Envoyé en préfecture le 20/10/2016
Reçu en préfecture le 20/10/2016
Affiché le
ID : 035-233500016-20161013-16_DGS_04-DE

**REGION BRETAGNE**

**Délibération N°16_DGS_04**

CONSEIL REGIONAL

13 octobre 2016

DELIBERATION

# La Bretagne, cyber valley européenne

Le Conseil régional, convoqué par son Président le 20 septembre 2016, s'est réuni en séance plénière le jeudi 13 octobre 2016 à 14h30 au siège de la Région Bretagne, sous la Présidence de Monsieur Jean Yves LE DRIAN, Président du Conseil régional.

**Étaient présents** : Monsieur Olivier ALLAIN, Madame Sylvie ARGAT-BOURIOT, Monsieur Eric BERROCHE, Madame Catherine BLEIN, Madame Mona BRAS, Madame Georgette BREARD (arrivée à 16 heures 25), Monsieur Gwenegan BUI, Monsieur Thierry BURLOT , Madame Gaby CADIOU, Monsieur Loïg CHESNAIS-GIRARD, Monsieur Marc COATANEA, Monsieur André CROCQ (départ à 20 heures), Madame Virginie D'ORSANNE, Madame Delphine DAVID, Monsieur Gérard DE MELLON, Monsieur Stéphane DE SALLIER DUPIN, Madame Laurence DUFFAUD , Madame Corinne ERHEL, Monsieur Richard FERRAND, Madame Laurence FORTIN, Madame Anne GALLO, Madame Evelyne GAUTIER-LE BAIL, Monsieur Karim GHACHEM, Madame Anne-Maud GOUJON (départ à 18 heures 15), Madame Claire GUINEMER, Madame Kaourintine HULAUD, Monsieur Bertrand IRAGNE, Madame Elisabeth JOUNEAUX-PEDRONO, Monsieur Pierre KARLESKIND, Monsieur Gérard LAHELLEC, Monsieur Jean-Michel LE BOULANGER , Monsieur Olivier LE BRAS, Monsieur Raymond LE BRAZIDEC, Madame Agnès LE BRUN , Monsieur Jean-Yves LE DRIAN, Monsieur Marc LE FUR, Monsieur Patrick LE FUR (départ à 19 heures 30), Madame Gaël LE MEUR, Madame Nicole LE PEIH, Monsieur Alain LE QUELLEC, Madame Gaël LE SAOUT , Madame Christine LE STRAT, Monsieur Christian LECHEVALIER, Madame Lena LOUARN , Monsieur Bernard MARBOEUF, Monsieur Martin MEYRIER (départ à 20 heures), Monsieur Philippe MIAILHES, Monsieur Paul MOLAC, Madame Gaëlle NICOLAS , Madame Gaëlle NIQUE (arrivée à 16 heures 25), Madame Anne PATAULT, Madame Isabelle PELLERIN , Monsieur Gilles PENNELLE, Monsieur Stéphane PERRIN, Monsieur Maxime PICARD, Monsieur Bernard POULIQUEN, Monsieur Pierre POULIQUEN, Monsieur Bruno QUILLIVIC, Monsieur Dominique RAMARD, Madame Emmanuelle RASSENEUR, Madame Agnès RICHARD, Monsieur David ROBO (départ à 18 heures 15), Madame Claudia ROUAUX (arrivée à 16 heures 15, départ à 17 heures 40), Monsieur Stéphane ROUDAUT , Madame Catherine SAINT-JAMES, Madame Forough SALAMI-DADKHAH, Monsieur Emeric SALMON, Madame Hind SAOUD, Monsieur Sébastien SEMERIL (départ à 20 heures 15), Madame Renée THOMAIDIS, Madame Martine TISON, Madame Anne TROALEN, Monsieur Hervé UTARD, Madame Anne VANEECLOO, Madame Gaëlle VIGOUROUX, Madame Sylvaine VULPIANI.

**Avaient donné pouvoir** : Madame Georgette BREARD (pouvoir donné à Madame Forough SALAMI-DADKHAH de 14 heures 30 à 16 heures 25), Monsieur Pierre BRETEAU (pouvoir donné à Monsieur Bernard MARBOEUF), Monsieur André CROCQ (pouvoir donné à Madame Laurence DUFFAUD à partir de 20 heures), Madame Anne-Maud GOUJON (pouvoir donné à Madame Agnès LE BRUN à partir de 18 heures 15), Madame Sylvie GUIGNARD (pouvoir donné à Monsieur Marc LE FUR), , Monsieur Philippe HERCOUET (pouvoir donné à Madame Anne TROALEN), Monsieur Roland JOURDAIN (pouvoir donné à

Envoyé en préfecture le 20/10/2016
Reçu en préfecture le 20/10/2016
Affiché le
ID : 035-233500016-20161013-16_DGS_04-DE

**REGION BRETAGNE**

Madame Emmanuelle RASSENEUR), Madame Isabelle LE BAL (pouvoir donné à Madame Gaëlle NICOLAS), Monsieur Patrick LE DIFFON (pouvoir donné à Madame Christine LE STRAT), Monsieur Patrick LE FUR (pouvoir donné à Monsieur Gilles PENNELLE à partir de 19 heures 30), Monsieur Martin MEYRIER(pouvoir donné à Madame Catherine SAINT-JAMES à partir de 20 heures), Madame Gaëlle NIQUE (pouvoir donné à Monsieur Maxime PICARD de 14 heures 30 à 16 heurs 25), Monsieur Bertrand PLOUVIER (pouvoir donné à Madame Claire GUINEMER), Monsieur David ROBO ( pouvoir donné à Monsieur Stéphane DE SALLIER DUPIN à partir de 18 heures 15), Madame Claudia ROUAUX (pouvoir donné à Madame Hind SAOUD de 14 heures 30 à 16 heures 15 et à partir de 17 heures 40), Monsieur Sébastien SEMERIL (pouvoir donné à Monsieur Hervé UTARD à partir de 20 heures 15).

Vu le code général des collectivités territoriales ;

Au vu du rapport présenté par Monsieur le Président du Conseil régional ;

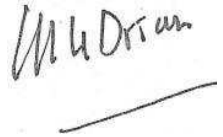
Après avoir pris connaissance de l'avis formulé par le Conseil économique, social et environnemental régional lors de sa réunion du 3 octobre 2016 ;

Après avoir pris connaissance des avis de la commission Éducation, Formation et Emploi du 5 octobre 2016 et de la commission Économie, Agriculture et Mer, Europe du 7 octobre 2016 ;

Et après en avoir délibéré ;

**A pris acte** de la communication, jointe en annexe, relative à la Bretagne, cyber-valley européenne.

Le Président du Conseil régional



Jean-Yves Le Drian

Annexe à la délibération du Conseil régional
n° 16 DGS 04
Reçu en préfecture le 20/10/2016
Affiché le
ID : 035-233500016-20161013-16_DGS_04-DE



Direction générale des services

Session du Conseil régional
13 octobre 2016

# La Bretagne, cyber-valley européenne

La cybersécurité et la cyberdéfense sont désormais des priorités pour les Etats, pour les entreprises mais aussi pour les citoyens. Le récent rapport de l'agence nationale de la sécurité des systèmes d'information (ANSSI) rappelle qu'en 2015 la France a subi plus d'une vingtaine d'attaques majeures (le double de 2014). Il n'est plus aujourd'hui d'Etats non menacés par des opérations cyber-terroristes, de citoyens à l'abri d'un piratage de leurs données personnelles ou d'acteurs économiques définitivement protégés d'un vol de données.

Cette omniprésence de la cyber nous est rappelée par la définition qu'en donne l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) : la cybersécurité est "l'état recherché pour un système d'informations lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises". Elle est donc de haute importance pour les particuliers , mais aussi, à plus grande échelle, pour les entreprises, pour les infrastructures, pour les Etats.

La cybersécurité concerne la sécurité des systèmes d'information (SSI) : les réseaux, les logiciels, les politiques de sécurité, les moyens d'authentification, de détection et de riposte, les algorithmes, et protocoles de chiffrement, les composants électroniques… et concerne à court et moyen termes tous les marchés civils, publics et militaires, toutes les industries stratégiques et les administrations publiques, services bancaires et secteurs médicaux, BtoB puis BtoC. La sécurisation du cyberespace est à la fois une condition de nos libertés individuelles mais aussi de la compétitivité et de la viabilité de nos entreprises. C'est un enjeu planétaire qui nécessite des investissements considérables dans le domaine de la recherche, de la formation et de l'innovation. Les perspectives de développement sont donc considérables à condition de prendre et de garder de l'avance car les cycles économiques, en particulier dans ce domaine, sont de plus en plus courts.

La France s'est dotée dès 2013 d'une doctrine et a engagé des moyens. A la suite de la publication du livre blanc de la Défense, le Ministère de la Défense a présenté sa stratégie. Il a ensuite présenté le plan Défense Cyber de 2014 qui a conduit par exemple à renforcer les équipes de la Direction générale de l'Armement-Maîtrise de l'information à Bruz et à créer un pôle numérique de Défense.

Le Ministère de l'intérieur a aussi publié sa stratégie nationale pour la sécurité du numérique en 2015 qui se fixe comme objectifs de lutter contre la cyber criminalité, accompagner les victimes, faire dialoguer les acteurs cyber et faire évoluer le cadre juridique.

Dans cette temporalité, la Bretagne a fait de la cybersécurité une des priorités de sa stratégie de développement économique, d'innovation et d'internationalisation et a inscrit la cyber comme une des priorités de sa Stratégie Régionale de Spécialisation (S3). Ce choix de positionnement sur la cyber a par ailleurs été confirmé dans le Pacte d'avenir pour la Bretagne. Dès lors, un travail a commencé d'identification des acteurs bretons du domaine et d'écriture d'une feuille de route.

La rencontre de la stratégie régionale et de celle de l'Etat s'est traduite par l'annonce en février 2014 de la création du Pôle d'excellence cyber (PEC) en Bretagne. Ce pôle regroupe une centaine d'acteurs issus du monde militaire avec par exemple la DGA-Maîtrise de l'information et l'ensemble des écoles militaires présentes en Bretagne, et du monde civil avec plusieurs grandes entreprises, des PME et les acteurs de l'enseignement supérieur et de la recherche. Il s'est organisé dans une logique projet autour de 3 enjeux majeurs : la formation, la recherche et l'innovation. Il est désormais organisé en association et présidé par un représentant du groupe La Poste.

L'ambition de notre région est, à partir de nos savoir-faire et avec la structuration qu'offre le pôle d'excellence cyber et la mobilisation de notre écosystème numérique, d'être le territoire leader en Europe, capable de répondre à l'ensemble des enjeux cyber, des besoins correspondants et ainsi de voir se développer massivement cette nouvelle filière sur notre territoire.

# 1. Pourquoi un positionnement breton sur la cyber ?

## 1.1. Un enjeu mondial de société et de développement économique

Le marché de la cybersécurité devrait atteindre 2 milliards d'euros en 2017 en France avec une croissance annuelle de plus de 10 %. Son essor ne devrait pas ralentir au vu de la poursuite de la révolution numérique et de l'émergence de l'internet des objets ou du cloud qui ne feront qu'accroître les besoins en nouveaux outils et services capables de sécuriser les données.

Ce marché répond à un besoin majeur qui se révèle aujourd'hui au travers d'affaires spectaculaires (Sony, cyber-terrorisme, TV5 Monde, Ashley Madison…). Des affaires qui montrent la montée en puissance d'une nouvelle criminalité organisée, bien loin de l'image « sympathique » du jeune hackeur piratant depuis sa chambre.

Les risques ne concernent plus seulement l'intégrité de nos données numériques ou de nos échanges mais s'étendent à l'ensemble des infrastructures critiques (eau, gaz, services financiers…), à la mobilité, à la santé, bref à l'ensemble de notre vie quotidienne et de nos activités économiques.

Les besoins en formation, en recherche et innovation pour toujours garder un coup d'avance sur les menaces ne vont donc pas se tarir dans les années qui viennent.

C'est aussi une question de souveraineté car celui qui disposera des technologies pour se défendre occupera une place plus enviable que celui qui devra les acheter. Il y a donc, non seulement un besoin économique mais aussi un engagement des pouvoirs publics pour faire émerger ce secteur en France et en Europe.

## 1.2. Une concentration des forces en Bretagne unique en Europe

La Bretagne peut s'appuyer sur une concentration de savoir-faire et de moyens sans équivalents en Europe comme nos échanges avec la Commission Européenne ou l'OTAN en témoignent.

La Bretagne s'appuie d'abord sur son histoire et ses implantations militaires. Les forces en présence sont bien sûr celles du Ministère de la Défense avec la DGA-MI basée à Bruz ou le CALID (Centre d'Analyse en Lutte Informatique Défensive) à Rennes qui se voient renforcées. Mais ce sont aussi l'ensemble des écoles militaires telles que l'école navale à Brest, Saint-Cyr Coëtquidan, l'ETRS (école des transmissions), ENSTA Bretagne qui sont en première ligne pour répondre aux besoins militaires de formation. Enfin, c'est l'héritage d'une histoire industrielle qui a permis en Bretagne de développer des compétences dans les télécoms, l'électronique de Défense et l'implantation de leaders comme Orange, Alcatel, Thales ou DCNS et de devenir la 2ème région numérique de France après l'Ile-de-France.

La Bretagne dispose également d'un écosystème de formation et de recherche civile de niveau mondial. Ce ne sont pas moins de 200 chercheurs travaillant exclusivement sur des problématiques cyber qui ont été identifiés. Ils couvrent autant des compétences en numérique, en électronique, en mathématiques qu'en sciences sociales. Peuvent être citées l'Université de Rennes 1 et l'Université Bretagne Sud qui ont développé depuis quelques années le premier cursus en alternance d'ingénieur cyber, des grandes écoles comme Centrale-Supélec ou Mines Télécom Bretagne et des laboratoires de recherche comme l'INRIA qui constituent des références internationales.

Ce groupe d'acteurs de très haut niveau peut par ailleurs s'appuyer sur des formations de type IUT présentes sur plusieurs territoires bretons et qui permettent de développer des cursus courts dans le domaine cyber ou d'enrichir les cursus informatiques.

Reçu en préfecture le 20/10/2016
Affiché le
ID : 035-233500016-20161013-16_DGS_04-DE

Enfin, la Bretagne peut se targuer de la présence de leaders mondiaux du domaine tels que Thales, DCNS, Orange, Sopra, CGI et désormais Nokia qui a annoncé des investissements à Lannion sur la cyber. Derrière ces grands groupes, une centaine de PME évoluent sur le marché de la cyber dont certaines, identifiées comme les champions de demain, connaissent des croissances fortes à l'international.

En lien avec ces acteurs, notre région peut aussi s'appuyer sur un écosystème performant dont l'ensemble a fait de la cyber une priorité. Nous pouvons citer le pôle Images & Réseaux, l'institut de recherche technologique B-COM, Meito qui a apporté un soutien essentiel à la structuration de la filière et dont les missions cyber ont été reprises au sein de Bretagne Développement Innovation, agence elle-même à la manœuvre sur le volet économique. Ou bien encore Bretagne Commerce International, par son appui au développement de nos entreprises bretonnes de la cyber à l'étranger ou l'accompagnement à l'implantation d'entreprises étrangères en région.

**Au total, on évalue à 2500 le nombre d'emplois** directs concernés en Bretagne par le développement de la cybersécurité et nous pouvons revendiquer de jouer les premiers rôles en Europe sur ce domaine.

### 1.3. Une filière qui concerne tout le territoire breton, qui renforce notre économie numérique et électronique

Si la concentration des acteurs est forte à Rennes, l'ensemble du territoire breton est concerné par la présence d'écoles, d'universités et d'entreprises. L'action du Conseil régional mobilise la Bretagne toute entière, à la fois en raison de la présence d'acteurs cyber, mais aussi par l'impact positif sur l'ensemble du tissu numérique et électronique qu'aura le développement de la cyber.

En effet, cette spécialisation sur la cyber apporte à notre filière numérique, deuxième de France, un nouvel atout pour rayonner et se développer. Il n'est pas un acteur numérique qui ne soit pas concerné par les problématiques de sécurité. De plus, les très hautes technologies que ces métiers développent permettent de mettre en valeur l'ensemble du tissu d'enseignement supérieur et de recherche ainsi que bon nombre de PME. Enfin, il s'agit d'un marché mondial qui nous permet d'accroître notre visibilité en Europe et à l'international comme le montrent déjà les nombreuses marques d'intérêts de groupes étrangers et de l'OTAN.

Les acteurs de la cyber en Bretagne (Source : BDI - année : 2015)

Pour la Bretagne, développer la cyber renforce notre filière électronique en vertu d'un principe simple : sécuriser des flux de données n'a pas grand sens si les outils et les composants de ces derniers ne sont pas aussi sécurisés. C'est aussi tout l'enjeu de la sécurité de l'internet des objets (téléphones mobiles, automobile..). Pouvoir s'appuyer sur notre histoire industrielle dans l'électronique est une force de plus. L'électronique est stratégique pour notre région et nous avons là l'occasion de le démontrer. Dans ce nouveau contexte économique, nous ferons partie des territoires crédibles pour des entreprises souhaitant relocaliser des étapes de leur production de composants ou d'équipements électroniques. La cyber peut ainsi concrètement contribuer à développer de l'emploi de tous les niveaux, de services et industriels sur l'ensemble du territoire.

# 2. Le pôle d'excellence cyber opérationnel

## 2.1. Un pôle d'excellence cyber à l'action

Initié par le ministère de la Défense et par le Conseil régional, le Pôle d'excellence cyber s'est implanté naturellement en Bretagne. Avec une portée nationale et un objectif de rayonnement international, il se concentre autour des acteurs du ministère basés en Bretagne. Reconnus de longue date dans le domaine de la cyberdéfense, ceux-ci s'appuient sur le tissu académique et industriel régional, particulièrement dense en matière de cybersécurité et de numérique, mais aussi sur des partenaires nationaux ou d'autres territoires.

Le pôle d'excellence cyber est une des déclinaisons opérationnelles du Pacte Défense Cyber présenté par le Ministre de la Défense en février 2014. Ce pôle a pour vocation de mobiliser des compétences, ainsi qu'une expertise opérationnelle et technique de pointe. Il constituera ainsi un atout non seulement pour la supériorité opérationnelle de nos forces, mais aussi pour le dynamisme et le développement économique de notre industrie et, au-delà, pour toute la communauté nationale de cyberdéfense.

Il s'est donné pour objectif initial de stimuler le développement de la recherche, de la formation et de l'innovation au profit du ministère de la défense et de la communauté nationale cyber.

Il se veut un outil pragmatique au service de trois grands enjeux :

- Disposer des compétences nécessaires pour répondre aux besoins de développement de la filière,
- Disposer d'une offre de recherche en adéquation avec les besoins du ministère et des industriels,
- Disposer de produits et de services de confiance.

## 2.2. Un pôle dont l'essor s'appuie sur le travail mené par BDI et Meito et l'ensemble de l'écosystème

### Bretagne Développement Innovation et la Meito

Les travaux en région autour de la notion de cyber sécurité avec les PME, ont démarré dès **2004**, notamment par un atelier de la MEITO sur la sécurité des objets connectés ; depuis, le sujet n'a cessé d'être considéré comme d'avenir et la connaissance fine des entreprises du territoire s'est enrichie au fil du temps. En **2012**, des ateliers autour de la sécurité dans le cloud se tenaient.

Avec le lancement du PEC en février **2014**, l'écosystème breton s'est donc emparé de cette opportunité avec l'ambition, très tôt, d'afficher l'objectif de faire de la Bretagne une « CYBER VALLEY » européenne. Une stratégie a été co-construite, très rapidement suivie par une feuille de route partagée entre tous les acteurs. BDI en tant que coordinateur en lien étroit avec la MEITO s'est attaché à accélérer la dynamique car de réelles perspectives de marché s'ouvraient aux entreprises bretonnes. Les tout premiers travaux ont consisté à cartographier les forces en présence sur le territoire, à visiter de nombreuses PME pour bien connaître leur savoir faire, produire des contenus à destination de l'écosystème, dont BCI, pour valoriser cette offre territoriale à l'international. Sur un marché en devenir, la connaissance « fine » des atouts bretons a été déterminante dans le soutien à l'installation du PEC. La première participation au FIC (Forum International de la Cybersécurité) à Lille en janvier 2015 a été une grande réussite, renouvelée en 2016. L'objectif de faire reconnaître en France et auprès d'acteurs internationaux les atouts de la Bretagne a été atteint.

Enfin, depuis 2014, la MEITO n'a eu de cesse d'être bien identifiée au niveau national par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) ce qui a conforté la Bretagne dans son ambition.

Reçu en préfecture le 20/10/2016
Affiché le
ID : 035-233500016-20161013-16_DGS_04-DE

En parallèle de ce travail, les autres acteurs de l'écosystème numérique se sont aussi emparés de la cyber, chacun dans ses compétences. Le pôle images et réseaux et B-COM en ont fait un de leurs axes de développement permettant de renforcer nos savoir-faire sur la sécurisation des réseaux notamment. La French-Tech Rennes-Saint Malo a aussi fait de la cybersécurité une de ses spécialisations reconnues et l'engagement de la French-Tech Brest+ dans les technologies financières offrira un champ d'action supplémentaire.

Le pôle d'excellence cyber peut aujourd'hui compter sur ces différents acteurs qui contribuent dans les différents groupes de travail et portent des projets.

## 2.3. De premiers accords structurant la filière

La richesse de ce cluster est de créer des habitudes de collaboration entre des acteurs militaires et civils, des acteurs publics et privés, des acteurs du monde de la formation, de la recherche et de l'entreprise, entre des PME et des grands groupes. Cette multidimensionnalité fait du pôle d'excellence cyber un objet unique en Europe.

Si le pôle ne s'est constitué juridiquement que le 12 juillet dernier en élisant son conseil d'administration[1] et en portant à sa présidence le groupe La Poste, il a néanmoins été le creuset de nombreux projets depuis février 2014. Dès son annonce, il s'est réuni de manière informelle et s'est organisé autour de trois groupes de travail portant sur la formation, la recherche et le développement économique.

En décembre 2014, il a été le lieu de signature d'un accord général de partenariat pour la recherche entre la Direction générale de l'armement, la Région Bretagne et quatre grands laboratoires de recherche dépendant de 11 universités, écoles d'ingénieurs et acteurs de la recherche permettant le partage d'une stratégie commune et le renforcement des moyens, notamment par une augmentation du nombre de thèses. Ce travail sur la recherche s'est aussi traduit par la création du Laboratoire de Haute Sécurité, fruit d'un partenariat entre l'INRIA et la DGA-MI.

En septembre 2015, les principaux leaders du secteur ont signé un accord d'engagement au sein du pôle d'excellence cyber renforçant son assise économique : Airbus D&S, Nokia, Bertin, Cap Gemini Sogeti, DCI, DCNS, EDF, La Poste, Orange, Sopra-Steria, Thales…

Autour du ministère de la Défense et de ce réseau dense d'entreprises, laboratoires et écoles, le Pôle d'excellence cyber a ainsi pris naissance au cœur de la Bretagne et continue à se développer avec les acteurs nationaux, à travers des accords de partenariat avec des grands groupes et des opérateurs d'importance vitale. A ce titre, l'annonce récente du groupe PSA de vouloir rejoindre le PEC, en lien avec l'annonce de l'investissement industriel et de l'attribution d'un nouveau véhicule à l'usine de Rennes La Janais, permettra d'ajouter la question de la mobilité et de la voiture connectée aux axes de travail.

## 2.4. Un pôle à la logique européenne et internationale

La Bretagne n'est pas la seule région à s'engager sur la cybersécurité. Notre stratégie est d'aller vite, de prendre toute notre place et de le faire dans une logique partenariale.

Ainsi, nous avons engagé un partenariat avec le centre OTAN de Talinn (Estonie), autre territoire cyber en Europe, nous sommes présents au niveau de l'Union Européenne et nous sommes ouverts aux partenariats avec d'autres régions françaises et européennes.

Par ailleurs, le PEC a aussi une volonté d'échanges avec d'autres régions, d'autres clusters comme Hexatrust ainsi qu'avec les grandes associations professionnelles du type Cigref (réseau des grandes entreprises sur le numérique) ou CDSE (club des directeurs sécurités des entreprises).

Si le pôle d'excellence cyber est bien basé en Bretagne, son positionnement est national et son rayonnement européen et international.

1 Ce dernier est composé de : Monsieur le Vice Amiral Arnaud Coustillière et Madame Marie-Noëlle Sclafer représentants le Ministère de la Défense ; Messieurs Loïg Chesnais-Girard, 1er Vice-président du Conseil régional, et Bernard Pouliquen, Vice-président, représentants la Région Bretagne ; Monsieur François Lavaste pour Airbus DS ; Monsieur Pierre Jeanne pour THALES ; Monsieur Frédéric Rémi pour Amossys ; Monsieur Jean Le Traon pour Institut Mines Télécom – Télécom Bretagne ; Monsieur David Alis pour l'Université de Rennes 1 ; Monsieur Stéphane Ubeda pour l'INRIA et Monsieur Philippe Verdier pour le groupe La Poste.

# 3. Les résultats concrets de 18 mois d'engagement

La Région agit directement sur la structuration et le soutien aux projets et aux acteurs de cette filière. Elle le fait dans une approche systémique entre ses politiques économiques, d'innovation, de formation et d'enseignement supérieur et de recherche. Et elle le fait en engageant des moyens financiers significatifs : sur la période 2014-2020, l'engagement sera de plus de 15 millions d'euros (cf. tableau de synthèse 2014-2016 ci-après). Et elle le fait en mobilisant l'ensemble de l'écosystème, en particulier Bretagne Développement Innovation et Bretagne Commerce International.

Budget régional consolidé sur la période 2014-2016 par politique :

| *En K€* | 2014 | 2015 | 2016 | TOTAL |
|---|---|---|---|---|
| Formation | 449 | 154 | 961 | 1564 |
| Enseignement supérieur et recherche | 275 | 840 | 1784 | 2899 |
| Économie | 713 | 1121 | 1101 | 2935 |
| Total | 1437 | 2115 | 3846 | 7398 |

## 3.1. Une attractivité européenne et internationale qui s'affirme

Le rayonnement européen et international du pôle d'excellence cyber et de la filière cyber bretonne est essentiel pour marquer solidement l'avance bretonne alors que d'autres territoires commencent à se positionner sans avoir autant de compétences.

Dès le début du PEC, plusieurs actions prolongeant l'action régionale ont été engagées : présence sur le Forum International de la Cybersécurité à Lille depuis deux ans, partenariat avec l'OTAN, collaboration avec la Commission Européenne, création de l'European Cyber Week pour ne citer que les plus structurantes.

### Le Forum International de la Cybersécurité

Le FIC est l'événement de référence en Europe sur la cyber. Tous les ans, il rassemble les principaux acteurs européens du domaine tant civils que militaires. Le Conseil régional apporte son soutien au PEC afin de disposer d'un plateau permettant d'accueillir une partie des acteurs du PEC et en particulier des PME. On peut d'ailleurs souligner que quatre entreprises bretonnes ont été lauréates du Label France Cybersecurity : Akerva, Gfi, Opale Security et Siepel. En 2017, ce sera la troisième année consécutive et la deuxième en partenariat avec le Ministère de la Défense qui intègre désormais son plateau à celui du PEC.

### L'Europe et l'OTAN

Les relations avec la Commission européenne ont été nouées dès 2014. L'un des aboutissements est la participation du PEC et du Conseil régional comme administrateurs au partenariat public privé que vient de lancer la Commission. Cette participation offre à notre territoire une visibilité unique, la Bretagne étant la seule région représentée à ce niveau. Son objectif est de renforcer les capacités industrielles et d'innovation dans le domaine de la cyber en Europe.

Dans le même temps, le PEC a engagé des échanges avec l'OTAN qui dispose d'un site cyber stratégique en Estonie à Tallinn. Ce partenariat se traduit par des échanges entre universitaires et la valorisation des savoir-faire des PME bretonnes auprès de l'OTAN.

### European Cyber Week

Visant un public de spécialistes de la cybersécurité (ingénieurs, responsables des systèmes d'information, chefs de projet, militaires, chercheurs, étudiants), d'institutionnels (élus, agents de développement économique…) ou d'interfaces avec les entreprises (pôles de compétitivité, clusters, réseaux européens…), l'European Cyber Week se tiendra pour la première fois à Rennes, du 21 au 25 novembre prochain.

Envoyé en préfecture le 20/10/2016
Reçu en préfecture le 20/10/2016
Affiché le
ID : 035-233500016-20161013-16_DGS_04-DE

Avec ses sept manifestations ciblées et une plénière, l'événement qui vise un rayonnement européen, et qui du reste répond à un appel à manifestation d'intérêt européen, offrira une diversité de formats : conférences, rendez-vous b2b avec des partenaires technologiques ou des investisseurs, rencontres entre régions européennes…

Les sept temps forts sont les suivants :

- **C&ESAR** : état des avancées technologiques en matière de cyber-défense et de cybersécurité – Thématique 2016 : l'Internet des objets
- **EIT Digital symposium** : faire du lien entre recherche et entreprises de la cybersécurité
- **Regional EC Event** : Peer learning entre régions européennes sur le développement de la cybersécurité en tant qu'activité économique
- **Convention ECW EEN** : matchmaking entre entreprises, entre entreprises et labo, entre entreprises et investisseurs, entre PME et grands groupes
- **Invest in cyber** : faciliter les levées de fonds des startups
- **Colloque REI** : état de l'art de la recherche en matière de sécurité des réseaux électriques intelligents
- **Challenge ECW** : Challenge de hacking entre étudiants

Les acteurs impliqués dans l'European Cyber Week sont le Conseil régional de Bretagne, le ministère de la Défense, la DGA Maîtrise de l'information, BDI, EIT Digital, Images & Réseaux, Rennes Atalante, INRIA, l'Université de Rennes 1, Telecom Bretagne, Meito et les entreprises participantes… L'événement est organisé avec le soutien de l'Union européenne.

### 3.2. Des réponses concrètes aux besoins de formation

La filière cyber offre un nombre croissant d'opportunités de carrière mais les entreprises et organismes publics et militaires rencontrent de réelles difficultés pour former leurs personnels aux métiers de la cyber et recruter de nouveaux personnels qualifiés. Pour éviter que l'insuffisance de personnels qualifiés ne constitue un frein au développement de la filière cyber, le Club formation du PEC s'est donné comme objectifs de créer de nouvelles formations et faire évoluer les formations existantes.

Les activités du club formation ont débuté par un recensement des formations en cyber proposées par les partenaires académiques du PEC et par un recensement des besoins des industriels. Le recensement des besoins fait clairement apparaître une pénurie de talents en cybersécurité. Cette pénurie concerne notamment des généralistes pluridisciplinaires de la sécurité de haut niveau et des compétences pointues sur des thématiques particulières de la cybersécurité.

Face à ces besoins, le recensement des formations à la cyber, effectué en 2014 et mis à jour en 2015, a permis de conclure que le nombre total de diplômés ayant reçu une formation à la cybersécurité en Bretagne s'élevait à un peu plus de 2000 personnes (en incluant les étudiants sensibilisés à la cyber). Un premier objectif a été de passer de 2000 à 2800 pour l'année 2015 (augmentation de 40%), puis de 2800 à 3500 pour l'année 2016 (augmentation de 25%).

L'objectif pour l'année 2015 a été atteint et l'on peut raisonnablement anticiper que l'objectif 2016 sera également réalisé.

Une vingtaine d'opérateurs de formation sont d'ores et déjà partenaires du pôle d'excellence cyber : Université européenne de Bretagne, Université de Rennes 1, Université de Rennes 2, Université de Bretagne Occidentale, Université de Bretagne Sud, Supélec, Télécom Bretagne, ENS Rennes, INSA Rennes, ENSIBS, ENSTA, ENSSAT, St Cyr, Ecole Navale, ETRS, École de formation des sous-officiers de l'armée de l'air à Rochefort, Sciences Po, CNAM, IUTs, Institut Mines-Télécom, et Centrale-Supélec.

Ces opérateurs couvrent l'ensemble de la chaîne de formation initiale, supérieure et continue :

- Formations universitaires de technicien (BAC+2/3) : DUT, licences pro ;
- Diplômes universitaires : DU ;
- Formations universitaires : master (bac+5) ;
- Formations d'ingénieur (bac+5) ;
- Formation continue longue : mastères spécialisés : MS (bac+6), certificats d'études spécialisées…
- Formation continue courte.

Les formations sont réparties en cinq catégories (« hygiène numérique », formation complémentaire au profit du personnel des SIC, formation à la cyber-sécurité des spécialistes des SI, formation d'experts techniques et de responsables sécurité de haut niveau, formation des généralistes de la conduite des opérations cyber et de la gestion des crises).

Envoyé en préfecture le 20/10/2016
Reçu en préfecture le 20/10/2016
Affiché le
ID : 035-233500016-20161013-16_DGS_04-DE

Un catalogue de l'offre de formation a été élaboré en 2014 et est remis à jour chaque année. Il recense l'ensemble des formations ouvertes sur le territoire.

Cependant, le nombre limité de formateurs qualifiés à l'enseignement de la cyber est un paramètre à prendre en compte pour décider de déployer de nouvelles formations. Le projet CyberEdu, initié par l'ANSSI et réalisé par un consortium composé de partenaires du PEC, a permis de développer des guides pédagogiques à destination des enseignants non experts en cybersécurité pour les aider à intégrer les concepts de la cyber dans leurs cours. Un groupe de travail a également analysé le besoin de plateformes comme outils d'entraînement et de sensibilisation aux risques cyber.

D'autres paramètres contraignants pour atteindre les objectifs du club formation sont la disponibilité des personnels pour se former en entreprise ainsi que les contraintes de localisation lorsque la formation est dispensée en présentiel. Pour répondre à ces différentes contraintes, un groupe de travail cyber e-learning a été créé au sein du club formation du PEC. Ce groupe de travail s'est donné comme objectif ambitieux de définir un projet complet de formation à la cyber à base de techniques de e-learning. Ce projet Cyber e-learning doit répondre aux besoins de compétences en Cybersécurité des entreprises et des organisations publiques de recruter des généralistes de la Cybersécurité, développer les compétences de leurs équipes techniques ou accompagner les reconversions internes vers les métiers de la cybersécurité. Le projet prend également en compte le besoin de sensibiliser le plus grand nombre possible de personnes aux risques liés à la cybersécurité, et aux opportunités professionnelles liées à ce domaine. Ce dernier point constitue un réel besoin qui est aujourd'hui mal pris en compte par les formations existantes.

Les actions concernent non seulement le renforcement de la cyber dans l'enseignement supérieur et l'offre de formation continue mais également son intégration dans les programmes d'enseignement secondaire. Pour cela, un groupe de travail a été créé pour définir un parcours d'excellence pour les filières STI2D. Ce groupe piloté par le Rectorat élabore en collaboration étroite avec les experts du club formation un programme de formation aux problèmes techniques ainsi qu'aux différents métiers de la cyber. Les Lycées et les IUTs de ST Malo, Lannion et Vannes, travaillent en étroite collaboration au maquettage de ce parcours d'excellence dans un continuum Bac -3/+3, pour aller jusqu'à la création de L3 Pro, sans doute en 2017.

Pour répondre aux exigences du Livre blanc sur la Défense et la sécurité nationale, la DGA Maîtrise de l'information poursuit le recrutement d'ingénieurs de très haut niveau, spécialisés dans l'analyse et la prévention des attaques informatiques. À terme, le site de Bruz comptera ainsi plus de 500 experts en 2019 "*cyber*" (contre 350 aujourd'hui en 2016 versus 150 en 2012). Plus largement, la montée en puissance de la DGA en matière de cyberdéfense se traduit par le renforcement de la recherche amont et un soutien accru aux PME et aux laboratoires de recherche qui interviennent dans ce domaine, avec le triplement du budget de R&T correspondant. La DGA participe activement à l'animation d'une filière d'excellence cyber tant sur le plan de la recherche, de la formation supérieure que sur celui du développement des entreprises françaises innovantes.

### 3.3. Des investissements dans la recherche appliquée

#### 3.3.1. Le soutien aux programmes de recherche et l'accord général de partenariat

Démarrée en 2015, cette action finance chaque année 20 thèses supplémentaires dans le domaine de la cyberdéfense et la cybersécurité. Ce sont ainsi 12 millions d'euros sur 6 ans qui sont investis sur l'écosystème de recherche régional permettant ainsi de doubler le nombre de thèses cyber financées chaque année. Les 12 millions d'euros sont apportés pour moitié par la DGA et l'autre moitié par le Conseil régional de Bretagne.

Cinq Unités Mixtes de Recherche (UMR) sont principalement concernées : IRISA, LabSTICC, IETR, IRMAR, IODE ; s'y ajoutent les laboratoires de la défense : IRENAV, ENSTA, CREC… et d'autres laboratoires universitaires qui sont aussi concernés. Ce sont environ 200 chercheurs qui travaillent sur des thèmes cyber en Bretagne.

L'accord général de partenariat signé fin 2014 entre la DGA, la Région, le CNRS, l'INRIA et 9 universités et écoles d'ingénieurs définit un cadre de travail sur le long terme, avec une vision stratégique commune en matière de recherche et de valorisation de la recherche en lien avec le tissu industriel régional. Entre autres actions, il permet notamment le financement des thèses supplémentaires évoquées plus haut, mais aussi d'attirer de nouveaux talents dans les équipes existantes voire de créer de nouvelles équipes avec le soutien des grands organismes comme l'INRIA, le CNRS mais aussi avec le soutien des écoles et de nos universités qui ouvrent des postes sur cette thématique.

#### 3.3.2. Laboratoire de Haute Sécurité (LHS)

Le Laboratoire de Haute Sécurité (LHS) est un laboratoire commun entre la Région Bretagne, la DGA, INRIA et CentraleSupelec, né de la volonté de renforcer la recherche en Cyber sécurité en Bretagne au sein du Club Recherche du Pôle d'Excellence Cyber (PEC). Il s'inscrit dans le cadre du Contrat de Plan Etat-Région (CPER). Il a vocation à un rayonnement européen voire international à travers la chaire CentraleSupélec et la création d'une équipe projet INRIA (EPI).

Le LHS-PEC a deux objectifs : le premier est de favoriser le développement de la recherche en cyber sécurité pour des thèmes jugés importants mais peu couverts par des équipes de recherche bretonnes, le second objectif est de favoriser le transfert technologique vers l'industrie lorsque les sujets le nécessitent.

### 3.3.3 Les chaires industrielles

La stratégie menée est de développer la recherche applicative et donc de soutenir les collaborations entre industriels et académiques. A ce titre, nous soutenons la création de chaires industrielles qui permettent un travail collaboratif en lien direct avec les besoins des entreprises. Ces deux dernières années, quatre chaires ont vu le jour.

#### La Chaire cybersécurité des infrastructures critiques

Lancée le 25 janvier 2016 au Forum International de Lille, la Chaire Cybersécurité de l'Institut Mines-Télécom répond aux enjeux de cybersécurité des infrastructures critiques (réseaux d'énergie, processus industriels, usines de production d'eau, systèmes financiers, …).

La chaire est portée par Télécom Bretagne, en collaboration avec Télécom ParisTech et Télécom SudParis, la Région Bretagne, dans le cadre du Pôle d'Excellence Cyber, et désormais 8 entreprises : Airbus Defence and Space, Amossys, BNP Paribas, EDF, La Poste, Nokia, Orange et le groupe Société Générale.

#### La Chaire sur la cybersécurité appliquée à l'analyse de la menace et des vulnérabilités des systèmes militaires et civils

Cette chaire portée par Centrale Supelec est l'une des composantes du Laboratoire de Haute Sécurité (LHS) du Pôle d'Excellence.
En partenariat avec la DGA, la Région Bretagne, INRIA, CNRS et Rennes, la chaire doit permettre de dégager un ensemble de techniques permettant de détecter des comportements non prévus d'un logiciel et d'exploiter ces comportements (mise en défaut de la confidentialité, de l'intégrité ou de la disponibilité des données ou des services).

#### La «chaire de cyberdéfense des systèmes navals »

École Navale, TELECOM Bretagne, DCNS et Thales ont en 2015, créé cette chaire afin de concrétiser une tradition d'échanges scientifiques et de collaborations dans les domaines des systèmes navals, des systèmes d'informations et de télécommunications. Elle a vocation à renforcer la formation des élèves officiers de la marine nationale et élargir les recherches en cyber sécurité et cyber défense au milieu marin. Elle est soutenue par la région Bretagne.
Cette chaire cyber défense constitue une plateforme de diffusion et de valorisation des résultats des recherches et des projets développés, tant sur le plan national qu'international, au profit des partenaires.

#### La Chaire de Cyberdéfense et Cybersécurité Saint-Cyr, Sogeti, Thales

Inaugurée avant la création du Pôle d'Excellence Cyber, la chaire Cyberdéfense et cybersécurité Saint-Cyr, Sogeti, Thales a pour ambition de mieux anticiper les futures cyber menaces en associant les compétences des mondes militaire et civil. Au service du ministère de la Défense, et à vocation interarmées, son objectif est de développer une réflexion scientifique de premier plan sur les dimensions stratégiques du cyberespace, à l'aide d'un programme de recherche international fédérant acteurs publics et privés.
Le renforcement de la recherche partenariale entre les mondes académique et industriel, civil et militaire doit logiquement conduire à des avancées applicatives et préindustrielles. Pour faciliter les démarches, l'État et la région ont défini, dans le cadre du CPER un programme d'investissement de plus de 6 millions d'euros afin de déployer des plateformes sur l'ensemble des sites bretons et mobilisable, pour la formation et la recherche appliquée aux cas d'usage.

### 3.3.4. CyberSSI

En complément de ces différentes actions (LHS, Chaires industrielles, projets de recherche), se met en place le projet CyberSSI dans le cadre du CPER 2014-2020. Doté de 6,3 millions d'euros, il a pour objectif de déployer des plateformes de recherche, d'expérimentation, d'entraînement et de test des usages entre 2014 et 2020.

Reçu en préfecture le 20/10/2016
Affiché le
ID : 035-233500016-20161013-16_DGS_04-DE

Ce programme se décline en plusieurs projets concernant la cryptographie, la conception d'algorythme, les méthodes d'analyses, la protection des systèmes industriels et la détection des défaillances des systèmes physiques. Ils seront répartis sur les sites de Brest, Lannion, Vannes, Lorient et Rennes.

### 3.4. La Bretagne aux cotés du développement de ses entreprises et mobilisée pour accueillir de nouveaux acteurs

Les formidables applications que permet le numérique ne seront durables que si elles recueillent la confiance de leurs utilisateurs. Pour construire une société capable de faire face à des risques croissants, à des acteurs agiles aux techniques d'attaques de plus en plus sophistiquées, il faut systématiquement intégrer les composantes de la sécurité numérique.

Au-delà du confort de la vie quotidienne et de la disponibilité de ces applications numériques devenue parties intégrantes de nos vies, l'enjeu est économique. Il est désormais vital pour préserver les données et compétences, savoir-faire et avantages concurrentiels, en un mot la compétitivité et donc l'emploi, que les entreprises se protègent des attaques informatiques. L'impératif de cybersécurité concerne le parc informatique dans son ensemble, depuis le développement de la bureautique jusqu'à la conception du système industriel intégré à la chaîne production.

Nous constatons que de plus en plus d'entreprises, comme dans l'électronique embarquée, commencent à valoriser leur offre en mettant en avant la cyber sécurisation de leurs produits. C'est un phénomène nouveau, signal faible mais annonciateur d'une évolution au sein des entreprises, qu'elles soient « offreurs » de solution ou « intégrateur » de solutions cyber.

Le marché de la cyber va donc offrir des perspectives de développement importantes pour les entreprises bretonnes du secteur. Notre volonté est d'être à leurs cotés pour les aider à se positionner sur ce marché et à se développer.

Les premiers résultats sont d'ores et déjà perceptibles. Les différents investissements annoncés au sein de la DGA-MI ou chez des opérateurs privés comme Sopra, Orange ou Nokia, se traduisent déjà par la création de plusieurs centaines d'emplois. D'autres projets sont par ailleurs en cours d'étude.

Dans le cas de Nokia, notre spécialisation cyber a joué un rôle important dans les décisions de renforcement du site de Lannion suite au rachat d'Alcatel-Lucent. Le groupe a décidé d'investir dans la cyber à Lannion en lien avec son centre principal de R&D en région parisienne. Rappelons que Lannion et Paris sont désormais les seules implantations en France du groupe Nokia.

5 enjeux ont été identifiés au sein du Pole d'excellence Cyber pour permettre le développement d'une filière industrielle en lien avec les initiatives prises au niveau de la formation et de la recherche ;

- Enjeu 1 : favoriser les interactions entre les grands donneurs d'ordre de la cybersécurité et l'écosystème du PEC ;
- Enjeu 2 : favoriser la création et l'intégration dans des solutions globales de briques technologiques par domaine fonctionnel au sein du PEC notamment à l'aide d'intégrateurs / assembliers ;
- Enjeu 3 : aider au développement des entreprises du PEC, notamment les PME avec un focus sur le développement à l'export ;
- Enjeu 4 : faire monter les entreprises en compétence à travers les cas d'usage et la sensibilisation ;
- Enjeu 5 : assurer la visibilité, la promotion et l'attractivité du Pôle d'Excellence Cyber sur le territoire français et à l'international.

Pour ce qui est du dernier enjeu, les principales actions sont décrites dans le point 3.1.

Les enjeux présentés viennent s'inscrire pleinement dans la SRDEII régionale. Ainsi, le Conseil régional mobilise ses dispositifs traditionnels, développe des dispositifs ciblés et intègre la cyber comme priorité dans les nouveaux dispositifs. D'ailleurs, outre les actions spécifiques, il est aussi important d'intégrer la cyber comme une composante transversale des politiques régionales et des actions portées à destination des entreprises. Des filières majeures pour la région, comme l'agro-alimentaire ou l'automobile, qui semblent de prime abord plus éloignées que des filières traditionnelles, sont tout autant impactées par les enjeux de cyber, dès lors que l'on parlera santé ou mobilité. C'est bien d'une manière globale et intégrée qu'il faut traiter ces dimensions.

#### 3.4.1. L'appel à Projets Cyber PME pour soutenir l'innovation et la collaboration

Le premier appel à projets a été lancé fin 2014 et a permis de soutenir 13 PME en 2015 dans le développement de nouvelles solutions. Il était doté de 600 k€ et visait particulièrement la mise au point et l'expérimentation de solutions de confiance ou de briques technologiques cyber destinées à la protection et à la défense des infrastructures, réseaux et systèmes d'information civils.

Cet appel à projet s'est appuyé sur l'expertise de la Meito en lien avec le Pôle d'Excellence Cyber et la DGA-MI.

Face au succès de ce dispositif, la Région a annoncé sa reconduction pour 2016 avec, cette fois-ci, la volonté d'accompagner les entreprises dans l'expérimentation de nouvelles solutions chez un client. L'objectif opérationnel de ce dispositif est de permettre aux porteurs de projets d'expérimenter leurs solutions avec un client pilote. Sont visées les entreprises dont le cœur d'activité est la cybersécurité ainsi que les entreprises de toutes les filières bretonnes qui souhaitent monter en compétences par l'intégration de briques technologiques cyber.
Ce nouvel appel à projets est doté de 800 K€ et les résultats seront annoncés dans le courant du mois de novembre.

### 3.4.2. Invest in Cyber, pour faire rencontrer entreprises et investisseurs

Si l'appel à projets est ciblé sur le soutien à la réalisation de nouvelles offres de produits et de services, il est apparu qu'il fallait également travailler avec les acteurs sur la question des fonds propres. Plus une capitalisation est solide, plus l'entreprise sera en capacité d'assurer sa phase de recherche et développement, et par ailleurs de se donner les conditions de son développement.

Deux outils ont été mis en œuvre sur cette problématique:

- une convention d'affaires pour que se rencontrent entrepreneurs et investisseurs : Invest in Cyber

- et l'inscription des entreprises cyber dans les cibles visées par Breizh-Up, le fonds de co-investissement du Conseil régional.

Invest in Cyber est la seule convention d'affaires française dédiée aux investissements de l'industrie de la cybersécurité. La première édition s'est tenue en 2015 sous l'impulsion du Pôle d'Excellence Cyber et du Pôle de compétitivité Images & Réseaux, ainsi que de l'ensemble des partenaires. L'objectif est de **faire se rencontrer investisseurs, grands donneurs d'ordres et acteurs innovants de la cybersécurité.**

Organisé sur 1 jour et demi pendant les Opportunités Digitales Rennaises, Invest in Cyber a eu pour ambition de **centraliser les opportunités stratégiques d'investissement de l'industrie de la cybersécurité** en facilitant la rencontre d'investisseurs avec les experts nationaux du secteur (entrepreneurs, experts de l'industrie et analystes).

Les sociétés émergentes à la recherche de fonds ont pu ainsi se confronter à des investisseurs nationaux et des partenaires potentiels afin d'accélérer le développement de leur entreprise.

Invest in Cyber a accueilli des conférenciers reconnus, travaillant pour des entreprises leaders du secteur, qui ont dévoilé aux participants des données de premier ordre sur le marché et ont pu échanger sur les enjeux de la cybersécurité.

Co-organisé par le Pôle d'Excellence cyber, le Pôle de compétitivité Images & Réseaux, Bretagne Développement Innovation, la MEITO, Télécom Bretagne, la CCI de Rennes, BPI France, Rennes Atalante, l'Irisa et l'INRIA avec le soutien de la French Tech Rennes, de Rennes Métropole et de l'ensemble des technopoles bretonnes et ligériennes, l'évènement s'est déroulé dans les locaux de l'INRIA Rennes les 14 et 15 octobre 2015.

Face au succès de ce premier événement, un second Invest in Cyber se tiendra lors de l'European Cyber Week fin novembre.

### 3.4.3. Breizh-Up et Performance PME Bretagne : des fonds propres aux ressources humaines, deux exemples de dispositifs régionaux qui appuient des PME cyber

Le fonds Breizh-Up n'a pas été spécifiquement créé pour investir dans des entreprises cyber mais la cyber fait partie de ses priorités. Il est ainsi probable qu'au cours des années qui viennent, plusieurs start-ups évoluant sur le marché de la sécurité numérique bénéficient du fonds. Par ailleurs, dans le cadre de sa politique de labellisation de fonds, plusieurs partenariats sont en cours avec des fonds intéressés par ce marché.

Le dispositif Performance PME Bretagne, lancé le 9 septembre dernier dans les locaux de Multiplats à Vannes, et qui vise à accompagner de façon intensive quelques entreprises à fort potentiel par du conseil extérieur, n'est pas exclusivement fléché sur les entreprises cyber mais sur des entreprises qui ont des potentiels de croissance forte. Parmi les dix entreprises sélectionnées pour ce programme, quatre sont des entreprises du domaine de la cyber.

Les résultats après moins de trois années de mobilisation en Bretagne sont très encourageants. Notre effort va donc se poursuivre et s'amplifier. La poursuite de notre présence au FIC et l'European Cyber Week sont confirmés. L'appel à projets PME poursuivra son adaptation pour répondre au plus proche des besoins des PME. Sur l'attractivité, nous conforterons le travail de marketing territorial afin de jouer sur tous les leviers et être ainsi capable de créer les conditions de développement des entreprises bretonnes et d'accueil des entreprises étrangères.

### 3.4.4. Accompagner le développement des entreprises à l'international et créer les conditions d'accueil des entreprises étrangères

Envoyé en préfecture le 20/10/2016
Reçu en préfecture le 20/10/2016
Affiché le
ID : 035-233500016-20161013-16_DGS_04-DE

Pour permettre le développement à l'export des entreprises bretonnes, des actions spécifiques sont identifiées ou engagées, portées par Bretagne Commerce International (BCI), BDI, le PEC ou encore d'autres partenaires régionaux. Il s'agit en particulier d'identifier les principaux canaux d'appels d'offres internationaux, identifier les pays à forte demande et/ou cible, organiser pour les entreprises des missions dédiées vers ces pays, participer aux salons internationaux ou bien encore assurer le lien avec les initiatives régaliennes à l'international, notamment dans le secteur de la défense.

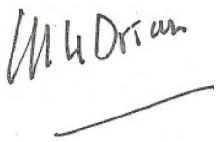
Au titre du partenariat engagé avec la défense, on peut souligner l'accord entre la DGA-MI et BCI dans le cadre de "BCInside", convention signée en novembre 2015. Une vingtaine de PME bretonnes de la cybersécurité sont accompagnées par un conseiller de BCI 1 à 2 journées par mois pour établir un diagnostic des forces et faiblesses de l'entreprise à l'international et proposer un plan d'action mobilisant les différents leviers proposés par les acteurs régionaux (BCI, Conseil régional, BPI France, Business France..). Les acteurs œuvrant sur l'international, organisés autour du Plan Régional d'Internationalisation des Entreprises (PRIE), vont d'ailleurs consacrer leurs prochains travaux à l'automne à une réunion Cyber afin d'échanger et de renforcer la coordination entre acteurs du développement à l'international.

Les acteurs régionaux, avec en tête de pont BCI, assurent également la phase de prospection et d'accompagnement d'entreprises étrangères du secteur. Il s'agit d'un travail qui se fait dans la durée, mais les exemples récents d'implantation en région constituent une véritable vitrine qui permettra de valoriser tous les atouts bretons dans le domaine de la cyber et faire de la Bretagne une région à la pointe au niveau national et international.

**En conclusion,** la finalité de la glaz-économie est de prendre des positions stratégiques qui feront de la Bretagne un acteur indispensable à l'économie mondiale de demain. C'est ce qui guide notre action pour la cybersécurité. Mais c'est la même logique sur les smart-grid, sur les nouveaux matériaux, sur le maritime, l'alimentation, le numérique et l'aéronautique. Sur la cyber, notre positionnement est désormais incontestable et sera source de création massive d'emplois tout en contribuant à renforcer l'image d'une région au sommet de l'innovation.

**Je vous propose de prendre acte de cette communication.**

Le Président



Jean-Yves Le Drian