Commission « Développement économique et recherche »
Rapporteur : M. Thierry LEMETAYER

Avis du CESER sur le dossier du Conseil régional « La Bretagne, cyber-valley européenne »

1. Rappel des propositions du Président du Conseil régional

Le Conseil régional fait de la cybersécurité l'une des priorités de sa stratégie de développement économique, d'innovation et d'internationalisation, choix par ailleurs confirmé dans le Pacte d'avenir pour la Bretagne.

La cybersécurité est un élément clé de la révolution numérique en cours, tant pour les réseaux, que pour le stockage des données ou encore le développement des objets connectés. Se positionner sur la cybersécurité a des impacts sur tout l'écosystème numérique. L'ensemble du territoire breton est concerné par la présence d'écoles, d'universités et d'entreprises ; cette spécialisation sur la cybersécurité apporte à la filière numérique, deuxième de France, un nouvel atout pour rayonner et se développer.

L'ambition du Conseil régional est de faire de la Bretagne le territoire leader en Europe, de voir se développer massivement cette nouvelle filière sur le territoire, en s'appuyant sur ses savoir-faire et la structuration qu'offre le Pôle d'excellence cyber et la mobilisation de l'écosystème numérique.

2. Observations du CESER sur les propositions du Président du Conseil régional

Observations sur la partie 1 : « Pourquoi un positionnement breton sur la cyber » ?

Dans le cadre de son étude sur la transformation numérique des entreprises (qui sera présentée lors de la session de décembre 2016), le CESER a pu constater à quel point l'introduction à grande échelle du numérique dans notre quotidien génère des problèmes massifs de sécurité. Le marché de la cybersécurité, qui sera au cœur de la révolution numérique, est donc appelé à se développer. Or, la Bretagne dispose d'un savoir-faire indéniable au travers de différents acteurs militaires (Direction générale de l'armement - DGA, Écoles militaires) et civils (grandes entreprises, PME, enseignement supérieur et recherche). 2 500 emplois directs seraient d'ores et déjà concernés dans la région par le développement de la cybersécurité. Dans ces conditions, le CESER ne peut que soutenir la stratégie qui vise à structurer une filière cybersécurité sur le territoire.

Observations sur la partie 2 : « Le pôle d'excellence cyber opérationnel »

Ancrer la cybersécurité durablement sur le territoire nécessite de générer, d'attirer et surtout de garder les entreprises et les talents. A l'heure où il existe une pénurie de main d'œuvre qualifiée, il semble opportun de mettre l'accent sur la formation, tant par son volume, à savoir le nombre de personnes formées chaque année, que par sa qualité, à savoir ce qui est enseigné. Sur ce dernier point, l'expertise des enseignants, et donc la recherche, sont primordiales. Il convient aussi d'offrir un environnement permettant à l'ensemble des acteurs de l'écosystème, entreprises, formations, armées, de se rencontrer, de travailler ensemble et de trouver des financements.

Dans ce contexte, le CESER note avec satisfaction la création du Pôle d'excellence cybersécurité (PEC), qui permet de regrouper une centaine d'acteurs et de favoriser les échanges. Il se réjouit en particulier que ce pôle prenne en compte les trois enjeux majeurs que sont la formation, la recherche et l'innovation.

Observations sur la partie 3 : « Les résultats concrets de 18 mois d'engagement »

L'accent est bien mis sur la formation, ce dont le CESER se félicite. Ainsi, le Club formation du PEC s'est donné comme objectifs d'en créer de nouvelles et de faire évoluer les formations existantes. Une vingtaine d'opérateurs sont d'ores et déjà partenaires du Pôle. Ils couvrent l'ensemble de la chaîne de formation initiale et continue. Pour le CESER, il est important que ces échanges ne portent pas uniquement sur les formations les plus pointues mais conduisent bien à intégrer la cybersécurité dans des formations de tous niveaux, s'adressant à des publics variés. La mise en place d'un parcours en lien avec la cybersécurité dès le lycée pour les filières STI2D (Sciences et technologie de l'industrie et du développement durable) est un premier pas en ce sens. Le CESER souhaite que la réflexion concernant ce « parcours d'excellence » soit poussée plus loin pour aller vers des contenus, peut-être plus modestes mais pouvant bénéficier à davantage d'élèves. Il encourage le Conseil régional et ses partenaires à prolonger la réflexion dans cette voie. Par ailleurs, il souhaiterait connaître les établissements et les spécialités STI2D qui seront concernés par l'expérimentation.

Concernant la recherche appliquée, le CESER constate les efforts importants consentis notamment par le Conseil régional : chaque année, 20 thèses supplémentaires sont financées dans le domaine de la cyberdéfense et la cybersécurité, ce qui constitue un doublement de leur nombre. Il est prévu à cet effet un budget de 12 M€ sur 6 ans apportés pour moitié par la DGA et pour moitié par le Conseil régional. Le CESER souhaiterait savoir s'il s'agit de moyens supplémentaires de la part de ce dernier, venant s'ajouter aux moyens déjà alloués à la formation et la recherche, ou s'il s'agit d'un redéploiement des moyens. Par ailleurs, s'agissant de ces thèses, il espère que certaines seront engagées dans le champ des sciences humaines. En effet, les questions éthiques, juridiques et sociologiques font partie de la culture « cyber » que l'on souhaite produire au sein de l'enseignement supérieur et recherche.

La création du Laboratoire de haute sécurité commun entre la Région Bretagne, la DGA, l'Institut national de recherche en informatique et en automatique (INRIA) et Centrale Supelec s'inscrit dans le cadre du Contrat de Plan État-Région. Il a vocation à atteindre un rayonnement européen à travers la chaire Centrale Supélec et la création d'une équipe projet INRIA. La création de quatre chaires industrielles ces deux dernières années permet un travail collaboratif entre industriels et académiques en lien direct avec les besoins des entreprises.

Par ailleurs, le marché de la cybersécurité va offrir des perspectives de développement importantes pour les entreprises bretonnes de la filière numérique. Le CESER note la volonté du Conseil régional d'être à leurs côtés pour les aider à se positionner sur ce marché et à se développer. Il relève aussi que le PEC a identifié cinq enjeux pour permettre le développement d'une filière industrielle :

- favoriser les interactions entre les acteurs. Le CESER rappelle que la nécessité de renforcer les liens entre les donneurs d'ordres de la filière numérique et les PME du territoire a été diagnostiquée depuis longtemps (voir par exemple le rapport publié par l'Agence économique de Bretagne en 2009), mais que des difficultés persistent. Il espère donc que la mise en place du PEC contribuera à avancer dans cette voie ;
- favoriser la création et l'intégration dans des solutions globales de briques technologiques ;
- aider au développement des entreprises du PEC, notamment les PME avec un focus sur le développement à l'export ;
- faire monter les entreprises en compétence. Le volet sensibilisation apparaît particulièrement important à ce titre, en cohérence avec ce qui est dit plus haut, notamment lorsque le Conseil régional explique que l'intégration de la cybersécurité est un moyen de renforcer d'autres filières, à commencer par la filière électronique ;
- assurer la visibilité, la promotion et l'attractivité du PEC en France et à l'international.

Ces priorités s'inscrivent pleinement dans la SRDEII. Le CESER relève également qu'ils couvrent assez largement les enjeux de développement de la filière, même si le volet 4 peut sembler moins avancé à la lecture du bordereau. Pour le CESER, il est important de s'appuyer pleinement sur chacun de ces piliers, afin que l'excellence de la recherche et de l'enseignement supérieur, ainsi que le soutien aux entreprises de la filière cybersécurité aillent de pair avec une exemplarité dans la prise en compte des enjeux de la cybersécurité par toutes les entreprises. Ce point appelle un accompagnement des entreprises du territoire, qui doit mobiliser de nombreux acteurs, au-delà des membres du PEC.

Cette dynamique se traduit par exemple par plusieurs centaines d'emplois créés dans de grandes entreprises, par le soutien à 13 PME en 2015 via un appel à projets reconduit en 2016, par la convention d'affaires « Invest in Cyber », ou encore par l'inscription des entreprises cyber dans les cibles du fonds Breizh-Up. Pour le CESER, ces différentes mesures sont encourageantes quant à la capacité du PEC à transformer une excellence reconnue dans le domaine militaire et sur le plan de la recherche en perspectives de développement pour les PME et en création d'emplois sur le territoire.

Enfin, le CESER salue les actions visant à promouvoir le savoir-faire des acteurs implantés en Bretagne à l'international.

En conclusion, le CESER se réjouit de la mise en place du PEC, qui semble être un moyen pertinent pour favoriser la convergence des acteurs et ainsi sécuriser l'implantation d'une filière cybersécurité en Bretagne. L'objectif doit bien être la création massive d'emplois durables et de qualité, ancrés sur le territoire. Pour le CESER, cette stratégie de filière, comme toutes les stratégies liées aux filières numériques, doit également être mise au service des autres filières du territoire. Au vu de cette feuille de route, les résultats sont encourageants et devront être renforcés, car la filière va devoir faire face à une concurrence très dynamique. Il semblerait également opportun d'accélérer la sensibilisation et l'accompagnement des acteurs économiques implantés en Bretagne, car la prise en compte des enjeux de la cybersécurité reste un enjeu majeur pour tous.

Vote sur l'Avis du CESER de Bretagne
La Bretagne cyber valley européenne

Nombre de votants : 100

Ont voté pour l'avis du CESER : 98

Valérie FRIBOLLE (CCIR), René LE PAPE (CCIR), Jean-François LE TALLEC (CCIR), Dominique LECOMTE (CCIR), Evelyne LUCAS (CCIR), Emmanuel THAUNIER (CCIR), Edwige KERBORIOU (CRAB), Laurent KERLIR (CRAB), Nathalie MARCHAND (CRAB), Emmanuelle TOURILLON (CRMA), Patrick CARE (UE-MEDEF), Christine LE GAL (UE-MEDEF), Jean-Bernard SOLLIEC (UE-MEDEF), Lucien TRAON (CGPME), Didier LUCAS (Par accord FRSEA-CRJA), Franck PELLERIN (Par accord FRSEA-CRJA), Henri DAUCE (Confédération paysanne de l'Ouest), Pierre LEC'HVIEN (Coordination rurale), Thierry MERRET (Par accord CERAFEL-UGPVB-CIL), Jean-Yves LABBE (Bretagne pôle naval), Gérald HUSSENOT (CRPMEM), Olivier LE NEZET (CRPMEM), Hervé JENOT (Par accord Comités régionaux de la conchyliculture de Bretagne nord et Bretagne sud), Philippe LE ROUX (UNAPL), Sylvère QUILLEROU (CNPL), Jean-Philippe DUPONT (Par accord SNCF-RTF-EDF-ERDF-RTE-GDF-SUEZ-La Poste), Martial WESLY (Comité régional de la fédération bancaire française), Françoise BOUJARD (CFDT), Michel CARADEC (CFDT), Norbert HELLUY (CFDT), Marie-Madeleine HINAULT (CFDT), Patrick JAGAILLE (CFDT), Chantal JOUNEAUX (CFDT), Véronique LAUTREDOU (CFDT), Véronique LE FAUCHEUR (CFDT), Thierry LEMETAYER (CFDT), Catherine LONEUX (CFDT), Gilles POUPARD (CFDT), David RIOU (CFDT), Marie-Pierre SINOU (CFDT), Joël SIRY (CFDT), Jacques UGUEN (CFDT), Olivier CAPY (CGT), Jean-Edmond COATRIEUX (CGT), Claudine CORNIL (CGT), Stéphane CREACH (CGT), Danièle KERJAN (CGT), Françoise LE LOARER (CGT), Thierry LENEVEU (CGT), Jean-Luc PELTIER (CGT), Nadine SAOUTI (CGT), Marie-France THOMAS (CGT), Gaëlle URVOAS (CGT), Joël JOSSELIN (FO), Annie KERHAIGNON (FO), Eric LE COURTOIS (FO), Fabrice LERESTIF (FO), Pierrick SIMON (FO), Annie COTTIER (CFTC), Pierre EUZENES (CFTC), Catherine TANVET (CFE-CGC), Bertrand LE DOEUFF (UNSA), Jean-Marc CLERY (FSU), Annie GUILLERME (URCIDFF), Nadia LAPORTE (FCPE), Guylaine ROBERT (APEL), Isabelle TOXE (Par accord UNAPEI-CREAI), Marie-Martine LIPS (CRESS), Joseph-Bernard ALLOUARD (Mouvement Agir Tous pour la Dignité), Jacqueline PALIN (CROS), Jean KERHOAS (Nautisme en Bretagne), François HERVIEUX (Par accord CLCV-UFC-Que choisir), Michel MORVANT (Union régionale des PACT-ARIM et Habitat et développement en Bretagne), Hervé LATIMIER (Kevre Breizh), Patrice RABINE (Théâtre de Folle Pensée), Alain LE FUR (UNAT), Carole LE BECHEC (Réseau Cohérence), Jean-Emile GOMBERT (Universités de Bretagne), Pascal OLIVARD (Universités de Bretagne), Alain CHARRAUD (Conférence des directeurs des Grandes écoles de Bretagne), Anne-Claude LEFEBVRE (Par accord CRITT-Centres techniques de Bretagne), Jean LE TRAON (IRT B-COM), Antoine DOSDAT (IFREMER), Patrick HERPIN (INRA), Yann-Hervé DE ROECK (France énergies marines), Bertrand LAOT (Union régionale de la Mutualité française), Didier GILBERT (Par accord CPAM-CAF-RSI-MSA), Bernard GAILLARD (CRSA), Zoé HERITAGE (IREPS), Léa MORVAN (CRIJ), Yannick HERVE (CRAJEP), Marie-Pascale DELEUME (Eau et rivières de Bretagne), Jean-Yves PIRIOU (Eau et rivières de Bretagne), Michel CLECH (REEB), Jean-Yves MOELO (Personnalité qualifiée environnement et développement durable), Chantal BEVILLON (Personnalité qualifiée), Christian COUILLEAU (Personnalité qualifiée), Anne LE MENN (Personnalité qualifiée)

Ont voté contre l'avis du CESER : 0

Se sont abstenus : 2

Serge LE QUEAU (SOLIDAIRES), Viviane SERRANO (SOLIDAIRES)

Adopté à l'unanimité

Intervention de M. Jean-Bernard SOLLIEC
Union des entreprises (UE) – MEDEF Bretagne

L'évolution des technologies et notamment de ce que l'on appelle globalement le « numérique » ouvre des perspectives de développement économique majeur tout en faisant peser des menaces nouvelles, importantes, sur les particuliers, les entreprises, les administrations, les Etats.
Il est capital de se mobiliser collectivement pour apporter des réponses fortes, techniques, crédibles, à la hauteur des enjeux et des risques.

Cette mobilisation est essentielle pour préserver ce que nous avons réussi à construire collectivement : des institutions démocratiques garantissant le respect des droits fondamentaux et de l'état de droit, menacés, comme nous l'avons vu depuis au moins deux ans par des actes d'une extrême cruauté et qui peuvent revêtir demain un caractère plus « numérique ».

Mais c'est aussi, un marché en plein développement sur lequel la demande, les besoins, par nature très évolutifs, génèreront en Bretagne, si nous sommes compétitifs, une activité en forte progression. Il est donc nécessaire de créer les conditions d'une réponse pertinente, puissante, émanant, d'une part, des administrations concernées, et d'autre part, des entreprises, très nombreuses en Bretagne, qui collaborent activement avec nos établissements d'enseignement supérieur et de recherche, comme notamment, l'école d'ingénieurs de Vannes, l'ENSIBS, qui a ouvert récemment une section spécialisée en cyber sécurité, dont la contribution sera décisive dans notre capacité à capter une demande en pleine croissance.

Ce positionnement stratégique de la Bretagne sur cette question nous semble fort opportun et nous mobiliserons tous les outils à notre disposition pour y apporter notre concours plein et entier, certes pour notre développement économique et social mais aussi pour préserver nos valeurs, notre souveraineté, notre liberté.

Intervention de M. Stéphane CREACH
Comité régional CGT de Bretagne

Comme le souligne l'avis du CESER, la CGT partage cette notion que la question de la cybersécurité est nécessairement en lien avec l'ensemble du domaine du numérique qui effectivement nécessite une prise en compte des problématiques liés à la sécurisation des systèmes.

Cette filière est bien prise sous l'angle d'une activité complémentaire qui s'inscrit dans une logique de combinaison.

La cybersécurité présente des enjeux économiques, sociaux, stratégiques et politiques qui vont donc bien au-delà de la seule sécurité des systèmes d'informations.

La cybersécurité doit être appréhendée de manière globale pour prendre en compte les aspects économiques et industriels, sociaux, de gestion, éducatifs, juridiques, techniques, diplomatiques, militaires et de renseignement.

Comme le souligne l'avis, qui est conforté dans sa rédaction par l'approche tout à fait essentiel de la formation puisqu'il s'agit bien de combiner excellence technique, adaptabilité et coopération qui sont essentielles dans ce domaine, l'objectif doit bien être la création massive d'emplois durables et de qualité, ancrés sur le territoire.

Une stratégie nationale de cybersécurité va demander de la continuité politique et une vision à long terme.

La stratégie déclinée en Bretagne tout autant.

C'est pourquoi, sous le concept "cyber-valley", la CGT s'interroge sur l'analogie possible avec la silicon-valley, toute proportion gardée bien évidemment.

C'est plutôt sur le concept de concentration que nous voulons attirer l'attention.

Si on peut comprendre que dans ces concepts informatisés à outrance, la proximité des spécialistes favorise les interactions entre acteurs, la technologie elle-même n'est pourtant pas bloquante sur une concentration de type métropoles qui, avec un effet "aimant", aurait tendance de fait à favoriser autour d'elle de véritables déserts.

C'est pourquoi, dans ce domaine comme dans d'autres, l'aménagement intelligent du territoire est particulièrement utile pour avancer ensemble.

Intervention de Mme Valérie FRIBOLLE

Chambre de commerce et d'industrie de Région Bretagne

Je m'exprime au nom des acteurs économiques du collège 1.

Avec plus de 40 000 emplois en Bretagne, l'économie dite « numérique » représente pour notre région un puissant vecteur de développement. Outre qu'aucun territoire ne peut aujourd'hui se dispenser d'agir pour intégrer toutes les potentialités et les risques de la digitalisation, nous avons la chance en Bretagne de disposer d'entreprises et de savoir-faire historiques dans ce domaine.

Nous saluons donc ici l'effort réalisé pour développer un secteur clé de cette nouvelle économie qu'est la cyber sécurité. Nous approuvons les grandes lignes du projet, depuis la nécessaire adéquation avec les politiques nationales et internationales jusqu'au soutien à l'export porté notamment par Bretagne Commerce International.

Nous souhaitons cependant formuler trois remarques sur cette communication :

Tout d'abord, nous partageons les enjeux recensés dans le document sur la question de la formation. Sur les diplômes les plus avancés et les plus experts bien sûr. Mais également sur les formations plus généralistes et plus courtes. Nos entreprises auront besoin de compétences techniques largement sensibilisées aux enjeux de la cyber-sécurité, en complément de savoir-faire informatiques plus classiques. Toutes les entreprises ne pourront se payer des spécialistes dans ce domaine. Leur futur responsable informatique se doit d'être doté des compétences indispensables à la sureté de leurs activités numériques. Plus largement, il nous faut également s'interroger sur la capacité des PME à rémunérer des spécialistes de ces questions. Une réflexion sur le travail partagé de cadres de haut niveau est peut-être à engager.

Ensuite, nous constatons que de grands groupes structurent l'écosystème de la cybersécurité, autour de la DGA, du Conseil régional et des laboratoires universitaires. S'il est indispensable de s'adosser à ces donneurs d'ordres, il nous faut être attentif à l'intégration de plus petites structures dans la filière. Cela doit permettre d'une part de favoriser l'émergence de nouvelles entreprises en Bretagne dans ce domaine et d'autre part d'en faciliter la croissance par une insertion dans un environnement innovant et dynamique.

Enfin, nous observons que la construction de la Cyber Valley repose totalement sur une logique « d'offre », sans intégration à ce stade des besoins des entreprises et acteurs publics victimes des cyber attaques. Pourtant les travaux d'observations menés récemment par la CCI Bretagne montraient que :

- près de 17% des entreprises de la région ont subi durant l'année écoulée une ou plusieurs atteintes de leur système informatique, liées essentiellement à des attaques de programmes malveillants ou des techniques de hameçonnage ou « phishing ».
- Près de 50% des entreprises qui ont mis en place un dispositif de sécurisation l'ont fait par obligation ou après une fuite d'information.

Les risques sont là, et nous concernent tous directement. Face à cela, nos entreprises paraissent insuffisamment acculturées aux enjeux de la cybersécurité. Il nous faut collectivement envisager davantage d'actions de sensibilisation directes en ce sens, auprès de toutes les entreprises, qu'elles soient dites « stratégiques » ou non. Des compléments sur la suite qu'entend donner le Conseil régional au projet nous seraient utiles pour envisager le déploiement de ce type d'actions.

Intervention de M. Jean-Marc CLERY

FSU Bretagne

Le projet de développement d'une filière « cyber-sécurité » en Bretagne présenté ici revêt une importance particulière, ne serait-ce qu'au regard des financements annoncés pour l'enseignement supérieur et la recherche, cela dans un contexte où, à l'évidence, ces derniers sont bien loin de bénéficier des budgets à la hauteur de leurs besoins.

A cet égard, le CESER a été bien inspiré de poser la question de la réalité des moyens annoncés pour les bourses de recherche dans le domaine « Cyber ». Car il ne faudrait pas que les vingt bourses supplémentaires proposés soient allouées par redéploiement avec pour effet de limiter d'autant les autres projets de recherches.

La FSU se reconnaît également dans deux autres observations du CESER. La première insiste pour que les formations envisagées ne se limitent pas seulement au haut niveau et aux formations de pointe, mais que celles-ci soient étendues le plus largement possible à tous les niveaux. La FSU partage bien entendu entièrement cette idée.

La seconde recommande que le développement de la filière « Cyber » soit véritablement ancré dans les territoires. Il est important en effet que le modèle suivi ne soit pas celui d'une « techno-valley » hors-sol. Mais au-delà, pour la FSU, il faut créer les conditions d'une appropriation sociale la plus large d'un tel projet. Cela doit passer par des réalisations ambitieuses, aussi bien en termes d'évolution des équipements dans les territoires que de développement d'une culture commune accessible aux citoyens. C'est déjà ce que la FSU avait souligné en mars 2012 à l'occasion de l'étude de le Section prospective sur l'Appropriation sociale et la mise en débat des sciences et des technologies.

A cet égard justement, la FSU trouve que l'avis du CESER aurait pu aller plus loin dans ses recommandations sur les formations à développer. En effet, les technologies du cryptage et de la reconnaissance, le traitement et la captation des donnés, ne constituent pas que des enjeux technologiques. S'il n'y a certes pas que des « gentils hackeurs », le champ de la cyber-sécurité n'est pas non plus forcément voué à la vertu : la captation et l'utilisation des données, l'incursion inédite dans nos comportements via les nouveaux objets connectés ou les big data, posent également des problèmes redoutables, que ce soit en termes d'appropriation des données issues de nos « privacy » ou de respect des libertés. Ces problèmes sont autant de champs de recherche actuels pour le droit, la réflexion éthique ou les sciences sociales.

Mais ces questionnements doivent également inciter dès aujourd'hui tous les acteurs régionaux du « Pôle d'Excellence Cyber », à adopter une attitude de vigilance et de responsabilité, que ce soit à l'égard des usages qui seront faits de ces technologies, ou des contrats et des partenariats internationaux.
Dans un contexte marqué aujourd'hui par le « grand désordre mondial », mais aussi par le retour au sein du commandement de l'OTAN d'une inquiétante doctrine de la confrontation à l'est de l'Europe, ignorer les risques potentiels de dévoiement ou d'instrumentalisation de ces technologies serait commettre une lourde erreur.