés partout en France, de Rennes à Toulouse, en passant par Bordeaux, Paris ou Vannes.

Ces temps d'échange ont permis aux Cadettes de la cyber de créer un lien direct et privilégié avec les collégiens et lycéens, leur permettant de découvrir les métiers et expertises de la cybersécurité, d'envisager des parcours de formation, et de mieux comprendre les risques et enjeux actuels du numérique.

Au-delà des actions de sensibilisation menées sur le terrain, le programme s'appuie également sur des dispositifs plus engageants et immersifs.

Cette approche s'est concrétisée par l'engagement des Cadettes de la cyber dans le projet Bootcamp Cybersécurité, porté par l'association Stem4All et coorganisé avec Cyber4Tomorrow et la Fondation Inria, qui s'est tenu en août 2025. Ce temps fort a permis de sensibiliser des lycéennes à des thématiques structurantes de la cybersécurité, telles que l'OSINT ou la Red Team, tout en ouvrant des perspectives concrètes de formation et de parcours professionnels.

Cette année a également été marquée par l'accompagnement de projets ambitieux portés par les Cadettes de la cyber.

Parmi eux, l'ouvrage collectif « Cybersécurité : un défi citoyen et stratégique », officiellement présenté lors de l'European Cyber Week 2025.
Ce projet a constitué une opportunité pour les Cadettes de vulgariser des sujets de cybersécurité auprès d'un public non-expert, tout en démontrant leurs compétences en recherche, analyse et synthèse, à travers une approche pluridisciplinaire intégrant des dimensions géopolitiques, techniques, juridiques et sociales.

Le programme a également accompagné la production d'une application-web développée par les Cadettes, « Cyber-Chall ».

Destinée à appuyer les actions de sensibilisation des Cadettes auprès des nouvelles générations, « Cyber-Chall » est un outil pédagogique composé de différents modules permettant de rendre plus dynamique et ludique ces interventions auprès des collégiens et lycéens. Testée pour la première fois lors de l'ECW 2025 auprès d'une classe de seconde, l'application a permis aux Cadettes de recueillir leurs premiers retours utilisateurs. Ces enseignements servent aujourd'hui à améliorer l'outil afin d'envisager un déploiement progressif lors de l'ensemble de leurs interventions.

En 2026, nous poursuivrons l'accompagnement de ces projets, ainsi que de ceux menés lors des précédentes années, comme le podcast « La Matrice a buggé » qui fêtera cette année ses 3 ans et qui témoigne de l'inspiration des Cadettes à vouloir varier les formats afin de vulgariser la cyber à tous.

De nouveaux projets sont également en cours de développement, comme la production d'une bande dessinée destinée à un jeune public non initié, visant à proposer une nouvelle approche de la sensibilisation à la cybersécurité.

Les Cadettes sont également actives sur les réseaux sociaux en proposant de nouvelles lignes éditoriales telles que :

- les « News-bimensuelles », des publications dont le but est de partager deux fois par mois les dernières l'actualité du monde de la cyber,

- « le Panorama des métiers » dont les premiers contenus verront le jour prochainement et donc l'objectif est de présenter de manière ludique les différents métiers de la cybersécurité.

- Ou bien "Woman Cyber Field", un format de vidéos courtes portant sur les aspects général du monde de la cyber et du numérique ainsi que sur la féminisation de milieux encore majoritairement masculins.

À travers ces projets solidaires et collectifs, toutes ont appris à découvrir leur plein potentiel, alliant cyber et féminisation. Un beau symbole d'inclusion pour les enjeux sociétaux et le Pôle d'Excellence Cyber.

Aussi, afin de développer l'esprit de sororité et de solidarité au sein du programme, ces dernières ont pu vivre cette année un stage d'« aguerrissement » effectué cet été et qui a été source pour elles de cohésion et de dépassement de soi.

Pour conclure, la 5e promotion des Cadettes de la cyber a été officiellement présentée lors de la 10e édition de l'European Cyber Week, une promotion composée de 14 femmes aux profils variés prêtes à poursuivre les actions et engagements de leurs prédécesseuses au sein d'un programme qui fêtera cette année ses 5 ans d'existence et d'accompagnement de la féminisation de la filière cybersécurité.

PÔLE D'EXCELLENCE
CYBER

www.pole-excellence-cyber.org