Compte-rendu du colloque du 1er décembre 2016

# « La transformation numérique pour les collectivités territoriales : quels enjeux de sécurité et quels accompagnements ? »

*Palais des Arts, Vannes*

**dans le cadre des activités de la chaire Cyberdéfense et Cybersécurité Saint-Cyr, Sogeti, Thales**

Les Écoles de Saint-Cyr Coëtquidan ont organisé le jeudi 1er décembre 2016, dans le cadre des activités de la chaire cyberdéfense et cybersécurité Saint-Cyr, Sogeti, Thales, en collaboration avec le CREOGN et la ville de Vannes et avec le soutien de la région Bretagne un colloque sur la transformation numérique pour les collectivités territoriales.

Il s'est voulu un lieu d'échange et de réflexion sur la question de la sécurité des systèmes d'information des collectivités territoriales, problématique nouvelle à laquelle elles doivent répondre rapidement compte tenu de l'importance croissante de ces systèmes. Il a aussi permis de montrer l'importance de la collaboration entre les collectivités territoriales et les différents acteurs de la cyberdéfense pour élaborer une solution.

## *Introduction au séminaire :*

Après un mot d'accueil de M. **Lucien JAFFRÉ**, 1er Maire adjoint de la ville de Vannes, qui a rappelé l'implication importante de la ville de Vannes dans les nouvelles problématiques liées au numérique, M**. Gérard de BOISBOISSEL**, ingénieur de recherche au CREC Saint-Cyr (centre de recherche des écoles de Saint-Cyr Coëtquidan), s'est chargé d'introduire ce colloque. Il a d'abord rappelé l'importance croissante de la numérisation des systèmes d'information des collectivités territoriales et de leur interconnexion, puis a insisté sur la valeur des données placées sous leur responsabilité et sur la nécessité de les protéger. Les problématiques de sécurité soulevées par la protection des données numériques sont communes aux mondes civil et militaire. Ce colloque a donc réuni différents experts civils et militaires pour tenter de trouver des solutions pour mieux protéger les systèmes d'information.

## *Première partie : Les opportunités de la transformation numérique pour les territoires*

Bien qu'elle s'accompagne de freins et de difficultés à surmonter, la transformation numérique représente des opportunités nouvelles pour les collectivités territoriales, comme le rappelle **Mme Anne LE HÉNANFF**, maire-adjointe en charge de la communication, des systèmes d'information et du développement numérique pour la mairie de Vannes.

Selon **M. Jean OLLIVRO**, géographe à l'université de Rennes II. L'humanité est tiraillée entre une innovation qui libère et une volonté de contrôle. Les systèmes d'information évoluent actuellement à une vitesse fulgurante, notamment en Bretagne. On assiste aujourd'hui à l'apparition de nouveaux usages dus aux nouvelles technologies. Plus important, ces nouveaux usages se banalisent très rapidement. Cette évolution s'accompagne de nouveaux risques, comme la commercialisation de données privées recueillies par les nouvelles technologies. On constate aussi que le développement du numérique ne se fait pas à la même vitesse sur tous les territoires et engendre par conséquent des fractures.
Cependant, malgré les risques qu'elle occasionne, la transformation numérique est avant tout une source d'opportunités qu'il convient de saisir. Pour commencer, elle a permis à la Bretagne, région oubliée en 1950, de rattraper son retard, comme en témoignent la diminution rapide du nombre de zones blanches

ou encore son rôle stratégique dans la problématique mondiale des câbles haut débit. Les usages du numérique se démocratisent rapidement et les fractures semblent s'estomper, notamment entre les villes et les campagnes, et le concept de ville intelligente pourrait rapidement se généraliser au milieu rural, qui dispose de nombreux attraits pour les entrepreneurs de demain. Des réseaux se mettent aussi en place à l'échelle locale pour permettre une meilleure organisation des actions sur le territoire régional. La mise en place de différents *blockchains* permet aux habitants de s'associer et de se coordonner plus facilement. Enfin, des organisations locales tangibles sont rendues possible grâce à des acteurs locaux s'appuyant sur le numérique suivant quatre stratégies : la dynamique de l'ancrage, la dynamique de la redécouverte de l'itinérance, l'animation des transports collectifs grâce au numérique et la dématérialisation. Finalement, le numérique a permis de grands bouleversements en Bretagne, et doit aujourd'hui être vu avant tout comme une source d'aubaines malgré les risques qui l'accompagnent. Il est à l'origine d'un nouveau « pacte spatial », en permettant la diffusion d'informations entre les différents acteurs et territoires pour soutenir les initiatives et projets locaux.

Afin de pouvoir développer efficacement les services et usages liés au numérique en Bretagne, il est nécessaire de mettre en place des infrastructures adaptées. C'est le but du projet Bretagne très haut débit présenté par M. **Thomas RENAULT**, qui en est le directeur chez Syndicat mixte Mégalis Bretagne. La principale mission de cet organisme est de mutualiser des services trop compliqués à mettre en place pour de petites collectivités afin de leur permettre d'y accéder.
Comme on a pu le voir précédemment, le numérique se développe rapidement en Bretagne. Ce développement s'accompagne de l'apparition de nouveaux usages et équipements (smartphones, tablettes, objets connectés…) qui nécessitent toujours plus de bande passante pour pouvoir fonctionner correctement. Aujourd'hui, l'information numérique transite en partie sur les réseaux téléphoniques en cuivre. Or ces réseaux, qui n'ont pas été prévus pour transporter cette information, posent un problème d'atténuation lorsqu'on s'éloigne de la source du signal. Il est donc nécessaire de déployer un nouveau réseau, non plus en cuivre mais en fibre optique. Un tel réseau permettra, selon M. **Thomas RENAULT**, de répondre aux besoins croissants en bande passante actuels et à venir. Il s'agit aujourd'hui d'une tendance importante, comme le montre par exemple l'ambition de l'opérateur téléphonique Orange de déployer un réseau de fibre optique pour 60% des français à l'horizon 2020.
La fibre optique n'est pas une technologie très récente, mais elle présente de nombreux avantages qui lui permettent de répondre aux nouveaux besoins induits par la transformation numérique. En effet, elle résout le problème d'atténuation du signal lorsqu'on s'éloigne de la source, mais elle permet aussi de ne restaurer la symétrie entre réseau descendant et réseau ascendant : l'envoi d'information sur le réseau est aussi rapide que sa réception. À terme, cette technologie remplacera complètement le réseau en cuivre actuel, y compris pour les appels téléphoniques.
Cependant, le déploiement de nouveaux réseaux par des acteurs privés peut engendrer de nouvelles fractures numériques sur le territoire. En effet, ces acteurs auront tendance à mettre la fibre optique en place en priorité dans les zones où la rentabilité à court terme sera la plus élevée, comme les grandes villes par exemple. De nouvelles « zones blanches » du haut débit pourraient alors apparaître, puisque les usages du numériques de la part d'habitants de milieux ruraux ne sont pas différents de ceux d'habitants de milieux urbains. Une action publique est donc nécessaire en complément de l'action privée afin de pouvoir compléter leur initiative.

La discussion entre les différents acteurs publics a commencé très tôt, dès 2009, afin de coordonner leur action et de se fixer des buts communs. L'objectif qui en a émergé est de pouvoir fournir un accès au haut débit à l'ensemble des bretons à l'horizon 2030. Pour cela, il a fallu identifier les zones qui constitueront une priorité pour l'action privée (par exemple les grandes agglomérations comme Vannes ou Lorient) et celles qui pourraient décrocher et doivent donc bénéficier d'un soutien prioritaire de la part des acteurs publics (petites agglomérations, zones à faible densité de population, etc…).
Ce projet public est très couteux (2 milliards d'euros d'investissement public), ce qui explique la nécessité de l'étaler dans le temps et d'obtenir de nombreux financements (européens, nationaux, régionaux, départementaux et communaux). Certaines opérations ont commencé à partir de 2015 et se poursuivront en montant en puissance, notamment grâce à l'effort industriel qui se met en place aujourd'hui, afin d'atteindre l'objectif fixé en 2030.

Comme le rappelle M. **Daniel DEIN**, maire d'Orgères, les outils numériques sont utilisés quotidiennement par 80% des bretons, et la transformation numérique est donc une nécessité pour les collectivités territoriales, quelles que soient leurs dimensions. Par conséquent, les élus locaux doivent avoir un rôle moteur pour cette transition, en s'associant notamment avec des acteurs publics et privés. Bien que cette transformation prenne du temps, elle est un enjeu majeur pour le territoire et doit donc faire dès à présent l'objet d'une attention toute particulière.
Un exemple de l'importance de la transformation numérique pour les collectivités territoriales est la dématérialisation de la chaîne comptable. Cet impératif a des répercussions sur leur organisation interne, puisqu'elles doivent être en mesure de traiter des factures dématérialisées comme des factures sur support papier. Il faut donc mettre en place de nouveaux processus de traitement des données entrantes, acquérir de nouveaux équipements et former le personnel à leur utilisation.
La proposition de nouveaux schémas organisationnels, bien qu'elle s'accompagne de difficultés à surmonter, permet souvent de revoir l'organisation précédente. On peut ainsi d'alléger le système existant en évitant certaines étapes inutiles ou encore repérer des failles de sécurité ou dysfonctionnements et y remédier.
Le développement de services dématérialisés présente des avantages importants pour les habitants des communes. En effet, la plupart d'entre eux souhaite utiliser les nouvelles technologies, ce qui leur confère une certaine autonomie – sous réserve que les collectivités territoriales mettent les outils adéquats à leur disposition. Le recensement, par exemple, pourrait s'effectuer en ligne. L'autonomie ainsi acquise par les citoyens utilisant ces technologies et qui sont largement majoritaires (de l'ordre de 80% de la population) permet aux communes d'accorder davantage de temps à ceux qui ne souhaitent pas ou ne sont pas en mesure de les utiliser. Il est donc important de mettre ces outils technologiques à la disposition de tous, afin de fournir de l'autonomie à ceux qui veulent et peuvent les utiliser et être ainsi capable d'accompagner plus efficacement les autres.

Les intercommunalités ont quant à elle été créées en 1992. M. **Christophe MARTINS**, président de Montfort Communauté (35), explique que les nouvelles technologies et la transformation numérique ont immédiatement été intégrées à leur mode de fonctionnement. L'une des raisons permettant de l'expliquer est que les intercommunalités font appel à des personnes dont le niveau d'études – souvent deuxième ou troisième cycle – est globalement supérieur à celui des personnes travaillant pour les

communes, et appartenant en grande partie à une tranche d'âge plus jeune. Ainsi, les intercommunalités ont par exemple été les premières à se doter de sites internet. Elles ont aussi été à l'origine de nombreuses initiatives, comme la création de bases de données sur le logement à l'échelle intercommunale.

Cependant, la dématérialisation de nombreux services engendre le stockage d'une quantité importante de données sensibles sur les habitants (revenus, propriétés, composition de la famille…) par les collectivités territoriales. Par conséquent, des mesures doivent être prises pour les sécuriser efficacement et éviter qu'elles ne tombent entre de mauvaises mains. Or, ces questions de sécurités sont nouvelles pour les collectivités territoriales, qui sont mal préparées pour y faire face. Pour M. **Christophe MARTINS**, il y a deux facettes à ce problème. La première est la formation et l'information des personnels amenés à manipuler ces données. En effet, les failles de sécurité viennent fréquemment de l'intérieur des collectivités et les fuites d'informations qui en résultent ne sont pas toujours intentionnelles. La seconde est la question des moyens technologiques utilisés pour sécuriser et stocker les données. Bien souvent, les collectivités territoriales font le choix d'assurer elles-mêmes le stockage de leurs données, surtout pour les plus petites qui ne disposent pas des moyens financiers pour faire appel à des acteurs extérieurs. Cette analyse est partagée par M. **Daniel DEIN**, pour qui la sécurisation des données passe d'une part par la formation et d'autre part par l'acquisition d'outils technologiques adaptés, et qui met également en avant le problème des moyens financiers limités des petites communes pour faire face à cette nouvelle problématique.

Pour résoudre le problème du financement des mesures de sécurisation des données, les communes peuvent faire appel à l'intercommunalité. Cependant, M. **Christophe MARTINS** rappelle que les communes recherchent pour l'instant principalement des fonds et non pas encore la mutualisation des moyens et services avec ceux de l'intercommunalité.

Ces dernières sont conscientes de la nécessité de répondre à la problématique du stockage sécurisé des données, et prennent diverses initiatives dans ce but, comme l'embauche d'un technicien pour entretenir un réseau, mais cela ne semble pas suffisant et il parait nécessaire d'avoir des ingénieurs à disposition. Or, l'embauche d'un pôle d'ingénierie est coûteuse, et les petites intercommunalités réfléchissent donc à un moyen de mutualiser un tel pôle dans le futur. La mutualisation des moyens mais aussi les transferts de compétence (par exemple de la commune vers les intercommunalités) semblent donc inévitables pour pouvoir être efficients en matière de sécurité, comme le souligne M. **Daniel DEIN**. Pour cela, il faut donner le temps aux agents de prendre en compte les changements dans leur métier. Ensuite, il faut mettre en place des cycles de formation dans les collectivités territoriales.

La ville de Vannes, par exemple, a désigné un référent cybersécurité au sein de sa structure, afin de lui permettre de se former à l'extérieur et de sensibiliser ensuite les personnels aux questions de cybersécurité en interne, comme en témoigne Mme **Anne LE HÉNANFF**.

Enfin, les collectivités territoriales ne sont pas les seuls acteurs à prendre en compte. Le Trésor Public, par exemple, peine à suivre la progression très rapide de la dématérialisation des services, notamment en matière de paiement à distance.

## *Deuxième partie : Les enjeux de la transformation numérique pour les collectivités territoriales*

Les collectivités territoriales disposent de nombreuses données sensibles, comme l'état civil de leurs habitants, et sont aussi responsables du fonctionnement de systèmes sensibles comme la distribution de l'eau, rappelle M. **Ronan DOARÉ**, directeur du centre de recherche des écoles de Saint-Cyr Coëtquidan (CREC). Elles sont de plus la cible de nombreuses attaques, dont les *ransomwares* sont un exemple. La transformation numérique s'accompagne donc d'enjeux particulièrement importants pour leur bon fonctionnement.

Pour M. **Alexis BOUDARD**, directeur du programme DcANT (développement concerté de l'administration numérique territoriale) au secrétariat général pour la modernisation de l'action publique (SGMAP), la transformation numérique offre des opportunités de transformation et de modernisation de l'action publique. Elle intervient dans la vie quotidienne des citoyens et des entreprises, pour qui les technologies numériques revêtent une grande importance. De plus, le numérique est désormais omniprésent dans les politiques publiques et est responsable d'une transformation culturelle et managériale. Ces enjeux importants s'accompagnent cependant de grandes problématiques, comme les expertises à mettre en place ou le budget à allouer à ces nouveaux services.
En réponse aux nouveaux besoins liés au développement du numérique, M. **Alexis BOUDARD** propose différentes briques élémentaires avec lesquelles une solution peut être construite. Elles ont des fonctions très variées, allant des APIs (interfaces permettant d'accéder à des bases de données) à la mutualisation des services et équipements, en passant par leur simplification. L'une de ces briques est le « mode agile », permettant de développer un outil numérique en un temps très court en réunissant simultanément tous les acteurs ainsi que ses futurs utilisateurs. D'autres briques visent à simplifier la démarche des citoyens en ligne. Ainsi, le projet « France Connect » permet aux utilisateurs déjà connus d'une administration de ne pas avoir à saisir à nouveau toutes ses données lorsqu'il se connecte au site d'une autre administration. Un des projets présentés a par exemple pour but de diminuer la quantité d'informations à renseigner en ligne en utilisant les données dont l'État dispose déjà sur les citoyens.
Le développement de l'administration numérique a donné lieu à de nombreux échanges entre l'État et les collectivités territoriales, et ils se partagent la gouvernance du projet DcANT (développement concerté de l'administration numérique territoriale), lancé fin 2015. Ce programme a pour objectif de rendre les relations internes entre les différentes administrations plus efficientes. Il devra aussi fluidifier les échanges entre les différents acteurs publics (État, collectivités territoriales…) afin d'unifier leurs relations avec les usagers. Enfin, ce projet s'intéresse également à la question de la simplification et de la sécurisation de l'archivage électronique, ainsi qu'au développement de « l'écosystème numérique ».
Le programme DcANT a déjà produit des recommandations, comme la simplification des modes d'échanges entre les acteurs publics, la valorisation des démarches publiques en ligne ou le développement de la dématérialisation des démarches de bout en bout. Toutes ces recommandations ont pour but d'accroître le soutien et l'accompagnement des acteurs publics locaux dans l'élaboration de l'administration numérique à leur échelle.
À titre d'exemple, l'une des recommandations de ce projet est de simplifier les mécanismes d'identification et d'authentification des agents et des élus. Elle a donné naissance à un prototype,

« FranceConnect Agents », qui mettra notamment en place une « identité pivot » qui répondra à cette recommandation et qui sera rendue possible par un partenariat entre les différentes administrations.

La transformation numérique offre aux collectivités territoriales de nombreux outils qu'elles peuvent être tentées d'utiliser pour simplifier les démarches administratives et faciliter le travail collaboratif, comme la possibilité de partager des informations en ligne sur un *cloud*. Cependant, M. **Didier DANET**, responsable du pôle Action Globale et Forces Terrestres au CREC Saint-Cyr, explique que l'utilisation de ces outils est très réglementée. C'est le cas des *clouds*, qu'il développe à l'aide d'un cas pratique mettant en jeu une secrétaire de mairie, le maire et deux de ses adjoints, qui échangent des informations sur un espace de stockage en ligne et une adresse mail gérés par une entreprise américaine.
Une note d'information du 5 avril 2016, signée par le ministère de l'intérieur et le ministère de la culture et de la communication, précise que « l'utilisation d'un cloud non souverain, qui, par définition ne permet pas de garantir que l'ensemble des données sont stockées et traitées sur le territoire français, est donc illégale pour toute institution produisant des archives publiques ». Il est alors nécessaire de comprendre le raisonnement qui a abouti à une prise de position aussi extrême, et d'évaluer la portée juridique réelle de cette note.
Tout d'abord, cette note s'applique à tous les documents produits par une institution publique, qui sont considérés comme des trésors nationaux. Son impact est cependant affaibli par le manque de définition des termes employés. En effet, de nombreuses définitions de ce qu'est un « cloud souverain » existent : il peut s'agir d'un cloud qui traite et stocke les données sur le territoire, ou qui dispose en plus d'un actionnaire majoritaire français, ou encore qui respecte également les normes et la législation française. La note définit aussi les clouds « absolument français » comme étant souverains, mais il s'agit là encore d'une notion qui peut avoir plusieurs définitions.
De plus, la note n'a pas de portée juridique dans la mesure où elle n'est qu'une interprétation de la loi par l'administration française. De fait, elle ne préjuge en rien de la décision qui serait rendue par un tribunal confronté au problème. Les notions peu ou pas définies auxquelles elle renvoie rendent également possibles des situations absurdes. Par exemple, de nombreuses sociétés américaines ont déjà ou auront bientôt des serveurs de stockage sur le territoire français. De plus, imposer que l'actionnaire majoritaire soit français pourrait être interprété comme une violation des traités sur le fonctionnement de l'Union Européenne, car il pourrait s'apparenter à une forme de protectionnisme.
Enfin, cette note ne semble pas applicable en tant que tel dans l'optique du développement prévu de l'open data. Elle génèrerait un problème important : comment traiter le cas d'un individu qui stockerait sur un cloud non souverain des informations diffusées par une mairie ? Afin de résoudre ce problème, il faudrait tout d'abord s'interroger sur le statut des documents produits par les institutions publiques qui sont aujourd'hui considérés comme des trésors nationaux, ce qui parait abusif. Il faudrait peut-être aussi différencier ces documents selon la sensibilité des informations qu'ils contiennent. En l'état, la norme définie par cette note ne semble pas applicable.

Aujourd'hui, la question de la sécurisation des données prend une place croissante dans les réflexions sur la transformation numérique, surtout dans un contexte d'apparition de l'open data. Les collectivités territoriales seront de plus en plus amenées à mettre une partie des données dont elles disposent à la disposition des citoyens ou des entreprises. Mme **Sandrine TURGIS**, maître de conférences en droit public,

université de Rennes 1, chercheur associé au CREC Saint-Cyr et membre de l'IODE (CNRS 6262), voit différentes motivations à cela : tout d'abord, la demande de transparence de plus en plus forte, ainsi qu'une volonté de démocratiser l'accès à ces informations, qui permet par exemple un contrôle de l'efficacité des politiques publiques par l'ensemble des citoyens. L'utilisation de ces données pourrait aussi favoriser la création de nouveaux services innovants. Ensuite, des motifs juridiques motivent aussi le développement de l'open data : une loi de 2016 oblige les administrations publiques à mettre en ligne certaines données, comme certains documents administratifs ou les données mises à jour régulièrement et qui présentent un intérêt économique, social, sanitaire ou environnemental.

À la vue du développement rapide de l'open data, il convient de prendre des mesures adaptées pour s'assurer du respect de la vie privée des citoyens en protégeant efficacement leurs données personnelles et leurs données sensibles (informations médicales, opinions politiques, religion…). Pour cela deux pistes s'ouvrent à la législation. La première est l'interdiction de diffuser ces données ou une obligation d'occultation en cas de diffusion. La seconde, qui constitue une exception, est l'autorisation de diffuser ces données dans certains cas.

Le premier volet pose la question de la protection des collectivités territoriales en cas de diffusion par erreur d'une information à caractère personnel ou sensible. Une solution pourrait se trouver dans l'utilisation des licences, qui encadrent la réutilisation des données publiques et qui stipulent que « ne sont pas des données publiques susceptibles d'être réutilisées celles qui contiennent des données à caractère personnel ». Elles permettraient de limiter la réutilisation des données personnelles ou sensibles qui pourraient éventuellement fuiter.

Une autre solution envisagée par la loi est l'anonymisation des données personnelles. Ainsi, il est possible de rendre public les documents faisant intervenir des données à caractère personnel ou sensible après avoir occulté ces dernières. Cependant, cette anonymisation a un coût, à la fois matériel, humain et financier. Le projet de loi sur la République numérique le prend en compte, et fixe des limites à l'obligation de diffusion de certaines données trop difficiles à occulter pour les collectivités territoriales. Il existe d'autres méthodes pour rendre des données anonymes, comme leur insertion dans une base de données au caractère commun plus large ou de transformer la donnée elle-même pour ne plus pouvoir remonter à la personne d'origine.

Le problème majeur qui se pose alors est la capacité, dans certains cas, d'utiliser des méthodes d'analyse des données spécifiques pour remonter à la personne à partir de données occultées. Par exemple, on peut croiser différentes bases de données et identifier avec ce procédé des personnes à l'origine des données anonymisées. Afin de protéger les collectivités territoriales, qui pourraient dans ce cas voire leur responsabilité engagée, la CNIL va publier des référentiels d'anonymisation et délivrer des certifications.

Le second volet, qui porte sur l'autorisation exceptionnelle de publication de données personnelles ou sensibles, est particulièrement encadré. La diffusion de telles informations n'est possible que dans des cas très particuliers ou avec l'accord des personnes concernées. Un décret fixera les catégories de documents qui pourront être publiés sans faire l'objet d'un traitement d'anonymisation préalable.

Les collectivités territoriales auront aussi la possibilité de nommer un responsable de l'accès aux fichiers sensibles, et pourront toujours se référer à la CNIL, dont le rôle se trouve renforcé dans le cadre de l'open data, pour obtenir les conseils dont ils pourraient avoir besoin. Cette dernière, après concertation avec différents acteurs, adoptera un « pack de conformité en matière de données publiques » et publiera un guide de bonnes pratiques de l'open data. Afin de limiter les problèmes évoqués, il faudra désormais

inclure la protection de la vie privée dès la production des documents, dans la mesure où ils pourraient être destinés à être diffusés.

Des questions posées aux intervenants ont permis de mettre en lumière un paradoxe important de la protection de la vie privée. Bien que la loi interdise le stockage des données personnelles dans des clouds non souverains, la quasi-totalité de la population exporte de son plein gré une grande quantité de ces données vers des serveurs situés à l'étranger. Par exemple, les applications de santé présentes sur la plupart des smartphones collectent des données médicales sur leurs utilisateurs et les transmettent à des bases de données situées à l'étranger.
Ces questions ont également montré la difficulté pour les entreprises françaises, souvent de petite taille, à suivre le rythme imposé par les géants américains, bien que leur expertise soit tout aussi pointue. Ces derniers bénéficient en effet d'un développement beaucoup plus rapide que les TPE/PME françaises concurrentes. Selon M. **Didier DANET**, une volonté politique importante est nécessaire pour inverser cette tendance et venir en aide aux entreprises françaises.
Enfin, Mme **Anne LE HÉNANFF** est intervenue pour souligner la difficulté, pour les collectivités territoriales, de satisfaire à la fois les exigences de sécurisation des données d'une part et d'open data d'autre part auxquelles elles doivent répondre, et que l'un de ces aspects sera probablement amené, dans un premier temps, à prendre le pas sur l'autre.

## *Troisième partie : Les risques de la transformation numérique pour les collectivités territoriales au travers de cas pratiques*

La transformation numérique est une source d'opportunités, mais de nouvelles menaces apparaissent pour profiter des vulnérabilités qu'elle peut présenter. Le major **Fabrice CRASNIER**, commandant de la Division Analyse Criminelle et Investigations spécialisées de Toulouse à la Gendarmerie Nationale, lutte contre la cybercriminalité et a déjà été confronté à des attaques visant des collectivités territoriales.
Le *spoofing* est une usurpation d'identité qui peut prendre plusieurs formes, notamment l'usurpation d'adresse e-mail. Ce type de cyberattaque, très facile à mettre en place à l'aide d'outils disponibles sur internet, permet à un individu malveillant d'envoyer un mail en se faisant passer pour quelqu'un d'autre. Ces attaques peuvent par exemple cibler les collectivités territoriales pendant les périodes d'élections. On peut également trouver d'autres formes de *spoofing*, comme les attaques de type *man-in-the-middle*.
Le *spoofing* peut être particulièrement dangereux, puisqu'il peut servir à faire de la désinformation, mais aussi à propager des malwares. Un *ransomware* peut par exemple être joint à un mail, et il se propagera avec l'aide du destinataire, qui fera l'erreur d'avoir confiance en l'adresse mail de l'expéditeur.
Le *pharming* est une autre forme de cyberattaque, totalement transparente pour l'utilisateur. Il consiste à détourner des communications vers une adresse différente de celle du domaine que l'on souhaite atteindre. Pour ce faire, ce sont les vulnérabilités du protocole DNS qui sont exploitées. Plus précisément, ces attaques peuvent prendre pour cibles les serveurs DNS ou encore les routeurs locaux, ces derniers étant bien souvent insuffisamment protégés (par exemple par des mots de passe de type « admin – admin »). L'attaquant est ensuite en mesure de rediriger la victime de l'attaque vers les sites de son choix, comme des sites contenant des malwares.

Enfin, le défaçage est une attaque visant à pirater un site internet pour en modifier la présentation. Les attaques de ce type se sont multipliées au cours des dernières années. Cependant, elles sont facilement détectées, ce qui permet de rectifier le problème rapidement. Ce n'est pas le cas d'autres types d'attaques (*spywares* ou *rootkit* par exemple) visant à collecter des informations dans les systèmes des mairies sans se faire détecter. Ainsi, le major **Fabrice CRASNIER** explique que plusieurs mairies ont été la cible de telles attaques, qui sont passées inaperçues car elles ont été lancées au même moment que des défaçages. Des spécialistes ont donc réglé le problème posé par ces derniers sans remarquer des scripts introduits dans les systèmes des mairies par les hackers. Lorsque l'audit d'une mairie touchée a révélé leur présence, il s'est avéré que les hackers étaient allés jusqu'à diffuser leur code sur plus d'une dizaine d'autres mairies, et qu'ils collectaient depuis des informations à leur insu.
Les collectivités territoriales disposent de données particulièrement sensibles, comme l'état civil des habitants, les listes de recensement, l'aide sociale ou encore les services tels que le gardiennage ou les crèches. Face à la recrudescence des menaces évoquées ci-dessus, elles doivent donc mettre en place des mesures permettant de les protéger efficacement. Or, cette protection est bien souvent insuffisante voire absente, faute notamment de moyens pour les plus petites communes mais aussi de sensibilisation aux enjeux de la cybersécurité. Ce manque de protection peut aller de l'absence d'administrateur ou d'inspection régulière du réseau à la faible sécurité des mots de passe utilisés, en passant par l'utilisation de réseaux « open bar » permettant à tous les utilisateurs d'accéder à toutes les données présentes sur le réseau.
Les données dont disposent les collectivités territoriales sont sensibles et peuvent potentiellement intéresser les cybercriminels. Elles doivent prendre conscience de ces enjeux importants et modifier leur utilisation des technologies numériques pour les sécuriser au maximum. Pour cela, un accompagnement des collectivités territoriales est nécessaire, surtout pour les plus petites d'entre elles qui ne disposent pas des moyens d'adopter seules les mesures nécessaires à la protection de leurs données.

Afin de déceler les vulnérabilités d'un système, il est possible de faire appel aux services d'entreprises spécialisées réalisant des tests d'intrusion. Ces dernières reproduisent la démarche d'un attaquant, explique M. **Hervé TROALIC**, responsable Offre Expertise et Conseil SSI chez SODIFRANCE. Il a réalisé différentes tentatives d'intrusion qui ont souligné l'importance de mettre en place des mesures de cybersécurité adaptées.
Un premier test d'intrusion a ciblé un « reverse proxy ». Pour cela, SODIFRANCE a répliqué la méthode des cybercriminels. L'attaque a donc commencé par des recherches sur Google, qui ont permis d'obtenir des logins. Certains de ces logins étaient associés à des mots de passe de faible sécurité (comme la ville et le numéro du département), qui ont été aisément découverts par les assaillants. Ces derniers ont alors pu gagner un premier accès au serveur interne, dont ils se sont servis pour récupérer l'ensemble de la base de données du serveur et qui contenait notamment l'ensemble des mots de passe non chiffrés. Ils ont alors pu les utiliser pour accéder à certaines boîtes mail sécurisées par le même mot de passe et gagner ainsi accès au serveur proxy. Enfin, une faille du système leur a permis de devenir administrateurs du système.
Un second test a visé un site internet. En utilisant une faille très courante des sites web, il a été possible d'afficher la liste de tous les répertoires du site visé. La découverte dans ce répertoire d'un fichier

contenant les identifiants de la base de données a alors permis aux attaquants de prendre totalement le contrôle du site.
M. **Hervé TROALIC** a ensuite présenté un troisième test d'intrusion, utilisant cette fois le réseau wi-fi interne de l'entreprise. Les attaquants ont capté ce réseau et ont créé un faux point d'accès identique à celui-ci. Les smartphones des utilisateurs ont alors tenté de s'y connecter, ce qui a permis aux assaillants de récupérer leurs identifiants. Ces derniers étaient chiffrés, mais à l'aide d'un système de chiffrement très ancien qui a facilement été cassé. L'utilisation de ces identifiants a finalement permis la connexion au réseau interne de l'entreprise.
Le dernier test présenté a eu des conséquences importantes pour l'entreprise concernée puisque les vulnérabilités qu'il a mis en évidence ont retardé de six mois la création d'une application. Elle comprenait une faille qui a permis, après l'ajout d'une « backdoor » sur un profil utilisateur, de récupérer le mot de passe de l'administrateur, puis de récupérer l'ensemble des identifiants et mots de passe de tous les utilisateurs.
Ces tests d'intrusion mettent en évidence de nombreux manques en matière de cybersécurité. Selon M. **Hervé TROALIC**, il faut adopter plusieurs mesures pour corriger le problème. Tout d'abord, les utilisateurs doivent être sensibilisés aux problématiques de cybersécurité, afin d'adopter de bonnes habitudes pour sécuriser leurs données, gérer leurs mots de passe. Il est aussi nécessaire de formuler clairement une politique concernant les accès et les habilitations nécessaires pour accéder aux données, et de sécuriser efficacement les serveurs. Enfin, les tests d'intrusion apportent une réelle plus-value en repérant avant la mise en service d'un système ses failles de sécurité potentielles.

Comme le montre le récent développement des ransomwares, la transformation numérique est aussi une opportunité les cybercriminels. Ces malwares ont pour but d'empêcher les victimes d'accéder à leurs données, qu'elles ne peuvent récupérer qu'en échange du paiement d'une rançon. Il en existe deux types : les ransomwares bloquant, qui empêchent leurs victimes d'utiliser leur système, et les ransomwares chiffrant, qui chiffrent les données et ne fournissent la clé de chiffrement qu'en échange de la rançon. Ces derniers sont les plus problématiques, car les clés utilisées sont de plus en plus longues et rendent souvent le décryptage impossible sans payer la rançon. Le paiement s'effectue le plus souvent en monnaie virtuelle, ou plus rarement à l'aide de cartes prépayées. Comme le souligne M. **François PAGET**, administrateur au CLUSIF, le paiement de la rançon donne très souvent lieu à la récupération des données : *" Les cybercriminels démontrent ainsi l'intéret du paiement de la rançon, ils ne veulent pas tuer la poule aux oeufs d'ors".*
Les cibles des ransomwares se sont beaucoup diversifiées au cours des dernières années. Les particuliers ne sont plus les seules cibles des cybercriminels, qui s'attaquent désormais aux entreprises, aux administrations et même aux organismes de santé. Les collectivités territoriales, qui constituent des victimes de choix, n'échappent pas à cette nouvelle menace. En 2016, par exemple, une mairie du Lot-et-Garonne en a été la victime.
Compte-tenu de l'importance des données de certains organismes pour leur bon fonctionnement (entreprises, collectivités territoriales, etc…), le paiement de la rançon devient de plus en plus souvent la méthode choisie par les victimes pour espérer récupérer leurs données. Ainsi, les auteurs du ransomware Samsam auraient fait un bénéfice de 94 millions de dollars en six mois.

Le monde numérique offre de nombreux vecteurs d'infection aux cybercriminels. Ils peuvent, par exemple, infecter un système via un courriel avec une pièce jointe ou un lien piégé, ou par l'exploitation des vulnérabilités des navigateurs. Il est parfois difficile de se protéger de ces attaques, mais une sensibilisation à ces menaces et à une bonne utilisation des systèmes peut grandement réduire le risque. Ainsi, M. **François PAGET** rappelle qu'il faut s'assurer qu'un lien est fiable avant de cliquer dessus, mettre à jour régulièrement ses outils de bureautique et son système d'exploitation, et plus important encore, garder à jour son navigateur internet.
Enfin, la sauvegarde régulière des données du système permet de limiter fortement les conséquences d'une infection par un ransomware. En effet, il est alors possible de réinstaller le système et d'utiliser la sauvegarde pour récupérer ses données. En l'absence de sauvegarde, il est possible de faire appel à un expert pour identifier précisément le ransomware attaquant l'ordinateur. Dans certains cas, notamment si ce ransomware présente un bug exploitable connu, il est possible de restaurer les données. Cependant, en l'absence de sauvegarde et de possibilité de décryptage, le seul moyen de récupérer les données chiffrées est malheureusement de payer les attaquants. C'est donc à la victime de choisir si la valeur des données justifie le paiement de la rançon. Il est donc important de mettre en place des procédés de protection comme les sauvegardes fréquentes des données pour se prémunir de ce genre d'attaque, qui peuvent être particulièrement catastrophiques (par exemple pour une petite mairie ou encore un service de santé).

Les questions-réponses ont permis de développer certaines options disponibles pour protéger un système des attaques numériques. L'une des options est par exemple la mise en place d'un réseau interne, totalement déconnecté de l'extérieur. Cette solution a par exemple été adoptée par des organismes comme l'armée ou de grandes entreprises comme Airbus. La limite des mesures de cybersécurité prises pour protéger un système est souvent l'utilisateur lui-même : si les mesures de sécurité informatique sont trop contraignantes, le risque est que certaines personnes cessent de les appliquer systématiquement, affaiblissant ainsi la protection du système.
Quelle que soit l'issue d'une cyberattaque, le major **Fabrice CRASNIER** rappelle qu'il est absolument nécessaire de porter plainte. Bien que ces plaintes soient souvent classées sans suite, leur enregistrement est important pour faciliter le travail des gendarmes qui luttent contre la cybercriminalité en leur permettant de rester au courant de l'évolution des menaces numériques.
Enfin, le développement rapide des objets connectés va, selon M. **François PAGET**, en faire des cibles de choix pour les cybercriminels. Cependant, le colonel **Laurent VIDAL**, directeur adjoint du CREOGN (centre de recherche de l'école d'officiers de la Gendarmerie Nationale) rappelle qu'une bonne hygiène d'utilisation de ces données permet de limiter fortement le risque d'être victime d'une attaque. La plupart d'entre eux sont notamment protégés par un mot de passe, qui est très simple à la sortie d'usine (« 0000 » ou « 1234 » par exemple) et qu'il convient de changer dès la mise en marche du produit. Il est donc nécessaire de sensibiliser tous les utilisateurs aux bonnes pratiques à adopter pour protéger facilement ses systèmes d'une grande partie des attaques.

## *Quatrième partie : Les solutions pour faire face et les accompagnements*

Face à l'augmentation des menaces qui pèsent sur les systèmes d'information, M. **Gérard de BOISBOISSEL** rappelle que les utilisateurs peuvent compter sur le soutien de multiples acteurs pour les accompagner. Des solutions sont disponibles pour leur enseigner les bonnes pratiques à adopter pour limiter les risques, protéger efficacement leurs systèmes ou encore les aider lorsqu'ils sont victimes d'une cyberattaque.

Selon M. **Éric HAZANE**, représentant Bretagne de l'ANSSI, la transformation numérique est une source d'aubaines associée à de nombreux risques. Il cite notamment l'exemple de l'Internet des objets (IoT) qui se développe aujourd'hui très rapidement et qui suscite de l'inquiétude chez les experts de la cybersécurité. La sécurité des systèmes d'information s'articule autour de quatre axes d'effort majeurs : les dimensions technique, organisationnelle, juridique et humaine. L'aspect organisationnel est essentiel, puisque c'est grâce à lui qu'il sera possible de réagir si les techniques déployées ne permettent pas de se protéger suffisamment d'une cyberattaque. L'aspect juridique ne doit pas être ignoré, notamment dans le cas des collectivités territoriales qui sont déjà soumises à de nombreuses réglementations. Enfin, l'aspect humain est souvent déterminant en cas de cyberattaque et il est vital de le prendre en compte.
La complexification croissante des systèmes d'information constitue aussi un défi majeur pour les experts en SSI. Les nouvelles technologies, par exemple, introduisent souvent des failles de sécurité lorsque des utilisateurs les intègrent au réseau sans qu'elles soient préalablement sécurisées. La SSI devra aussi évoluer pour s'adapter aux nouvelles problématiques liées au développement de l'open data. Il est nécessaire pour les industriels d'intégrer ces questions de sécurité à leur processus de fabrication des outils technologiques afin de mettre en place une sécurité *by design*, bien souvent absente ou insuffisante aujourd'hui.
L'exemple des *ransomwares*, qui demeurent aujourd'hui difficiles à combattre, montre que les pratiques des utilisateurs ont un impact important sur la sécurité puisqu'elles peuvent limiter grandement le risque d'infection ou au contraire créer des vulnérabilités. Pour aider à sensibiliser le grand public aux questions de cybersécurité, des organismes comme l'ANSSI ou la DCPJ (direction centrale de la Police Judiciaire) mettent à disposition des guides expliquant les fondamentaux de la cybersécurité. La sauvegarde régulière des données sur un espace de stockage déconnecté du système est bien entendu toujours d'actualité.
L'ANSSI (agence nationale de la sécurité des systèmes d'information) est un service du premier ministre à compétence nationale, ce qui lui permet d'intervenir sur tout le territoire et d'être relativement autonome. Elle a notamment la capacité de déployer facilement des représentants dans les différentes régions. Ses deux missions sont la prévention et la cyberdéfense. L'action de prévention de l'ANSSI est effectuée avant les attaques et contribue à la sensibilisation des utilisateurs. L'action de défense intervient après une attaque et peut mobiliser un nombre beaucoup plus important de personnels. Sur les cinq cents personnes présentes à l'ANSSI, soixante-quinze d'entre elles peuvent être mobilisées simultanément, ce qui correspond à environ trois opérations de cyberdéfense. Ces dernières sont dédiées uniquement à la protection, l'ANSSI n'effectuant pas de cyberattaques ou de renseignement comme le rappelle M. **Éric HAZANE**.
Aujourd'hui, le nombre de cyberattaques continue de croître rapidement et les motivations des cybercriminels demeurent principalement financières. Cependant, la surface d'exposition à ces attaques

augmente elle aussi, avec notamment l'apparition des objets connectés, appelés à se multiplier dans les prochaines années. La cybersécurité est donc un enjeu majeur, et des organismes comme l'ANSSI sont nécessaires, notamment au sein des dispositifs de cybersécurité des régions. Ces dernières doivent aussi être une source d'initiatives en la matière pour pouvoir sécuriser efficacement les systèmes d'information.

Pour s'assurer de la protection des données dont disposent les collectivités territoriales, des contraintes réglementaires encadrent les mesures de cybersécurité, explique M. **Julien LEMOINE**, coordinateur technique du marché UGAP / Sécurité des SI, ESEC – Sogeti security center of competences. Cette réglementation définit un minimum de sécurisation des données que de multiples organismes comme les collectivités territoriales doivent mettre en place.
Certaines de ces mesures concernent principalement l'État, comme le PPST (Protection du Potentiel Scientifique et Technique de la Nation), qui cible plutôt les grandes écoles, universités ou encore les laboratoires de recherche. La PSSI – E oblige quant à elle les administrations de l'État à adopter une politique de sécurité des systèmes d'information, conforme à celle de l'État.
D'autres aspects de la réglementation concernant la sécurité des systèmes d'information peuvent être plus contraignants pour les collectivités territoriales. La LPM (Loi de Programmation Militaire) pourrait par exemple impacter le mode de transport des données qu'elles utilisent. Le RGF (Référentiel Général de Sécurité) peut se révéler encore plus contraignant. Il vise à améliorer la confiance des usagers dans les services numériques des organismes publics. Cela impose donc aux collectivités territoriales, entre autres, d'utiliser exclusivement des télé-services homologués au regard des normes définies par le RGF. On peut également citer les contraintes fixées par la loi informatique et libertés, encadrant notamment la collecte et le traitement des données personnelles et sensibles.
Pour pouvoir déployer des mesures de sécurité répondant aux standards fixés par la réglementation, les collectivités territoriales peuvent recourir à des acteurs privés. M. **Julien LEMOINE** explique qu'après avoir examiné leurs besoins en matière de cybersécurité, l'entreprise SOGETI a élaboré une offre y répondant qui s'articule autour de trois axes principaux : la gouvernance de la cybersécurité ; le conseil et la mise en œuvre de mesures de cybersécurité ; l'audit et les tests d'intrusion.
Les tests d'intrusion sont particulièrement demandés, en raison de leur capacité à déceler des failles de sécurité permettant ensuite de prendre des mesures pour y remédier, le tout à un coût relativement réduit. Ils donnent du poids à la parole des responsables de ces systèmes pour demander des moyens pour régler les problèmes détectés, en leur permettant de montrer les risques réels et les méthodes disponibles pour les réduire.
L'activité de conseil et d'accompagnement à la mise en œuvre de la cybersécurité est quant à elle plus souvent sollicitée pour des problématiques liées à l'architecture ou au durcissement des réseaux. En effet, les équipes de cybersécurité des collectivités territoriales ne sont souvent pas assez nombreuses pour gérer seules ces questions et peuvent donc faire appel à des entreprises extérieures. Ces dernières peuvent aussi être sollicitées pour aider des organismes dans le choix d'une solution de sécurité adaptée à ce dont elles ont besoin. Les métropoles peuvent par exemple leur faire appel pour le choix et la mise en place d'une solution de sécurité permettant aux usagers d'accéder à tous les services qu'elle propose en ne s'identifiant qu'une seule fois.
L'aspect de gouvernance SSI englobe un vaste panel d'activités. On peut par exemple citer l'accompagnement des organismes face aux nouvelles attentes en sécurité comme celles fixées par le

RGF. Une autre de ces activités est l'aide à la mise en place d'une PSSI, bien souvent absente ou insuffisante notamment dans le cas des collectivités territoriales.
On constate que parmi les collectivités territoriales, ce sont les communes qui sont le plus demandeuses d'assistance en cybersécurité. Cela s'explique entre autres par leur nombre mais aussi par les faibles moyens dont disposent les plus petites d'entre elles. Les demandes concernent très souvent des tests d'intrusion, qui leur permettent d'améliorer rapidement et de façon significative la sécurité de leur système.
Enfin, dans le but de couvrir les cyber risques, les collectivités territoriales peuvent également recourir à d'autres acteurs privés comme les assurances. **Mme. Kristell Bourgeaux-Semur**, experte technique pour le dommage aux biens et référante sur la souscription des risques émergeants au sein de la SMACL Assurances et **M. Olivier Daroux**, responsable sécurité à la SMACL Assurances interviennent afin de proposer des solutions et prévenir des cyber risques émergents. Tout d'abord **Mme. Kristell Bourgeaux-Semur** explique que les contrats actuels dit « traditionnels » n'apportent qu'une réponse partielle aux cyber risques. Une solution consisterait à proposer aux collectivités territoriales deux types de contrats dits « complets » avec la garantie « dommage immatériel non consécutif » (c'est à dire que le contrat assure plus que les dommages humains et matériels) :

- le contrat "standard" proposant uniquement une prestation d'assurance contre les cyberattaques.
- le contrat "hybride" incluant des offres groupées proposant des prestations d'assurances, de services ainsi que des partenariats avec des acteurs de la cyber sécurité. Celui-ci inclut trois garanties d'assurances :
    - des garanties de dommages avec la prise en charge des frais engagés pour les mesures d'urgences, la restauration des données, les frais de notifications, les frais de monitoring et de surveillance et enfin la remise en état du système d'information.
    - la garantie de responsabilité qui inclut la prise en charge de l'ensemble des réclamations des tiers du fait d'une intrusion dans un Système d'Information.
    - la garantie de cyber extorsion qui couvre les frais d'un possible consultant en cyber sécurité et le paiement d'une rançon.

En complément, **M. Olivier Daroux** insiste sur la prévention en complément des équipements de sécurité. Cela passe avant tout selon lui par une sensibilisation de l'utilisateur. Mise à part la prévention, il nous présente les services associés aux contrats d'assurance, avant et après les sinistres.

- Les services concernant l'avant sinistre permettent de diminuer l'impact de la future attaque en proposant :
    - une analyse préventive de la vulnérabilité des systèmes,
    - une assistance technique et organisationnelle pour le RGS,
    - une analyse des réseaux mafieux,
    - l'installation de matériel dans les Systèmes d'Information pour analyser les échanges réseaux,
    - une sensibilisation générale aux risques,
    - des conseils en sécurisation.

- En ce qui concerne les services après l'attaque il préconise, pour un retour plus rapide à la normale, d'intervenir rapidement pour diminuer les conséquences du sinistre grâce à l'aide :
    - d'une équipe d'assistance de gestion de crise,
    - un service de communication de crise,
    - un service d'expertise informatique pour les causes et la constatation des dégâts,
    - un service de conseil juridique,
    - un service de notification des tiers,
    - un service d'e-réputation pour réagir de manière appropriée aux informations non maîtrisées sur les réseaux sociaux.

Etant donné que la cyber menace est certaine il conclut en insistant sur le fait que l'assurance n'est qu'une des réponses aux cyber risques et que les points essentiels à respecter sont la prévention, l'hygiène informatique et la gestion de crise.

*Conclusions :*

Pour conclure ce séminaire, **M. Bernard Pouliquen**, vice-président du conseil régional de Bretagne en charge de l'enseignement supérieur, de la recherche et de la transition numérique après avoir remercié le CREC Saint-Cyr et la ville de Vannes, a rappelé que 50% des Etablissement Public de Coopération Intercommunale (EPCI) ont moins de 20 employés administratifs, 12% d'entre eux ont accès au très haut débit et 36% ont des personnels diplômés du supérieur avec des compétences en informatique, avec une forme hétérogénéité des formations au numérique. Il faut donc prendre en compte cette réalité concrète de ce que sont les EPCI d'aujourd'hui qui seront des acteurs clefs de la cybersécurité de demain, face à une exposition au risque qui va croître avec notamment pour exemple la problématique de la cyber protection de la gestion de l'eau.
**M. Bernard Pouliquen** a aussi rappelé les forces de notre région Bretagne avec le Pôle d'Excellence Cyber (PEC) qui va de son côté permettre d'améliorer les connaissances en cybersécurité, les offres de formation, créer de la valeur et une économie de la cyber sécurité dans un cadre d'intérêt général au service de tous. La recherche est également en pointe avec bien sûr la chaire de Saint-Cyr, Sogeti, Thales et plus récemment la création de nouvelles chaires crées sur la cybersécurité des infrastructures critiques et prochainement sur les IoT, toutes alliant acteurs académiques et industriels.

Une feuille de route de la région sur les questions de formation permettra également de répondre aux exigences des entreprises, ainsi qu'à la sensibilisation des acteurs locaux, avec l'idée de Kits fournis aux collectivités territoriales leur donnant des offres de solutions de cybersécurité construites avec le soutien de l'ANSSI, pour ainsi pouvoir limiter leur degré d'exposition aux risques cyber avec des solutions les plus à jour possibles.
Il appelle de ses vœux de nouvelles éditions de ce type de séminaire à l'avenir pour continuer la dynamique de recherche et d'échange initiée par cette journée du 1er décembre 2016 à Vannes.

*Aspirant Pierre MONNOT,*
*CREC Saint-Cyr, Mars 2017*