CYBER SÉCURITÉ & PARLEMENT

03 - NOVEMBRE - DECEMBRE 2014

AUTOUR DES 2EMES RENCONTRES PARLEMENTAIRES DE LA CYBERSÉCURITÉ

EDITO

par Bénédicte PILLIET, Directeur du CyberCercle

La deuxième édition des Rencontres Parlementaires de la Cybersécurité s'est déroulée le 23 octobre 2014 à l'Ecole Militaire avec plus de 500 auditeurs réunis autour d'une vingtaine d'orateurs. Une progression importante par rapport à la première édition qui avait accueilli l'année passée 250 auditeurs au siège de la Gendarmerie nationale. Je vois dans cette progression l'intérêt croissant pour les questions de cybersécurité, et nous ne pouvons que nous en réjouir tant celles-ci représentent un enjeu majeur pour la sécurité et le développement de notre pays.

Cette journée annuelle de Rencontres s'inscrit dans le cadre de la dynamique des petits-déjeuners-débats du CyberCercle qui accueillent chaque mois, sous présidence parlementaire, une personnalité experte de la cybersécurité, de la cyberdéfense ou de la lutte contre la cybercriminalité, et dont l'attraction ne cesse de se développer.

Les thématiques que nous avions choisi d'aborder cette année reflétaient la richesse de l'actualité en matière de cybersécurité : celle spécifique aux OIV un an après la LPM et dans la perspective de la publication des décrets d'application ; le dialogue public-privé dans la lutte contre la cybercriminalité, un thème abordé dans le récent rapport interministériel sur la lutte contre la cybercriminalité dit rapport Robert ; la déclinaison du Pacte Défense Cyber, un projet phare du ministère de la Défense en faveur de la cyberdéfense. Nous avons ainsi souhaité contribuer, à notre niveau, à l'enrichissement de la réflexion sur ces sujets fondamentaux, en favorisant les échanges entre les différents acteurs.

Je tiens ainsi à remercier l'ensemble des institutions publiques qui ont participé à l'élaboration de cette journée, l'EMA-Cyber, et plus largement le ministère de la Défense, mais aussi la Gendarmerie Nationale, la Direction Centrale de la Police Judiciaire, la Préfecture de Police de Paris, l'ANSSI, qui soutiennent notre action tout au long de l'année.

Je remercie également de leur soutien nos partenaires appartenant à la sphère privée dont la parole sur les sujets de cybersécurité est fondamentale.

Je remercie enfin les parlementaires qui depuis des années entendent mon discours sur la cybersécurité, faisant preuve d'une patience émérite, et qui s'investissent peu à peu sur ces sujets, et pour certains, même, beaucoup ! Leur implication dans ces sujets est vitale.

Cette journée a recueilli également le soutien de Jean-Yves LE DRIAN, ministre de la Défense, de Bernard CAZENEUVE, ministre de l'Intérieur, et d'Axelle LEMAIRE, Secrétaire d'Etat en charge du Numérique.
Défense, Intérieur, Numérique… on voit à travers les domaines dont ces ministres ont la charge que la cybersécurité est un sujet transverse qui ne concerne pas seulement la Défense ou la sécurité mais également le développement de notre économie par le numérique. Car il n'y a pas de développement économique s'il n'y a pas de confiance et de sécurité.

Ces Rencontres Parlementaires de la Cybersécurité illustrent la philosophie qui nous anime au sein du CyberCercle tout au long de l'année : être une plate-forme transverse, interministérielle, favorisant le dialogue entre les acteurs publics et les acteurs privés, les acteurs de la sécurité et les acteurs du numérique, sous dynamique parlementaire. Etre un lieu d'échanges privilégiés afin que par un meilleur dialogue, le niveau de cybersécurité de notre pays puisse progresser et être à la hauteur des défis qui nous attendent.

En publiant ce numéro de Cybersécurité & Parlement, et je remercie tous ceux qui y ont participé, nous avons voulu prolonger ces débats en attendant de nous retrouver le 21 octobre 2015 pour la 3ème édition des Rencontres.

LE PÔLE D'EXCELLENCE CYBER, UNE DYNAMIQUE AU SERVICE DE LA CYBERDÉFENSE FRANÇAISE

La cyberdéfense répond aux enjeux de sécurité de la France. Elle se développe mais elle renvoie à un «objet» lointain pour beaucoup de citoyens. Pourtant, la cyberdéfense concerne toute la population et la protection de nos intérêts vitaux. C'est d'ailleurs le sens de la nouvelle réserve citoyenne «cyber».

La cyberdéfense a été érigée au rang de priorité nationale par le Livre blanc et la loi de programmation militaire (LPM) 2014-2019.

Les moyens mis en œuvre par le gouvernement impactent positivement nos territoires. Ils sont facteurs de sécurité, d'emploi et d'innovation.

En présentant le Pacte Défense Cyber en février 2014, le ministre de la Défense a annoncé un effort d'un milliard d'euros sur la durée de la LPM et le renforcement significatif de la cyberdéfense. Celle-ci se construit actuellement en Bretagne autour d'un «Pôle d'excellence cyber».

Ce Pôle d'excellence réunit notamment la DGA Maîtrise de l'Information à Bruz, l'école des transmissions à Rennes, les écoles de Saint-Cyr Coëtquidan, l'Ecole navale à Brest, l'Université de Bretagne Sud dans le Morbihan, les entreprises de la région et bien sûr le ministère de la Défense.

En détail, ce sont environ 1300 personnes - dont 75 % sont ingénieurs, qui travaillent quotidiennement dans notre centre de référence d'expertise à Bruz au travers des domaines variés tels que les systèmes d'information, les télécommunications, l'expertise en sécurité d'armes et de munitions.

Ce sont également 200 étudiants déjà formés - avec un chiffre qui augmentera de 40 % à la rentrée prochaine, et environ 20 thèses supplémentaires développées dans nos laboratoires de recherches.

Sur le volet « entreprises », on dénombre dans notre pays près de 50000 emplois concernés par la cyber. En Bretagne, on dénombre environ 75 entreprises d'ores et déjà positionnées sur ce secteur, soit environ 8000 emplois directs.

En terme opérationnel, beaucoup de femmes et hommes sont également concernés. En plus de la 65e compagnie de guerre électronique et Saint-Cyr Coëtquidan qui assurera les entraînements, ce sont 200 militaires spécialistes qui seront implantés à Rennes dans 2 unités combattantes : le CALID Bretagne et une compagnie de combat cyber électronique.

En cohérence avec ce nouveau champ stratégique, l'Université de Bretagne-Sud va pouvoir développer ses partenariats avec l'ensemble des acteurs. En effet, ouvert depuis septembre 2014, un cursus universitaire professionnel d'ingénieurs en cyberdéfense forme 26 étudiants par an permettant ainsi de répondre en partie aux besoins d'ingénieurs spécialisés en France dont on estime le nombre à 1000 environ.

Plus globalement, une véritable dynamique impacte la région dans son ensemble avec des événements à la clé. Je pense à l'organisation des journées C&ESAR à Rennes ou, comme l'a annoncé le ministre dernièrement, un évènement international qui devrait se tenir à Saint-Malo en septembre 2015 au service de nos entreprises.

La France avait déjà, depuis de nombreuses années, fait le choix de la cyberdéfense en Bretagne. Notre région est aujourd'hui au cœur de la sécurité des Français. Elle contribue également au rayonnement de la France à l'international. Il appartient à chacune et chacun de participer à cette dynamique !

Gwendal ROUILLARD
Député du Morbihan
Secrétaire de la commission de la Défense nationale et des Forces armées

LE COMBAT NUMÉRIQUE AU SERVICE DES OPÉRATIONS MILITAIRES

Le cyberespace est désormais devenu un lieu de confrontation ainsi qu'un domaine militaire, au même titre que les domaines terrestre, aérien, maritime et extra-atmosphérique, reconnaît le Livre blanc sur la défense et la sécurité nationale de 2013. Or, pour rester une puissance à vocation mondiale, la France doit investir pleinement ce nouveau champ stratégique, qui mêle civils, militaires, États, entreprises, groupes d'intérêts et individus.

Dans ce contexte, le ministre de la Défense, Jean-Yves Le Drian, rappelle que le ministère de la Défense participe à la préservation de la souveraineté nationale, en lien avec tous les autres acteurs de la communauté nationale de cyberdéfense. Le Livre blanc sur la défense et la sécurité nationale de 2013 définit une doctrine nationale de cyberdéfense et fixe des objectifs clairs qui visent à placer le combat numérique au service des opérations, soutenir la communauté nationale de cyberdéfense et participer à l'émergence d'un communauté internationale favorisant la stabilité du cyberespace. D'autre part, la loi de programmation militaire 2014-2019 de décembre 2013 définit les moyens nécessaires pour renforcer l'expertise technique et opérationnelle du ministère de la Défense dans ce domaine et consolider la structure opérationnelle unifiée et spécialisée déployée depuis 2011.

Cette posture originale du ministère de la Défense se concrétise notamment par l'emploi de capacités informatiques défensives et offensives, adossées à de solides capacités de renseignement, pour la défense des systèmes d'information du Ministère et le soutien aux opérations militaires. Ces missions sont assurées par une chaîne de commandement unifiée, centralisée et spécialisée placée sous l'autorité du chef d'Etat-major des armées.

A sa tête, l'officier général (OG) « cyberdéfense » remplit deux fonctions répondant à deux têtes de chaîne : l'une opérationnelle au sein du Centre de planification et de conduites des opérations (CPCO) pour planifier, coordonner et conduire les opérations de cyberdéfense, l'autre organique pour coordonner les travaux de développement des capacités du ministère de la Défense et contribuer à soutenir la communauté nationale de cyberdéfense.

Pour assurer la coordination et la conduite des opérations de lutte informatique défensive, l'OG « cyberdéfense » dispose d'un réseau spécialisé et d'un centre d'analyse dédié, le CALID. Responsable du volet spécialisé et de l'expertise opérationnelle de cyberdéfense, le CALID est le centre opérationnel de surveillance, d'alerte et de détection du ministère de la Défense placé sous les ordres du CPCO.

En substance, le CALID, qui travaille en étroite collaboration avec son homologue de l'ANSSI, le centre opérationnel de la sécurité des systèmes d'information (COSSI), assure la surveillance des réseaux du ministère, détecte les incidents, analyse les causes et conséquences, propose des solutions et envoie, si nécessaire, des Groupes d'intervention rapide (GIR) sur le théâtre pour recueillir des informations supplémentaires ou aider au rétablissement des systèmes.

Il faut poursuivre les efforts pour durcir la posture du ministère de la Défense et maintenir le niveau d'excellence requis par l'évolution extrêmement rapide des menaces. En réponse, le ministre de la Défense, Jean-Yves Le Drian a lancé le Pacte Défense Cyber le 7 février 2014. A travers 50 mesures concrètes réparties en 6 axes, ce plan embrasse tous les aspects de la cyberdéfense et comporte à la fois des mesures internes au ministère, mais aussi, un ensemble de mesures destinées à créer ou soutenir des projets extérieurs des collectivités locales, des grands groupes, des PME/PMI, de nos partenaires internationaux ou encore de nos opérateurs en formation.

Appuyée par un financement de 1 milliard d'euros entre 2014 et 2019, la cyberdéfense est devenue une véritable priorité pour le ministère de la Défense, qui vise à valoriser ses capacités opérationnelles et l'excellence cyber incarnée par ses femmes et ses hommes.

Vice-amiral Arnaud COUSTILLIÈRE
Officier Général cyberdéfense
État-major des armées

LPM & CYBERSÉCURITÉ : BILAN ET PERSPECTIVE

Le Parlement a voté la loi n°2013-1168 de programmation militaire le 18 décembre dernier. Ses articles 21 à 25 visent à renforcer de manière significative la sécurité des systèmes d'information des opérateurs critiques pour la Nation. Où en est-on aujourd'hui de la mise en œuvre du texte voté et quelles sont les perspectives ouvertes ?

Rappelons en quelques mots l'esprit et la lettre du texte.

L'esprit du texte tout d'abord. Présentés au cours des travaux de préparation du Livre blanc sur la défense et la sécurité nationale engagés en 2012, l'accroissement rapide de la menace et le faible niveau de sécurité des systèmes d'information souvent constaté lors du traitement d'attaques informatiques visant la compétitivité des entreprises ou les secrets de l'Etat ont conduit la commission du Livre blanc à proposer des dispositions législatives destinées à renforcer la cybersécurité des administrations et entreprises les plus critiques pour notre potentiel économique, notre sécurité et notre défense. Le Président de la République a retenu ces propositions, incluses dans le Livre blanc publié en avril 2013.
Le Gouvernement a choisi de proposer rapidement au Parlement les dispositions législatives correspondant aux préconisations du Livre blanc. Il a donc décidé de les inclure dans la loi de programmation militaire dont la présentation était programmée et qui portait des objectifs de défense et de sécurité plus larges. Faute de disposer d'une liste d'opérateurs plus adaptée à la réalité du numérique, le choix a été d'appliquer ces mesures en faveur des « opérateurs d'importance vitale » (OIV) tels que les définit le code de la défense – administrations et entreprises dont la liste est classifiée de défense, l'objectif étant que d'autres acteurs s'approprient ces mesures par effet « tache d'huile ».
Le texte institue donc au niveau du Premier ministre un dispositif parallèle et complémentaire à la législation et à la réglementation portant sur les OIV (« directives nationales de sécurité - DNS », « plan de sécurité opérateur », « point d'importance vitale », « plan particulier de protection » adaptés au monde physique et suivis par les ministères coordinateurs), qui répond aux contraintes et à la cinétique du numérique, ainsi qu'à la réalité des métiers : toutes les fonctions critiques identifiées par les DNS ne sont pas portées par des systèmes d'information, notamment dans les infrastructures les plus ancienne ; à l'inverse, certaines fonctions désormais portées par des systèmes d'information peuvent se révéler critiques pour la réalisation d'une mission d'importance vitale.

Ce que dit le texte adopté par le Parlement.

L'article 21 de la loi précise que le Premier ministre définit et coordonne l'action gouvernementale en matière de défense et de sécurité des systèmes d'information. Pour ce faire, il dispose de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Le même article autorise des services de l'Etat à effectuer les opérations techniques permettant de comprendre et de neutraliser les effets d'une attaque informatique dans les conditions fixées par le Premier ministre.
L'article 22 donne au Premier ministre la charge de définir les règles techniques qui devront s'appliquer aux systèmes d'information critiques des OIV. Ces opérateurs devront lui déclarer les incidents intervenant sur ces systèmes et accueillir les contrôles du niveau de sécurité et d'application des règles techniques qu'il décidera. Ce même article précise qu'en cas de crise informatique majeure, le Premier ministre pourra imposer aux opérateurs d'importance vitale des mesures à mettre en œuvre.
L'article 23 vise à actualiser la liste des équipements susceptibles d'être utilisés à des fins d'écoutes sur les réseaux de communications électroniques et soumis à autorisation.
L'article 24 donne à l'ANSSI la possibilité de s'adresser aux opérateurs de communications électroniques pour obtenir les moyens d'entrer en contact avec des victimes d'attaques informatiques.
Enfin l'article 25 vise à éclairer la notion de « motif légitime » à la détention de codes informatiques malveillants. Cet article n'appelle pas de texte réglementaire.

Ce qui a été fait depuis le vote de la loi.

Concernant l'article 21, des consultations ont été engagées entre services de l'Etat pour définir les conditions de mise en œuvre et de conduite des opérations techniques destinées à caractériser la menace. Aujourd'hui prévu sous forme d'instruction classifiée de défense, un texte sera proposé au Premier ministre au début de l'année 2015. Par ailleurs, la liste des services de l'Etat susceptibles de détenir et de manipuler des codes malveillants est en cours de finalisation et sera soumise au Premier ministre également début 2015.
Pour les dispositions portées par l'article 22, dès le vote de la loi, l'ANSSI a mis en place avec des opérateurs des expérimentations pilotes destinées à affiner les notions de système d'information d'importance vitale, les types d'incidents susceptibles d'être déclarés et la procédure de déclaration. Les ministères coordonnateurs de secteur d'activité d'importance vitale ont demandé aux opérateurs de leur secteur d'identifier les systèmes d'information qui, selon eux, sont critiques pour assurer leurs missions d'importance vitale.

Trois principes ont été retenus : les mesures qui s'appliqueront aux systèmes identifiés devront être efficaces techniquement, adaptées aux métiers des opérateurs et soutenables financièrement et humainement, la réglementation nouvelle devra s'intégrer au mieux dans les réglementations existantes afin de peser le moins possible sur les opérateurs, enfin le dispositif mis en place devra être le plus opérationnel et le plus réactif possible.

L'ANSSI a, au regard des menaces connues et des attaques informatiques qu'elle traite, élaboré un socle de règles techniques qui sera proposé après la phase d'identification des systèmes d'information critiques, comme base de discussion des travaux de déclinaison sectorielle qui ont été engagés depuis octobre ou le seront d'ici mi-janvier selon les secteurs d'activités d'importance vitale impliquant des opérateurs privés.
Le décret d'application de l'article 22 dont la rédaction est achevée a été transmis au Conseil d'État avant la fin de l'année 2014 pour une publication au cours du premier trimestre 2015. Les arrêtés seront élaborés courant 2015, par secteur d'activité d'importance vitale voire par opérateur et publié ou non selon la nécessité de confidentialité des mesures prises.

Les échanges techniques se poursuivent entre administrations quant au texte d'application de l'article 23 avec pour objectif l'équilibre entre exigences de sécurité et développement économique.

Enfin, le décret relatif à l'article 24 est en voie de publication.

Pour un observateur extérieur, le constat peut être fait d'une action collective exemplaire : exécutif, législatif et acteurs économiques travaillent ensemble à rendre notre Nation plus résiliente aux attaques informatiques qui mettent en péril la confiance dans le numérique. Il reste bien sûr beaucoup de travail à accomplir et tant l'ANSSI que les ministères coordonnateurs ou les opérateurs s'investissent pleinement dans une tâche qui, il ne faut pas se le cacher, ne sera pas sans difficulté opérationnelle. Ce sera, pour l'agence que je dirige, l'occasion de stimuler notre créativité technique. Comme le dit Valéry : « Il faut, en quelque manière, honorer, considérer les difficultés qui se présentent. Une difficulté est une lumière. Une difficulté insurmontable est un soleil. »

Guillaume POUPARD
Directeur Général
Agence Nationale de la Sécurité des Systèmes d'Information

Y A-T-IL DU BISPHÉNOL DANS MON EMAIL ?

Selon Wikipedia, « le bisphénol A (BPA) est un composé organique issu de la réaction entre deux équivalents de phénol et un équivalent d'acétone. »

Cet article ne s'est pas retrouvé ici par erreur !

Il s'agit bien d'une publication du CyberCercle et non du cercle des nouveaux-nés dont les biberons ne sont désormais vendus qu'avec une mention explicite et obligatoire : « Garanti sans Bisphenol », jugé nuisible pour l'être humain.

Par analogie, le cyberespace n'est-il pas, et l'actualité nous le rappelle au quotidien, une constellation de pièges pour le citoyen ? Photos privées sur iCloud, usurpation d'identité, faux sentiment de sécurité à l'instar de certaines implémentations de SSL, etc… En toute logique, pourrait-on alors espérer à notre prochain achat d'iPhone que son emballage soit flanqué des mentions « Garanti sans iCloud », « Synchronisation d'origine incontrôlée », « Nuit gravement à la vie privée » ?

Sommes-nous un tant soit peu lucides lorsque nous présumons que le citoyen est en mesure de paramétrer son smartphone ou sa tablette pour réduire cette fuite incontrôlée de données, de maîtriser ses messages sur les médias sociaux, ou encore d' « auditer » les applications mobiles qu'il télécharge ? Qui est en charge de l'éclairer, de l'informer, de le prévenir, de l'assister lors de son achat ?

A l'époque du consumérisme roi et de la course effrénée au tout connecté, sur qui pèse la responsabilité du principe de précaution ?

Les objets numériques sont tout autant un atout considérable qu'une arme de destruction massive pour notre vie privée et nos secrets d'affaires. Il faut en être conscient.

Sensibiliser le citoyen commence au moment où naît son intention d'achat, lorsqu'il rajoute l'objet numérique à son panier, lorsqu'il franchit le seuil du point de vente, lorsqu'il s'apprête à passer en caisse, … et non plus tard, beaucoup plus tard quand il se retrouve esclave d'un gadget fort sympathique au demeurant.

Élus, régulateurs, influenceurs, associations de consommateurs, citoyens, bénévoles, prestataires, formateurs, … il est de notre responsabilité collective de baliser ce parcours d'achat et de donner au citoyen l'information et les clés pour se protéger, protéger sa vie privée et celle des ses proches.

Acteurs du numérique, champions des objets connectés, éditeurs en tous genres, … faites en sorte que le durcissement de vos produits soit le plus intuitif possible, usez et abusez de pédagogie, faites preuve d'empathie et parlez le langage du citoyen …

N'allez pas très loin, regardez autour de vous, parmi vos proches et vos amis, vos collègues et vos voisins, et dites vous que toute amélioration en ce sens leur sera en premier chef bénéfique.

Hadi EL-KHOURY
Co-Président Fondateur
Issa France

CYBERSÉCURITÉ : POUR UNE POLITIQ

Comme chacun le sait, les attaques contre les systèmes d'information des institutions et entreprises se sont multipliées depuis quelques années. Le ministère de la Défense a par exemple été victime en 2013 de 780 incidents informatiques significatifs, soit près du double qu'en 2012. D'après les chiffres de Symantec, entre 2012 et 2013, il y aurait eu 91 % d'augmentation du nombre d'attaques ciblées.
Alors que cette cyber-menace ira inévitablement en s'accentuant, je me réjouis des dispositions de la loi de programmation militaire 2014-2019, qui font de la cyberdéfense une véritable priorité nationale, suite aux recommandations de mon rapport de juillet 2012. Parallèlement à l'augmentation des moyens humains et financiers, la LPM contient en effet des avancées normatives essentielles. Je pense en particulier à l'obligation pour les opérateurs d'importance vitale (OIV) de notifier les incidents informatiques significatifs à l'ANSSI. Mais il reste encore beaucoup à faire, notamment dans le domaine industriel.

Pour une politique industrielle en matière de cybersécurité

À mes yeux, il est crucial pour notre pays de conserver une autonomie stratégique dans le domaine de la sécurité des systèmes d'information. Afin de garantir notre souveraineté et la sécurité de nos infrastructures vitales, il est indispensable de s'assurer de la maîtrise de certaines technologies fondamentales, de la cryptologie, à l'architecture matérielle et logicielle en passant par les équipements de sécurité ou de détection.

Garder cette maîtrise, c'est protéger nos entreprises. On ne doit pas non plus négliger les enjeux économiques et en matière d'emplois dans ce secteur, en forte croissance, qui participent à la compétitivité d'un pays. Selon les chiffres mentionnés dans le « plan France numérique 2020 », la contribution du numérique à l'économie française représenterait 3,7 % de l'emploi en France et contribuerait à hauteur de 5,2 % à notre PIB. La filière cyber représente aujourd'hui 40 000 emplois en France et un chiffre d'affaires de 13 milliards d'euros.

La structuration de la filière industrielle, véritable enjeu

La France dispose d'acteurs importants avec des grandes entreprises, à l'image de Cassidian, Thales, Bull, Sogeti ou d'Alcatel-Lucent, spécialisées et renommées pour leur expertise dans les domaines de la sécurité des systèmes d'information. On trouve également un tissu de PME-PMI innovantes, à l'image de Prim'x et d'Arkoon en matière de logiciels et produits de sécurité ou de Sysdream, d'Atheos et de DevoTeam en matière de services. Notre pays dispose de véritables « trésors nationaux » ainsi que des savoir-faire d'excellence, par exemple en matière de cryptologie ou de cartes à puces.

Toutefois, le secteur des fournisseurs français de solutions en sécurité des systèmes d'information souffre aujourd'hui de plusieurs lacunes : une trop grande fragmentation, qui entraîne souvent une concurrence destructrice entre les entreprises françaises et entrave le développement des PME ; une difficulté d'accès à la commande publique et un problème majeur d'accès au financement pour les PME ; et un positionnement trop « franco-français » pour assurer le développement de groupes solides, exporter et gagner des parts de marché à l'étranger ou nouer des partenariats à l'échelle internationale ou mondiale.

La France pourrait, si elle en a la volonté et en partenariat avec d'autres pays européens, développer une industrie complète et souveraine dans le domaine de la sécurité des systèmes d'information, à la fois dans les secteurs des matériels, des logiciels et des services.

LES PETITES & MOYENNES ENTREPRISES NE SONT PAS PROTÉGÉES CONTRE LA CYBERCRIMINALITÉ. ET APRÈS ?

En criminologie, une matière a longtemps fait débat : la victimologie, surtout quand elle s'est attachée à décrire des profils types de victimes. Faisant peser le poids de la responsabilisation sur celles-ci, ces théories tombèrent en désuétude. Pourtant, il est tentant de se poser la question : face à un cybercriminel, existe t-il un profil type de victime ? La réponse est oui. Les PME en sont un.

Au-delà des chiffres connus en matière de cybercriminalité, c'est plutôt l'absence de chiffres concernant les PME en particulier qui intrigue. Par exemple, le dernier rapport de Symantec paru en avril 2014 nous apprend que les petites et moyennes sociétés étaient en effet la cible de 31 % des attaques informatiques en 2012, contre 18 % en 2011. Mais, il souligne que très peu de chiffres sont disponibles uniquement pour la France.

Comment expliquer ce vide préoccupant ?

Les PME sont radicalement tournées vers leur cœur de métier et disposent rarement d'un responsable de la sécurité. Ce sont aussi des entreprises très dépendantes de leur image de marque, qui vont éviter de communiquer sur les attaques dont elles sont victimes ou pire, ne même pas porter plainte. Ces structures ne réalisent pas en quoi elles suscitent de l'intérêt alors que leur rayonnement est faible, qu'elles sont peu connues, voire peu « digitalisées », et quand bien même elles sont conscientes de la valeur de leur patrimoine immatériel, elles ne réalisent pas forcément que le numérique en est un moyen de captation.

Dans ces conditions, il est évidemment difficile de leur demander leur avis sur la cybersécurité avant de les avoir convaincues qu'elles en sont des parties prenantes. C'est bien ce qui explique qu'il n'existe, comme l'énonce à juste titre l'étude « Cybersécurité et PME : perception du risque, pratiques, besoins » dans le cadre du projet européen 2CENTRE, « aucune étude statistique crédible sur la perception du risque cyber par les PME ». Mais, peut-on croire et attendre réellement des PME, dans un environnement tendu, qu'elles accordent leur confiance, qu'elles ouvrent leur porte, leur budget, leur système d'information et qu'elles divulguent les attaques subies au risque de perdre leurs clients, et alors même que les fournisseurs de solutions de sécurité, petits et grands, n'offrent que des prestations taillées pour le CAC40 ?

La cybersécurité telle qu'elle est pensée, normée, dictée, marketée et vendue, est-elle vraiment adaptée à une PME ?

Quant il est revendiqué qu'une quinzaine des quarante règles du guide d'hygiène de l'ANSSI est applicable aux PME, est-ce à elles de faire le tri ? Côté normes, peut-on demander à une PME aussi critique soit elle, d'appliquer de la même façon les bonnes pratiques dictées aux OIV, sans au préalable avoir étudié avec soin le niveau cible de sécurité strictement nécessaire à celle-ci ?

Comment concilier le martelage jargonneux et anxiogène de la cybersécurité, avec en parallèle le combat pour la transformation numérique, à l'heure même où 50 % des PME ne semblent pas convaincues par le digital ? N'y a t-il pas comme une élimination naturelle des deux combats à la fois, et donc un problème dans la stratégie adoptée pour façonner « l'entreprise digitale et sécurisée de demain » ?

Il n'existe pas de recette miracle mais bien des leviers à actionner, pour tenter d'atteindre les PME et les impliquer :

- Le numérique comme potentiel de croissance et comme tremplin à une sécurité embarquée au plus tôt des projets : l'impulsion politique au numérique doit être une aubaine pour la communauté cybersécurité. Elle doit interpeller les pouvoirs publics pour la mise en place de synergies avec la French Tech par exemple pour innerver la maîtrise du risque au plus tôt des projets des start-up et de leur culture d'entreprise.
- Aller aux devants des PME, s'innerver dans leur quotidien : la sécurité n'attire pas les foules. Pour la défendre, la communauté cyber, institutionnels comme offreurs, doit sortir de sa zone de confort et explorer des lieux comme les CCI, les pôles de compétitivité, les syndicats professionnels. Si la DGSI se prête déjà au jeu, l'action par exemple de la Réserve Citoyenne Cyberdéfense dans ce sens, déjà bonne ambassadrice et pouvant agir du fait de son maillage territorial fort, est à encourager.
- Des offres adaptées : s'il est souhaité que les PME consacrent à terme un budget à la cybersécurité qui coûte très cher, il est impératif d'aller vers des solutions intégrées au-delà des classiques ségrégations « Produits/Services » « Solutions/Conseils ». Le Conseil est très opaque, difficilement appréciable par rapport à des produits bien concrets, sauf que l'achat de technologies sans dimensionnement des besoins au préalable est un investissement vain, et pourtant c'est bien ce qui risque de se passer au regard des politiques classiques d'achat des PME.

Les réflexions sont ouvertes et tout est bon à prendre, surtout à l'heure d'un aveu d'échec sécuritaire des PME.

Si vous avez des doutes quant à la pertinence d'un soutien et d'un marché ciblant les PME, méditez ce propos de Jim Lewis (CSIS) : « *la cyber-criminalité est un impôt sur l'innovation; elle ralentit le rythme de l'innovation dans le monde en réduisant la rémunération des innovateurs et des inventeurs* » et pour rebondir sur mon propos liminaire, gare à ne pas confondre « comportement de victimisation » et « responsabilisation ».

Diane RAMBALDINI
Présidente Fondateur
Crossing Skills

UE INDUSTRIELLE VOLONTARISTE

Il faut bâtir des partenariats autour d'industriels et de prestataires de service de confiance. L'État devrait aussi encourager une consolidation structurelle et capitalistique du secteur, en favorisant le maintien ou l'émergence de « champions ». Il n'est pas encore trop tard mais il faut s'y engager !

Des initiatives récentes qui méritent d'être saluées

Dans ce contexte, le Pacte Défense Cyber, annoncé par Jean-Yves Le Drian, doit être salué. Celui-ci appelle en particulier au renforcement de notre base industrielle et technologique de la cyber. Pour cela, il prévoit un soutien accru aux PME/PMI du secteur par l'intermédiaire du dispositif RAPID (Régime d'Appui Pour l'Innovation Duale), porté par la DGA. Pour structurer la recherche et le développement au sein des acteurs industriels, les études conduites par la DGA verront leurs moyens triplés et portés à 30 millions d'euros par an.

Le « plan cybersécurité », l'un des 34 plans de la Nouvelle France Industrielle, va aussi dans le sens d'un renforcement de notre politique industrielle de cybersécurité. Ce plan, piloté par l'ANSSI et validé par le Gouvernement le 4 juin dernier, propose la création d'un label France, qui donnerait confiance dans les entreprises et serait privilégié dans les appels d'offres publics. Il vise aussi à renforcer la position des industriels à l'international, avec l'ambition de leur faire gagner 30 % de parts de marché par an, et suggère la création d'un fonds pour la cybersécurité pour consolider la filière. Si je souscris à ces objectifs, les moyens doivent désormais suivre pour mettre en œuvre cette stratégie.

Vers une politique européenne de la cybersécurité ?

Certes la protection des systèmes d'information doit demeurer avant tout une compétence nationale, car elle touche directement à la souveraineté de chaque État, mais l'Union européenne a un rôle important à jouer car une grande partie des normes relèvent de ses compétences. L'Europe pourrait être plus ambitieuse et avoir la volonté, comme d'autres puissances émergentes, de parvenir à une souveraineté numérique, ce qui veut dire retrouver la maîtrise de certains composants (comme les microprocesseurs par exemple). Aucun État membre ne peut atteindre seul cette souveraineté. L'Europe seule le peut !

A ce titre, la publication, le 7 février 2013, de la nouvelle stratégie de l'Union européenne en matière de cybersécurité, ainsi que l'adoption en mars dernier par le Parlement européen de la proposition de directive NIS (Network & Information Security) – qui avaient donné lieu à une résolution du Sénat – devraient permettre de réaliser d'importantes avancées au niveau européen en matière de cybersécurité.

En définitive, je continue de plaider pour une politique industrielle volontariste en matière de cybersécurité. C'est pourquoi j'ai créé un groupe informel de parlementaires pour soutenir dans cette démarche le tissu industriel des entreprises françaises, notamment des PME, proposant des produits ou des services importants pour la sécurité informatique. De même qu'il existe en France une base industrielle et technologique de défense (BITD), je considère qu'il devrait exister une base industrielle et technologique en matière cyber (BITC). Il en va de notre souveraineté dans le cyberespace ainsi que de la compétitivité de notre économie !

Jean-Marie BOCKEL
Ancien ministre, Sénateur du Haut-Rhin
Membre de la Commission des Affaires étrangères, de la Défense et des Forces armées

FACE À LA CYBERSÉCURITÉ : LE BON SENS VS RÉALITÉ

Sujet récurrent illustrant la prise de conscience de nos dirigeants, la cybercriminalité n'en reste pas moins une réalité avec laquelle se construira notre société. Pour autant, cette menace ne doit pas être découplée du monde physique ; la géolocalisation en est un bon exemple. Cette dernière permet de savoir qui est où et quand, à travers les réseaux télécom et informatiques avec les multiples capteurs existants transitant à travers le cyberespace, et donc de se prévenir efficacement contre les criminels en connaissant leurs déplacements, leurs habitudes et leurs fréquentations.

Une entreprise doit faire face au gouffre culturel français qui sépare le monde public du privé. L'administration se méfie intrinsèquement des entreprises dont le but ultime resterait à leurs yeux le chiffre d'affaires et non seulement l'intérêt général…

Les menaces ne respectant pas les frontières virtuelles du public/privé, tous les acteurs publics et privés sont concernés par la cybercriminalité. Ils sont à la fois victimes et acteurs face à cette criminalité 2.0. L'Etat reconnaît régulièrement l'apport des entreprises dans cette lutte hautement technologique. L'Etat a besoin des grands groupes pour leur vision internationale et leur capacité de veille technologique, et il profite des réponses innovantes et réactives des PME spécialisées.

Mais si l'on devait tirer un bilan de ce dialogue, il serait très mitigé. Pour les PME, le dialogue fonctionne plutôt mal. L'exemple des services réquisitionnés peut laisser penser que l'Etat fasse ce choix pour répondre à un besoin urgent sans engagement. Mais que doit-on penser quand ces réquisitions se poursuivent dans le temps ? Le coût de cette « liberté » de l'administration reste à interroger face à nos finances publiques…à moins que la réponse ne soit finalement l'incapacité de l'Etat à planifier un besoin qu'un marché public aurait dû dimensionner. Plus généralement, les PME s'échinent à faire valoir leur savoir-faire, mais n'obtiennent que rarement des marchés publics.

L'arrivée de Thierry Delville comme Délégué ministériel aux industries de sécurité, alliée à la mise en place des organes de concertation de la Filière industrielle de sécurité avec le Conseil des Industries de confiance et de sécurité, sont porteuses d'espoir de dialogue. Cette philosophie enclenche une bonne voie avec des démonstrateurs satisfaisant à la fois les besoins capacitaires de l'Etat et le besoin des entreprises de prouver leurs innovations et de disposer ainsi d'un creuset d'emplois.

Nous avons aussi d'autres pistes d'amélioration.

- Fixer des indicateurs de performance communs entre les ministères, les organismes concernés et les industriels pour progresser et faire des choix en toute cohérence.
- La piste du partenariat d'innovation. Dans la lutte contre la cybercriminalité, il faut aller très vite et expérimenter les solutions proposées. Jusqu'à récemment il était impossible de coupler un marché de R&D et une acquisition en cas de succès. Mais le décret du 26 septembre dernier permet désormais d'expérimenter des innovations avant de les acquérir si elles s'avèrent satisfaisantes.
- L'autre piste est juridique. Les entreprises ont besoin de références pour être crédibles. Mais les budgets étant en peau de chagrin, une autre voie reste peu explorée : l'offre de concours. Cette disposition du droit public permet à une partie privée d'offrir gratuitement à une administration une prestation, sans la nécessité d'un appel d'offre. Aucune exclusivité d'usage n'est possible et cela doit répondre à un besoin d'intérêt général.

Chacun y gagne.

La France a aussi la chance d'avoir l'Euro 2016 de football, carrefour de multiples risques et menaces y compris en cybercriminalité. Profitons de cette opportunité de démontrer notre savoir-faire français au monde entier et illustrer concrètement un dialogue public privé réussi.

Delphine ARIAS-BUFFARD
Directrice des Relations Institutionnelles
DEVERYWARE

CONCERTATION PUBLIC/PRIVÉ : UNE STRATÉGIE OPTIMALE POUR LUTTER CONTRE LA CYBERCRIMINALITÉ

Si le Livre blanc sur la Défense et la Sécurité Nationale a hissé la cyber-défense au rang de priorité nationale, le récent Pacte Défense Cyber, plan d'action ambitieux porté par le ministre de la Défense, réaffirme la détermination du gouvernement à bâtir une défense solide face à la virulence des cyberattaques visant son économie et ses fonctionnements vitaux.

Le cyber-crime connaît en effet une vitalité sans précédent. Motivé par le gain financier, l'espionnage ou le terrorisme, il offre un visage polymorphe dans lequel certains États occupent une place de choix. Les révélations de l'affaire Snowden aux États-Unis en sont un exemple retentissant, pointant du doigt les investissements possibles d'un gouvernement dans la surveillance électronique.

Les individus, les entreprises et leurs données sensibles sont devenues des cibles lucratives qu'il faut protéger des exactions. Pour contrer cette déferlante, de nombreux pays européens ont mis en place une réglementation plus stricte en termes de confidentialité et de recueil de données ; en attendant le prochain Règlement Européen sur la protection des données, qui imposera aux entreprises françaises l'obligation légale de notifier toute violation ainsi que de lourdes sanctions financières.

Engagé dans ce plan stratégique de grande ampleur, le Ministère de la Défense va appuyer les missions de l'ANSSI, en corrélation avec d'autres ministères, notamment le Ministère de l'Intérieur, chargé de la lutte contre la cybercriminalité. Outre cette mobilisation collective, le Pacte Défense Cyber prévoit également des coopérations renforcées avec des partenaires étrangers.

Alors que les entreprises et organisations publiques françaises sont intégrées de facto dans une mouvance internationale où les réseaux criminels coordonnent des attaques de grande envergure depuis n'importe quelle partie du globe, une vraie collaboration opérationnelle entre les autorités nationales, les forces de l'ordre et les acteurs privés est nécessaire pour les protéger, bien au-delà de leurs périmètres habituels, commente Loïc Guézo, directeur du Développement Europe du Sud chez Trend Micro.

Trend Micro collabore avec les autorités policières mondiales, mettant à disposition son expertise, ses outils analytiques de surveillance et sa connaissance mondiale des menaces. Cette approche multipartite s'est soldée, parmi d'autres opérations, avec le FBI, à l'arrestation du cerveau présumé du malware SpyEye et plus récemment à la dénonciation de l'opération Emmental, une campagne complexe de cyber-attaques visant 34 institutions financières dans le monde.

Partenaire historique d'INTERPOL et intervenant du nouveau Global Complex for Innovation à Singapour, centre d'excellence de lutte et de coopération internationale contre la cybercriminalité, Trend Micro travaille également avec Europol et l'International Cyber Security Protection dans une démarche prospective sur l'utilisation et l'évolution des nouvelles technologies. Localement, la société a entamé des démarches collaboratives avec la Gendarmerie et la Sous-direction de lutte contre la cybercriminalité de la DCPJ, offrant expertise technique, formations et données stratégiques.

Il est désormais crucial pour les pouvoirs publics et les organismes d'application de la loi de s'appuyer sur des acteurs privés pour échanger ressources, meilleures pratiques et connaissances afin de renforcer la coordination et l'efficacité de leur lutte contre la cybercriminalité à l'échelle nationale, européenne et internationale.

Loïc GUEZO
Directeur du Développement Europe du Sud,
Trend Micro France
Administrateur du CLUSIF et Membre de l'ARCSI

UN VÉRITABLE PARTENARIAT PUBLIC-PRIVÉ POUR LUTTER CONTRE LA CRIMINALITÉ LIÉE AUX NOUVELLES TECHNOLOGIES

Plus qu'un dialogue, un véritable partenariat public-privé pour lutter contre la criminalité liée aux nouvelles technologies : une évidence concrète pour la Gendarmerie.

En matière de lutte contre la criminalité liée aux nouvelles technologies, le dialogue public/privée est une quasi obligation. De fait, la Gendarmerie comme toute force de sécurité a un besoin sans cesse croissant de création de nouveaux moyens de lutte contre ce fléau, mais ne peut en aucune manière assurer un quelconque développement. Tout juste peut-elle créer des versions Bêta en fonction de ses exigences, grâce au formidable vivier que représente ses officiers et sous-officiers titulaires de diplômes de haut niveau. Cependant, seule une entreprise dont c'est le métier et la vocation peut développer et amener à maturité un projet prometteur, afin de pouvoir elle-même en tirer profit tout en permettant à l'Institution d'obtenir un retour en sécurité, suivant le principe du gagnant-gagnant.

C'est dans cet esprit que le Pôle judiciaire de la Gendarmerie nationale (PJGN) développe et enrichit sans cesse depuis quelques années ce dialogue, axé sur la recherche perpétuelle d'idées voire de solutions pour mieux remplir ses missions. Plusieurs fois par mois, au sein du Service central de renseignement criminel (SCRC) comme de l'Institut de recherche criminelle de la Gendarmerie nationale (IRCGN) des rencontres se déroulent pouvant réunir industriels, membres de la communauté scientifique et bien sur experts et enquêteurs du Pôle. Elles sont l'occasion d'échanges tout à fait pragmatiques permettant de croiser les besoins de chacun.

Plus largement, la Gendarmerie s'est particulièrement investie dans la création en janvier 2014 lors du Forum international sur la cybercriminalité (FIC) de Lille d'un Centre expert contre la cybercriminalité français (CECyF), qui vise à fédérer l'action partenariale en matière de sensibilisation, de formation et de recherche entre les acteurs privés et publics concernés par la lutte contre la cybercriminalité. Le CECyF constitue un réel espace de rencontre pour la création de projets collaboratifs contre la cybercriminalité. Il a vocation à accueillir en son sein tous les services d'enquête, des administrations, des établissements d'enseignement et des entreprises de différents secteurs concernés par ces questions. Des projets sont en cours dans des domaines très variés, pouvant aller du développement d'outils opensource d'investigations numériques, à la mise en place de formations à distance tant pour les services d'investigation que des acteurs privés ou des collectivités territoriales.

Le principe même de fonctionnement de l'IRCGN, notamment dans son volet formation des officiers, favorise grandement le dialogue avec le privé. En effet, la plupart d'entre eux effectuent un cycle d'enseignement scientifique et technique (CEST), formation de haut niveau en lien avec leur domaine d'expertise. Cette formation, du niveau minimum de master, comprend systématiquement un stage de 6 mois au sein d'une entreprise, choisi méticuleusement en début de formation par l'officier, en accord avec sa hiérarchie, afin de « rentabiliser » au mieux cette formation. Ce stage est ainsi l'occasion d'apporter des réponses concrètes à divers questionnements criminalistiques, et permet également d'établir des relations durables avec des sociétés importantes évoluant dans le domaine informatique au sens large, si l'on s'en tient au domaine qui nous intéresse ici, mais pas seulement.

Plusieurs exemples peuvent illustrer ce propos mais nous n'en retiendrons qu'un, actuel : un partenariat, intéressant le domaine du véhicule, en cours et semblant des plus prometteurs. Dans le cadre d'un CEST, un officier a pu développer, grâce à une société implantée à Toulouse, une mallette de diagnostic universel de véhicule, permettant en particulier de lire les numéros d'identification des différents calculateurs et identifier ainsi, le cas échéant, à minima une partie de véhicule volé. Ce projet est parti d'un besoin avéré des experts en identification de véhicules de disposer de ce type de mallette, évitant ainsi de multiplier les outils dont il fallait disposer (gain en coût et en efficacité). Développer au sein d'une entreprise française, ce projet sans équivalent au niveau mondial lui est bien évidemment profitable, puisqu'en cas de succès elle serait à même de pouvoir vendre la mallette ainsi créée à différentes forces de police chargées notamment de la lutte contre le trafic de véhicule.

Notons d'autre part que dans le domaine des investigations judiciaires, les spécialistes en cybercriminalité du SCRC ne sont pas en reste, et travaillent également aux côtés de groupes industriels de haut niveau sur des sujets portant entre autre sur les réseaux sociaux, afin de pouvoir mieux les sécuriser mais également être capable de mieux y enquêter, dans des volets aussi divers que la pédophilie ou encore le terrorisme.

Cependant, en matière de partenariat public/privé, une nouvelle étape majeure a été franchie le 22 septembre dernier par l'Institution, avec la proposition faite de cession gratuite du logiciel GendExif® .

Développé une fois de plus par un officier de l'IRCGN dans le cadre de sa formation CEST, ce logiciel peut se définir très brièvement comme un outil portable multi-plateforme très simple d'utilisation permettant le traitement automatisé d'un grand volume de photographies à partir de tout support et leur analyse de manière intuitive et visuelle sur un fond cartographique.

Initialement diffusé uniquement au réseau des enquêteurs en nouvelle technologie (NTECH) de la Gendarmerie, tout en étant présenté aux autres unités de la gendarmerie ainsi qu'à la Police nationale, ce logiciel et son inventeur ont été rapidement victimes de l'engouement suscité. Des demandes d'ouverture plus large du logiciel n'ont pas tardé à affluer, tout comme étaient réclamées de nouvelles fonctionnalités. Il est ainsi rapidement apparu que ce logiciel n'était en fait qu'une version V0, aux perspectives encore insoupçonnées. En proposant la cession gratuite de ce logiciel, procédure tout à fait nouvelle pour la gendarmerie mais qu'il importera de pérenniser, l'institution s'assure ainsi de pouvoir bénéficier d'un logiciel s'adaptant régulièrement à ses nouvelles exigences, tout en permettant à l'entreprise ayant remporté ce marché d'un nouveau genre de s'ouvrir à d'autres perspectives.

Force est de constater que la lutte contre la criminalité liée aux nouvelles technologies ne cesse de croître et impacte nos vies quotidiennes. Sa prise en compte constitue une véritable exigence publique et politique qui implique la mobilisation, à la hauteur des risques encourus, non seulement des forces de sécurité, mais également de l'ensemble du tissu industriel travaillant dans le secteur. Si la gendarmerie dispose d'atouts importants à travers notamment son expertise non seulement technique mais également judiciaire, seule l'industrie a la capacité à concrétiser les idées. En accomplissant cette synergie, on créé ainsi une nouvelle formule mathématique, qui veut qu'en ajoutant les connaissances, les compétences et les savoir-faire de chacun, on multiplie les résultats de tous.

Général de division Jacques HÉBRARD
Commandant le Pôle judiciaire de la Gendarmerie nationale

LUTTE CONTRE LA CYBERCRIMINALITÉ : LA NÉCESSITÉ D'UNE COOPÉRATION PUBLIC - PRIVÉ OPTIMISÉE

La lutte contre la cybercriminalité est tout à fait spécifique et nécessite aujourd'hui de nouvelles stratégies procédurales et la mise en place d'un dialogue institutionnalisé avec le secteur privé. En effet, les infractions commises via les réseaux numériques sont commises par des canaux spécifiques, à savoir les prestataires techniques, les grands opérateurs de l'Internet qui détiennent des éléments de preuves numériques qui vont être utiles lors de l'enquête à la manifestation de la vérité et l'établissement des preuves. Cette coopération est devenue indispensable et implique la conclusion de partenariats constructifs et lisibles dans un souci d'efficacité renforcée.

Une coopération indispensable

Dans une note d'analyse publiée le 19 mars 2013, le Centre d'Analyse Stratégique - institution d'expertise et d'aide à la décision placée auprès du Premier ministre - affirme l'urgence de renforcer la politique de cybersécurité de la France. Le Centre rappelle que la sécurité des systèmes d'information est depuis 2008 l'une des quatre priorités stratégiques de la Nation, et fait quatre propositions destinées à tous, des citoyens aux opérateurs d'importance vitale en passant par les administrations et les entreprises de toutes tailles. La réalisation de ces objectifs permettra d'améliorer les processus de coopération et de rendre disponibles des outils et solutions en matière de sécurité. Pleinement conscient des faiblesses de de l'écosystème industriel, le Centre estime qu'il y a en France un manque de dialogue et une coopération insuffisante entre les différents acteurs de la sécurité.
Par ailleurs, les grandes entreprises des secteurs clefs de l'économie principalement les opérateurs d'importance vitale (OIV) particulièrement exposés aux cybermenaces doivent désormais avoir un dialogue constructif avec les autorités publiques, en particulier avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Pour lutter efficacement contre la cybercriminalité, l'Etat ne peut agir seul, non seulement car il n'a pas la maîtrise des outils techniques concernés, et notamment d'Internet, mais aussi parce qu'il n'est pas toujours en possession de l'expertise nécessaire à la détection de cyberattaques.

Les enjeux de la lutte contre la cybercriminalité nécessitent un dialogue indispensable avec l'ensemble des acteurs concernés et dans certains cas la conduite conjointe d'actions opérationnelles communes, qu'il s'agisse de l'analyse de la menace, d'échange d'informations, de recherche et de développement, ou encore, comme on l'a vu, d'actions de prévention ou même de formation.
Un tel objectif n'est en rien contradictoire avec le souhait d'un meilleur encadrement de certaines prestations privées dont il sera question plus avant.

Des exemples concrets

Le Conseil de l'Europe a fixé des lignes directrices pour la coopération entre les organes de répression et fournisseurs de services internet contre la cybercriminalité qui ont été adoptées lors des conférences Octopus qui sont ouvertes aux experts sur la cybercriminalité des secteurs public et privé du monde entier. La Commission européenne s'engage également dans une telle politique.

On peut citer quelques exemple comme celui de Signal Spam est une association qui regroupe des organismes publics (CNIL, ANSSI, OCLCTIC, Gendarmerie nationale) et privés (fournisseurs d'accès Internet, expéditeurs de messages, éditeurs de logiciels de sécurité, etc.) dans le but de lutter contre les spams et la cybercriminalité. Pour cela, elle recueille les signalements des internautes grâce à sa plateforme en ligne (www.signal-spam.fr) et les redistribue à ses partenaires sous forme d'information adaptée à leurs différentes missions : « top 30 » des plus gros spammeurs en France pour la CNIL, détection d'ordinateurs infectés pour les fournisseurs d'accès et l'ANSSI, etc. L'association est intégralement financée sur fonds privés, car les entreprises trouvent un intérêt économique à y participer. Les projets en cours (rapprochement avec l'association Phishing Initiative, participation au projet européen de « Centre de cyberdéfense avancée ») témoignent de la volonté de Signal Spam d'accroître son influence dans la lutte contre la cybercriminalité. »
L'association Signal Spam, consciente de l'importance de cet enjeu, est ouverte au monde académique et de la formation.
Les écoles et universités peuvent adhérer et soutenir le projet Signal Spam sans paiement de cotisation
Un Centre expert contre la cybercriminalité français a aussi été créé ; il s'agit d'une association permettant aux services chargés de l'application de la loi, aux chercheurs de toutes origines (académiques, industriels, indépendants) et aux établissements d'enseignement de se rencontrer et d'échanger pour créer des projets qui contribuent à la formation, l'éducation et la recherche contre la cybercriminalité. D'autres associations œuvrent dans ce domaine comme le Clusif en publiant un panorama annuel sur les tendances en matière de cybercriminalité et l'AFsin.
On peut aussi citer les opérations coordonnées par l'Agence européenne chargée de la sécurité des réseaux d'information (ENISA) où les opérateurs de télécommunication de différents pays européens, les acteurs du secteur privé et les pouvoirs publics ont participé à un exercice de simulation visant à tester la sécurité du système contre d'éventuelles cyber-attaques. Cet exercice fut nommé Cyber Europe 2012. Ces opérations transnationales de cyber-sécurité sont organisées afin de tester l'efficacité des moyens pour faire face aux cyber-attaques, leur coordination et collaboration. Le rapport sur l'exercice a été rendu public le 31 janvier 2013 par l'ENISA.

Des partenariats constructifs

Les exemples de démarches positives sont nombreux comme le Forum relatif à la cybersécurité, les Assises de la sécurité, évènements qui se déroulent chaque année et qui deviennent incontournables pour l'ensemble des acteurs. On se doit aussi de citer les think tanks comme le CyberCercle qui, à travers des petits-déjeuners-débats mensuels et les Rencontres Parlementaires de la Cybersécurité, permet d'associer et de sensibiliser les parlementaires à ces questions fondamentales de cybersécurité.

Ces partenariats comportent aussi des échanges d'informations et de bonnes pratiques, des initiatives visant à améliorer la formation, et des activités pertinentes en matière de recherche et de sensibilisation dans les secteurs public et privé. Les entreprises privées sont en première ligne dans la mise en place d'une démarche globale de cyberdéfense nationale. Leur maîtrise des données (hébergeurs, opérateurs, fournisseurs de services web en tout genre…) renforce l'intérêt du partage d'informations sensibles au sein de réseaux de confiance associant entreprises et agences gouvernementales. Leur expertise peut aussi être mise à profit via la fourniture de services et de produits de cybersécurité.

Conclusion et perspectives

Ainsi que le souligne le rapport du groupe interministériel sur la cybercriminalité , si de tels partenariats sont efficients et prometteurs, il convient toutefois de veiller dans le même temps à éviter un éparpillement de ces structures, ce qui aboutit souvent à un manque de lisibilité tant pour les entreprises que pour les internautes.

En vue d'accroître la sensibilisation à ces questions, les pouvoirs publics aux niveaux local, national et communautaire doivent favoriser une collaboration plus ouverte et transparente avec les entreprises afin de lutter contre la cybercriminalité et progresser dans une démarche de cybersécurité.

Myriam QUÉMÉNER
Avocat général près la Cour d'appel de Versailles

« Cybersécurité & Parlement » est éditée par le CyberCercle
Directeur de la publication : Bénédicte PILLIET
CyberCercle - 135 avenue de Versailles, 75016 Paris - Tél. : 09 83 04 05 37
cybercercle@defense-et-strategie.fr - www.defense-et-strategie.fr