CYBER SÉCURITÉ & PARLEMENT

Autour des 3E Rencontres Parlementaires de la Cybersécurité

Édito

Les troisièmes Rencontres Parlementaires de la Cybersécurité se sont déroulées le 21 octobre 2015 à l'Ecole Militaire avec plus de 560 auditeurs réunis autour d'une trentaine d'orateurs.
Ces chiffres s'inscrivent dans la lignée de la deuxième édition, notre volonté étant de garder ce format qui permet à la fois de bénéficier d'une audience notable, accentuée au-delà de l'auditoire par la campagne réalisée sur Twitter qui fait du #RPCyber l'un des « topic items » de la journée, et d'échanger dans des conditions efficientes et « humaines ». Ils confirment l'intérêt porté pour ces Rencontres, et de fait pour les questions de cybersécurité : nous ne pouvons que nous en réjouir, tant ces dernières représentent un enjeu majeur pour la sécurité et le développement de notre société.

Les RPCyber, c'est plus qu'un colloque.

Elles constituent un événement original d'une journée pendant laquelle les auditeurs ont accès à de l'expertise de haut niveau à travers les travaux qui sont menés, échangent de façon personnalisée dans l'espace de rencontres-ateliers-démonstrations avec les représentants des institutions publiques en charge de la cybersécurité et des acteurs privés de qualité, assistent à des démonstrations, techniques ou de serious games, et, pour les entreprises du numérique ou de la cybersécurité, rencontrent de façon individualisée les acteurs publics qui peuvent les aider sur les questions de financement de R&D, de labellisation ou tout simplement pour mettre plus de sécurité dans leurs produits ou services. Elles allient ainsi dimensions conceptuelles, stratégiques et opérationnelles, vocation de diffusion et services personnalisés.

Le sujet que nous avions choisi d'aborder cette année avec le SGDSN et l'ANSSI, « **la dimension industrielle de la stratégie nationale pour la sécurité du numérique** », s'inscrivait directement dans la dynamique de l'annonce de cette stratégie, dévoilée le 16 octobre par le Premier ministre, Manuel Valls. Aboutissement de plusieurs mois de travail coordonné par l'ANSSI en interministériel, elle témoigne de la prise en compte par les plus hautes instances de l'Etat de la nécessité d'apporter une réponse innovante et volontaire, s'appuyant sur des axes multiples et coordonnés, aux nouveaux enjeux nés de la place de plus en plus prégnante du numérique. La France est à cet égard un exemple à suivre au niveau international.

Les thématiques que nous avons abordées lors de cette journée reflètent **la dimension transverse, trans-sociétale, mais aussi l'importance économique de la cybersécurité** : sécuriser le tissu industriel national, quel que soit le secteur d'activité ; renforcer la filière de cybersécurité de confiance, socle fondamental pour la sécurité et la souveraineté ; enjeux et process de mise en œuvre d'une stratégie de sécurité numérique d'une entreprise, pour sauvegarder notre richesse économique et l'innovation… Autant de sujets traités lors de cette journée, nous permettant de contribuer, à notre niveau, à l'approfondissement de la réflexion et à la diffusion des sujets de cybersécurité, grâce à des intervenants de haut niveau.

Cette journée ne serait pas ce qu'elle est si elle n'était pas soutenue par les institutions publiques, les parlementaires et nos partenaires privés.

Je tiens ainsi à remercier l'ANSSI, l'EMA-Cyber, la DGA et le CALID, et plus largement le ministère de la Défense, la mission Lutte contre les cybermenaces du ministère de l'Intérieur, le Centre des Hautes Etudes du ministère de l'Intérieur, le Pôle Judiciaire de la Gendarmerie Nationale, la Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information de la Préfecture de Police de Paris, la Délégation interministérielle à l'Intelligence économique ainsi que CCI France.

Je remercie également de leur confiance et de leur soutien les députés et sénateurs membres de notre Comité Parlementaire qui, depuis des années, ont la patience d'écouter mon discours sur la cybersécurité, s'investissent de plus en plus sur ces sujets et travaillent avec nous tout au long de l'année. Leur implication sur ces sujets est vitale.

Je remercie enfin de leur soutien nos partenaires privés qui s'associent à un événement original et atypique, et qui apportent une présence et une parole fondamentales dans une dimension où le partenariat public-privé est indispensable.

Les Rencontres Parlementaires de la Cybersécurité illustrent la philosophie qui anime les orateurs et les auditeurs du CyberCercle tout au long de l'année, notamment à travers les petits-déjeuners-débats qui ont lieu tous les mois depuis mai 2012 : être une plate-forme transverse, interministérielle, sous dynamique parlementaire, favorisant les échanges entre acteurs publics et acteurs privés, acteurs de la sécurité et ceux du numérique, quel que soit le secteur économique, et permettant de décrypter et de faire avancer le cadre institutionnel de la cybersécurité par une compréhension mutuelle et un dialogue renforcés.

Pour profiter d'ailleurs de cet éditorial pour remercier tous ceux qui, au-delà des Rencontres, en venant s'exprimer dans nos instances et en participant aux échanges, contribuent depuis près de quatre ans, à faire du CyberCercle un cadre privilégié de référence pour la réflexion sur la cybersécurité.

Rendez-vous tout au long de l'année pour les petits déjeuners débats du CyberCercle, le 14 avril pour les Rencontres Parlementaires Cybersécurité & Milieu Maritime et enfin pour la 4E édition des Rencontres Parlementaires de la Cybersécurité qui se déroulera le 23 novembre 2016.

Bénédicte PILLIET
Directeur du CyberCercle

2 **Guillaume POUPARD,**
Directeur général, ANSSI

3 **Jean-Marie BOCKEL,**
Ancien Ministre, Sénateur du Haut-Rhin

3 **Michel VAN DEN BERGHE,**
Directeur général, Orange Cyberdéfense

4 **Gwendal ROUILLARD,**
Député du Morbihan, Secrétaire général de la Commission de la Défense nationale et des Forces armées

4 **Loïc GUEZO,**
CyberSecurity Strategist SEUR, Trend Micro France

5 **Vice-amiral Arnaud COUSTILLIERE,**
Officier général Cyberdéfense, Etat-major des armées, ministère de la Défense

6 **François COUPEZ,**
Avocat à la Cour, Atipic Avocat

7 **Laurent BERNAT,**
Administrateur à la Division des Politiques de l'Economie Numérique, OCDE

8 **Sylvie SANCHIS,**
Chef de la BEFTI, Préfecture de Police de Paris

8 **ICA Frédéric VALETTE,**
Responsable du pôle sécurité des systems d'information, DGA

9 **Thibault RENARD,**
Responsable intelligence économique, CCI France

CHACUN EST RESPONSABLE DE TOUS

Le Premier ministre a présenté le 16 octobre dernier la « stratégie nationale pour la sécurité du numérique », en présence notamment de la secrétaire d'Etat chargée du numérique, de plusieurs parlementaires, du secrétaire général de la défense et de la sécurité nationale, du Président du Conseil national du numérique et de nombreux dirigeants d'entreprises.

Cette participation des plus hautes instances de l'État, d'élus et d'acteurs économiques de premier plan montre que, transition numérique aidant, les questions liées à la cybersécurité issues de la seule sphère technique sont devenues de réels enjeux de société, impactent la gestion de la cité –pensons aux projets de villes intelligentes, à la pénétration du numérique dans la vie des administrés et doivent donc être pleinement saisis par le politique.

C'est d'ailleurs une des idées fortes présentées dans la stratégie nationale, au-delà des orientations mises en avant et qui seront évoquées plus avant dans le texte.

Dans un monde numérique en construction, chacun d'entre nous a une part de responsabilité effective dans la sécurité et la défense nationale. Il ne s'agit pas simplement d'une sorte d'incarnation numérique de « l'esprit de défense » que chacun connaît bien et qu'il faudrait développer dans les réseaux. Comme le montrent les traitements de nombreuses attaques informatiques, les caractéristiques propres au cyberespace font que le comportement d'un seul peut compromettre la sécurité de beaucoup, de tous.

La stratégie nationale identifie trois communautés.

Il y a d'abord celle qui regroupe les innovateurs, les créateurs des nouveaux usages, services et produits du numérique, les chercheurs, les opérateurs de réseaux de communications électroniques, les entreprises du domaine de la cybersécurité, les équipementiers et les intégrateurs. Cette communauté a le devoir de proposer des produits et services dont le niveau de sécurité correspond aux besoins exprimés par la nécessaire analyse de risque qui doit accompagner tout projet numérique. L'accompagnement de cette communauté relève particulièrement de l'agence nationale de la sécurité des systèmes d'information (ANSSI).

La deuxième communauté est constituée de tous ceux qui prennent les décisions concernant le la « gestion de la cité » et en tout premier lieu les élus, le Gouvernement, mais également les dirigeants des administrations centrales et territoriales et des syndicats. La mission de cette communauté est d'intégrer la sécurité et la défense du numérique dans la vision politique des entités dont ils ont la charge. Il appartient, par exemple, à l'élu d'une collectivité territoriale de demander à ses services que le site internet de sa collectivité bénéficie du niveau de sécurité nécessaire comme il lui appartient de faire voter les budgets requis. Dans la construction des « villes intelligentes », il appartient à l'élu de veiller à ce que les infrastructures et services mis en place soit suffisamment sécurisés pour résister à une attaque informatique dont les conséquences pourraient être la perte de vies humaines ou des dommages économiques et des pertes d'emplois. Outre ces conséquences humaines, la responsabilité des élus pourrait alors être engagée.

La compréhension du décideur politique ou de ceux qui le conseillent des liens étroits entre la confiance que les administrés attendent — et qui sera demain la condition de leur utilisation des services publics numériques, et la sécurité informatique sont essentiels. Cette confiance doit être visée et financée dès la construction de projets dont la robustesse aux attaques informatiques doit être régulièrement mesurée.

La troisième communauté, la plus large, est constituée de tous les utilisateurs du numériques, des chefs d'entreprises ou de responsables d'associations, de tous les citoyens. Il leur revient d'utiliser les ressources du numérique avec la prudence nécessaire afin de ne pas se mettre en danger, mettre en danger leurs proches ou leur entreprise, leurs clients ou leurs fournisseurs.

Dans les faits, chacun appartient au moins à deux communautés de sorte que, dans le cyberespace, comme l'a écrit Antoine de Saint-Exupéry : « Chacun est responsable de tous. Chacun est seul responsable. Chacun est seul responsable de tous. »

Comme le Gouvernement soutient le développement de la prévention en matière de cybersécurité et le traitement des atteintes aux systèmes d'information et aux données qu'ils transportent, notamment en permettant le développement de l'ANSSI dans un contexte budgétaire tendu, le Parlement participe à l'augmentation du niveau de sécurité informatique de la France. Ainsi, le vote à l'unanimité en 2013 des articles relatifs à la sécurité des systèmes d'information de la loi de programmation militaire a permis d'engager le dialogue nécessaire avec les opérateurs d'importance vitale et de définir, avec eux, les mesures susceptibles de renforcer leur résilience face à des attaques informatiques dont le nombre et la sophistication sont en augmentation.

Afin de poursuivre le travail engagé, et comme l'indique la stratégie nationale pour la sécurité du numérique, le Gouvernement a indiqué que, dès 2016, les études d'impact des projets de loi comprendront un volet consacré au numérique et, au sein de ce volet, à la cybersécurité, « établi sous l'égide des hauts fonctionnaires chargés de la qualité de la réglementation ».

Une autre idée contenue dans la stratégie nationale pour la sécurité du numérique est encore naissante même si, intuitivement, chacun peut en comprendre les fondements. Elle a trait à la captation des données personnelles des Français. On peut l'illustrer par deux exemples. D'une part une captation massive de ces données personnelles à des fins d'exploitation économiques par des acteurs étrangers peut entrainer un déséquilibre défavorable susceptible de mettre en danger une part de l'économie nationale voire européenne. D'autre part et dans certains cas, une captation ciblée de données personnelles — par exemple celle disponibles sur les réseaux sociaux concernant directement ou indirectement tous les parlementaires — et leur exploitation peut constituer un problème de sécurité nationale.

Si quelques cas d'exploitation de données personnelles obtenues par attaque informatique ont mis en danger les personnes concernées ou les entreprises victimes, il n'y a pas, à ce jour, de démonstration corroborant cette menace même si, on en comprend aisément les mécanismes.

La troisième idée contenue dans la stratégie nationale est issue d'une anticipation fondée sur l'observation des faits: depuis plusieurs années, les attaques informatiques sont en croissance forte en nombre et en sophistication. Et donc, plus la France avance dans sa transition numérique… plus elle augmente sa « surface d'attaque » et plus le risque d'être victime d'attaque informatique est grand! Ce raisonnement est applicable dans tous pays. Pourtant, pour l'entreprise, pour l'administration et pour chacun d'entre nous, la sécurité est régulièrement présentée et toujours vécue comme une contrainte et un coût.

La stratégie nationale pour la sécurité du numérique propose en quelque sorte d'inverser la charge de la preuve. La sécurité informatique doit devenir un avantage concurrentiel pour les produits et services proposés par les entreprises françaises. Dans un marché mondial concurrentiel et face à des menaces révélées quotidiennement, notamment contre la confidentialité des données ou la résilience de produits connectés, les utilisateurs se tourneront demain vers les produits et services qu'ils estimeront de confiance. Ainsi, pensée et intégrée en amont de la conception, la sécurité numérique des produits et services proposés par les entreprises françaises seront, à performance égale, en position favorable sur les marchés internationaux.

Le 16 octobre, le Premier ministre a présenté les grands axes et orientations de la stratégie nationale pour le numérique. Issue d'un travail interministériel engagé en juin 2014, cette stratégie présente cinq objectifs et propose des orientations pour chacun d'entre eux des orientations. Il appartient désormais aux ministères, soutenus par l'agence nationale de la sécurité des systèmes d'information (ANSSI), de contribuer à l'atteinte de ces objectifs par des actions relevant de leurs champs de compétences.

Le premier axe de la stratégie est dans la continuité des orientations données par les Livres blancs sur la défense et la sécurité nationale de 2008 et 2013. Il vise à renforcer la protection des infrastructures critiques de la France par une croissance de la sécurité de leurs systèmes d'information. C'est le sens du travail engagé entre l'ANSSI et les opérateurs d'importance vitale pour la mise en œuvre des dispositions législatives relatives à la sécurité des systèmes d'information contenues dans la loi de programmation militaire de décembre 2013.

Le deuxième axe concerne plus particulièrement la protection de la vie numérique des Français. Complémentaire du premier axe, il s'agit d'une part de promouvoir et défendre dans le cyberespace les valeurs de la République et d'autre part d'apporter une aide de proximité aux entreprises et particuliers victimes d'actes de cybermalveillance. Sur ce dernier point, un groupe de travail co-piloté par le Préfet chargé de la lutte contre les cybermenaces du ministère de l'Intérieur et l'ANSSI a permis de poser les bases de ce que sera le dispositif d'aide qui sera mis en place courant 2016 sur l'ensemble du territoire. Ce dispositif permettra également de soutenir l'activité locale des entreprises compétentes en matière de cybersécurité.

Le troisième axe aborde les enjeux des formations initiales et continues. La stratégie souligne que l'ensemble des Français doit être sensibilisé et que toute formation initiale supérieure doit intégrer un volet sensibilisation ou formation à la cybersécurité adapté à la filière.

Le quatrième axe vise à favoriser le développement d'un écosystème favorable au développement de produits et services de sécurité performants et de confiance. Il s'agit également de transformer la contrainte budgétaire et humaine liée à l'intégration de la sécurité informatique dans les produits et services en avantage concurrentiel pour l'entreprise et en valeur ajoutée pour le client.

Le cinquième axe, enfin, vise à mobiliser les Etats membres de l'Union européenne pour atteindre une véritable souveraineté numérique propice au développement d'acteurs européens de la cybersécurité. L'objectif est également de renforcer l'influence française dans les instances internationales.

Les responsabilités et le rayonnement des parlementaires les placent naturellement en première ligne pour la mise en œuvre de l'effort qui permettra à notre Nation d'être résiliente à des attaques informatiques qui aujourd'hui grèvent notre compétitivité, nous appauvrissent et détruisent des emplois et qui demain viseront nos infrastructures critiques, au risque de pertes de vies humaines et de dommages économiques graves.

Mes équipes et moi-même sommes à la disposition des membres du Parlement qui souhaiteraient un éclairage plus précis sur ces sujets.

Guillaume POUPARD
Directeur général
ANSSI

La part du numérique dans les services, les métiers et les objets ne cesse de croître. Demain, tous les objets – du pacemaker à la voiture – seront reliés à internet. Vecteur de croissance et d'innovation, la transition numérique est aussi vecteur de risques en matière de cybercriminalité, espionnage ou exploitation excessive de données personnelles.

Dans ce contexte, le Livre blanc de 2013 et la Loi de programmation militaire 2014-2019 ont fait de la cyberdéfense une priorité nationale, conformément aux recommandations de mon rapport du Sénat de 2012. Les moyens mis en œuvre depuis ont permis une montée en puissance de la France sur les enjeux cyber, faisant de nous un « champion » européen. Pour autant, beaucoup reste à faire.

En présentant la Stratégie nationale pour la sécurité numérique en octobre dernier, le Premier ministre a annoncé cinq principales mesures visant à accompagner la transition numérique de la société française. Si je souscris à ces objectifs, les moyens doivent désormais suivre pour mettre en œuvre cette stratégie.

Parmi ces mesures, la plus fondamentale concerne la défense et la sécurité des systèmes d'information de l'Etat et des infrastructures critiques. Selon les chiffres de Symantec, la France occupe le 14e rang mondial des pays où la cybercriminalité est la plus active. Il est donc crucial pour notre pays de renforcer la sécurité de ses réseaux critiques et de sa résilience en cas d'attaque majeure. Une vigilance accrue des pouvoirs publics sur l'utilisation des données personnelles est également essentielle, tout en préservant un équilibre entre sécurité et liberté.

Plus largement, il est capital pour notre pays de conserver une autonomie stratégique dans le domaine de la sécurité des systèmes d'information. Pour garantir notre sécurité nationale et la sécurité de nos infrastructures vitales, il est indispensable de s'assurer de la maitrise de certaines technologies fondamentales – telles que la cryptologie, l'architecture matérielle et logicielle, ou les équipements de sécurité et de détection. Garder cette maitrise, c'est aussi protéger nos entreprises.

SÉCURITÉ NUMÉRIQUE : UN ENJEU NATIONAL

En cohérence avec le Plan « Cybersecurite´» de la Nouvelle France industrielle, la nouvelle feuille de route du Gouvernement veut faire de la sécurité numérique un avantage concurrentiel pour les entreprises françaises. Notre pays dispose en effet de « trésors nationaux » et de savoir-faire d'excellence, notamment en matière de cryptologie ou de carte à puce. Dans le domaine des moyens de paiement par exemple, plusieurs entreprises nationales disposent d'une position concurrentielle au niveau mondial du fait de leurs atouts en matière de sécurité. De plus, les enjeux économiques dans ce secteur en pleine croissance ne peuvent être négligés. Selon les chiffres du « plan France numérique 2020 », la contribution du numérique à l'économie française représenterait 5,2% de notre PIB et 3,7% de l'emploi en France.

En outre, le Gouvernement prévoit de renforcer la sensibilisation du grand public et des postes à responsabilités aux enjeux cyber. La cyberdefense concerne toute la population et la protection de nos intérêts vitaux. Elle reste pourtant un concept lointain et abstrait pour nombre de nos concitoyens. Pour cela, l'accent doit être mis sur le respect des règles élémentaires de sécurité – assimilées à des règles d'hygiène informatique élémentaires – souvent perçues comme des contraintes par les utilisateurs. Je crois en cette notion d'hygiène dans l'entreprise comme dans l'administration pour se protéger de 90% des attaques et des problèmes. Tout ne peut être dit par téléphone ou par email. Si chacun adopte un comportement prudent, la majorité des risques peuvent être limités ou éliminés au niveau d'une communauté nationale.

Dernier enjeu : la formation. Car le constat est simple, il existe peu d'ingénieurs spécialisés dans la protection des systèmes d'information et les entreprises ont du mal à recruter. C'est pourquoi, les liens avec les universités et les centres de recherche doivent être développés. Un premier pas a été fait avec l'annonce de la constitution d'un groupe d'experts pour améliorer les formations dans l'enseignement supérieur. Je regrette néanmoins que la question de l'apprentissage du chiffrement n'ait pas été clairement évoquée. A ce jour, seules les écoles spécialisées dans l'informatique enseignent la cryptographie. Les autres écoles d'ingénieurs ne le proposent que dans le cadre de programmes « découverte ». Pourtant, former les étudiants d'aujourd'hui, c'est préparer l'avenir.

Jean-Marie BOCKEL
Ancien Ministre
Sénateur du Haut-Rhin

La numérisation de l'économie contribue sans doute possible à son développement. Toutefois, la production et la diffusion de logiciels malveillants minent cette création de valeur. L'approche ancienne de sécurisation des seuls systèmes d'information des entreprises a montré ses limites. Les dispositifs tels les antivirus se cantonnent à chercher ce qu'ils connaissent déjà : les signatures des *malwares* qui ont été préalablement référencés dans la bibliothèque de leurs éditeurs respectifs. Ce n'est plus une fois que l'informatique cible a été contaminée qu'il faut se décider à agir. Mais bien en amont pour limiter l'impact d'une cyberattaque. L'avantage concurrentiel revient donc aux opérateurs de télécommunications qui sont en mesure d'analyser en temps réel les flots de données qui circulent sur leurs infrastructures.

Cette capacité sert d'abord à nourrir leur connaissance de l'état de l'art : ils sont les mieux placés pour observer et documenter les techniques employées par les centaines de millions d'utilisateurs de leurs équipements. Un panel d'une densité et d'une qualité sans équivalent chez les prestataires en sécurité dont le périmètre d'action se borne au nombre de postes de travail infectés de leurs clients.

Le positionnement des opérateurs télécoms est également valorisé pour limiter l'impact des campagnes de déni de service (DDoS). Quand des dizaines de milliers d'ordinateurs contaminés à l'insu de leurs propriétaires obéissent à l'ordre du pirate de se connecter simultanément à un site Internet afin de le rendre inaccessible, voire de le mettre hors d'état de fonctionner. L'analyse anonymisée des connexions et l'identification grâce aux technologies de Big Data des comportements inhabituels permettent de singulariser les prémices d'une campagne d'attaque DDoS. La capacité à sérier les connexions à destination d'un site Internet donne la possibilité à l'opérateur de leurrer le flux émanant d'ordinateurs zombies (Botnets), rendant au final l'assaut quasiment indolore pour la cible. En effet, les connexions illégitimes sont détournées afin qu'elles ne saturent pas l'accès au site Internet qu'elles visaient. Laissant le champ libre aux utilisateurs légitimes qui peuvent accéder aux pages souhaitées sans encombre.

LES ENTREPRISES ONT DES MOYENS DE RIPOSTER À DES CYBERATTAQUES

Cette riposte numérique intervient en quelques minutes, évitant des pertes économiques potentiellement considérables. Notamment pour les sites de e-commerce qui ne peuvent se permettre de voir leurs vitrines paralysées à des moments cruciaux de l'année (périodes des soldes, semaines précédant les Fêtes de Noël, lancement d'un nouveau produit particulièrement attendu…). L'entreprise est donc en mesure de se doter de moyens de réponse aux cyberattaquants afin de ne pas attendre passivement que l'attaque cesse. Ou de considérer le déni de service comme une fatalité. L'offre de location de batteries d'ordinateurs infectés devient de plus en plus accessible, tant du point de vue financier que par la facilité à trouver ce type de prestataires via des moteurs de recherche.

Cette arme numérique est donc appelée à prospérer encore dans les mois à venir. D'autant, comme le notait Arbor Networks en avril 2015 dans son rapport d'activités[1] que les attaques de ces derniers mois ont connu des intensités jamais égalées jusqu'à présent. Comme si les assaillants industrialisaient de plus en plus leurs pratiques. Ce nouveau contexte exige que les entreprises choisissent avec soin leurs prestataires, en privilégiant ceux qui tels les opérateurs télécoms peuvent réellement mettre à leur disposition les moyens techniques de se protéger. Ici la riposte fait pleinement partie de la cyberdéfense.

Michel VAN DEN BERGHE
Directeur général
Orange Cyberdéfense

[1]Arbor Networks Detects Largest Ever DDoS Attack in Q1 2015 DDoS Report, 28 avril 2015.

LE RENFORCEMENT DE LA FILIÈRE DE CYBERSÉCURITÉ

Un temps mésestimées, les menaces cyber ont été identifiées dans le Livre Blanc sur la Défense et la Sécurité nationale de 2013 puis dans la Loi de Programmation militaire 2014 – 2019, comme « *des menaces majeures susceptibles d'affecter la France* ».

L'essor du numérique a multiplié les interconnexions, marquant ainsi l'avènement d'un nouvel espace – aux frontières plus difficilement définissables – parfois qualifié de « cinquième champ de conflictualité ». L'organisation terroriste Daesh l'a d'ailleurs pleinement investi comme l'ont révélé les récents attentats de Paris, avec une organisation cyber très développée, l'utilisation de messages cryptés, l'omniprésence sur le réseau internet…

Le think tank américain CSIS – Center for Strategic and International Studies – estimait récemment le coût annuel des cyberattaques dans le monde à 327 milliards d'euros. En France, le nombre d'attaques cyber aurait augmenté de 51% en un an.

La menace plane partout où règne le numérique : des organismes d'importance vitale (OIV) aux collectivités, des grands groupes aux particuliers… L'affaire Stuxnet, les attaques subies par Bercy ou TV5 monde, les nombreux cas de *pishing*, tentatives d'escroqueries ou de captations de données ont prouvé que nous étions tous des cibles potentielles. Ayant pleinement pris la mesure de cet enjeu stratégique, le gouvernement a multiplié les moyens alloués à notre défense dans ce domaine et nous disposons aujourd'hui d'atouts exceptionnels.

D'abord avec le Pacte Défense Cyber, présenté par le Ministre de la Défense en 2014, qui prévoyait une hausse des budgets pour les programmes d'étude de la DGA – menés en partenariat avec l'ANSSI et l'EMA – ainsi qu'une augmentation des effectifs – le centre DGA - Maîtrise de l'Information, basé à Bruz, devrait par exemple compter plus de 400 ingénieurs cyber d'ici à 2017.

Ensuite avec le Pôle d'excellence cyber créé conjointement par le Ministère de la Défense et le Conseil régional de Bretagne et structuré autour de trois objectifs : la formation, la recherche et le développement économique. Après à peine deux ans d'existence, il peut déjà revendiquer de beaux résultats dans chacun de ces domaines, par exemple la signature d'un accord général de partenariat pour la recherche avec 11 institutions, universités et écoles d'ingénieurs, la publication d'un catalogue unifié de l'offre de formation, la participation à la 17ème édition de la conférence Cryptographic Hardware and Embedded Systems (CHES)…

Enfin, en octobre dernier, le Premier Ministre a annoncé la mise en œuvre de la stratégie nationale de sécurité numérique, qui vise à garantir la sécurité numérique de nos concitoyens à travers 5 objectifs : « garantir la souveraineté nationale, informer le grand public, apporter une réponse forte contre les actes de cybermalveillance, faire de la sécurité numérique un avantage concurrentiel pour les entreprises françaises et renforcer la voix de la France à l'international. »

Cependant, face à l'évolution de la menace, il nous faut franchir une nouvelle étape, notamment pour accélérer une prise de conscience sur les risques cyber. Il apparaît, par exemple, que les Petites et Moyennes Entreprises ont la conviction sincère qu'elles ne sont pas des cibles potentielles. Et aux alertes qui leur sont lancées, elles opposent des interrogations incrédules. Pourtant, selon un rapport de l'ANSSI, 77% des cyberattaques ciblent des petites entreprises.

La nouvelle étape doit donc nous permettre de répondre à ce défi et nous devons faire évoluer les outils créés en ce sens :

■ FORMER

- En Bretagne, le nombre d'étudiants formés aux questions cyber a augmenté de 40%. Il nous faut poursuivre cet effort de formation – en particulier continue – pour sensibiliser les personnels des entreprises. On évalue aujourd'hui à plus de 35% les piratages imputables à une erreur humaine. C'est donc vers l'acquisition de bonnes pratiques qu'il faut tendre pour éviter que les salariés soient le maillon faible de la chaine de sécurité.
- La réserve citoyenne cyberdéfense, qui se structure progressivement, sera également un vecteur important de sensibilisation.

■ PROTÉGER

- Aujourd'hui 76% des RSSI français considèrent « qu'il n'est pas nécessaire de souscrire une cyber assurance ou que celle-ci représente un cout trop élevé ». Nous devons permettre aux entreprises de se prémunir de ces risques.
- Des mesures d'accompagnement à l'international peuvent aussi atténuer leur vulnérabilité.

■ FINANCER

- La structuration du PEC en association loi 1901 lui confère de nouveaux moyens.
- Ainsi 13 grands groupes[1], fournisseurs et clients de solutions cyber, ont annoncé en septembre dernier un investissement de 10 millions d'euros dans la filière sur 5 ans portant le montant global alloué à 30 millions d'euros.

■ DÉVELOPPER

- Les 3 dimensions complémentaires du Pôle Excellence cyber permettent de répondre aux besoins des institutions européennes et internationales et, partant, de développer des partenariats avec l'ONU, l'OTAN, l'UE.
- Nationalement, formation, protection et financement permettront de développer notre Base industrielle et technologique de cybersécurité (BITC) et de mieux répondre aux enjeux de nos PME / PMI.

Le temps est à la mobilisation générale et chaque citoyen-ne doit apporter sa pierre à l'édifice de notre sécurité nationale…

Gwendal ROUILLARD, député du Morbihan,
Secrétaire général de la Commission de la Défense nationale et des Forces armée

[1]Airbus group, Alcatel-Lucent, Atos-Bull, Bertin, Capgemini, Sogeti, DCI, DCNS, EDF, La Poste, Orange, Safran, Sopra Steria et Thalès

Le Premier ministre, lors de son discours du 16 octobre, a annoncé que le gouvernement accélérait le renforcement de la sécurité numérique des infrastructures critiques et a présenté des mesures pour consolider la sécurité des opérateurs, essentiels à l'économie et à ses fonctionnements vitaux. Le Ministère de la Défense, le Ministère de l'Intérieur (en charge de la lutte contre la cybercriminalité) et le Ministère des Affaires Etrangères sont engagés dans ce plan stratégique de grande ampleur, et appuieront les missions de l'ANSSI.

La période de transition numérique que nous vivons favorise la cybercriminalité. Les individus, les administrations et les entreprises de toute taille, dans tous les secteurs d'activité, sont des cibles lucratives. D'une virulence sans précédent, escroqueries, chantages, prises en otage avec rançon ou sabotages augmentent. La France, on l'a vu, est en permanence la cible de cyberattaques portant atteinte à ses intérêts fondamentaux.

LA CONFIANCE S'APPUIE SUR LA SÉCURITÉ

Pour que le numérique reste synonyme de liberté, d'échanges et de croissance, les deux piliers que sont confiance et sécurité sont indispensables. Le vol de données économiques, financières, commerciales, technologiques, politiques, diplomatiques et militaires est un fait criminel qui inquiète les usagers autant que les acteurs économiques et politiques. Leur méfiance est encore renforcée par l'usage immodéré des données personnelles ou la surveillance de masse révélée par Edward Snowden. Il est désormais urgent de changer les pratiques pour développer un écosystème favorable à la confiance numérique.

Dans notre économie mondialisée, les réseaux criminels peuvent coordonner des attaques de grande envergure visant les entreprises ou les organismes publics français depuis n'importe quelle partie du globe. La collaboration opérationnelle entre les autorités nationales, les forces de l'ordre et les acteurs privés est nécessaire pour

INSCRIRE NOTRE ACTION DANS LA STRATEGIE NATIONALE

une protection réelle et dépassant les frontières. Trend Micro contribue déjà à cet effort collectif.

TREND MICRO, UNE EXPERTISE « 3ÈME VOIE » ?

Entreprise japonaise cotée à Tokyo, Trend Micro est génétiquement impliquée dans les démarches de sécurité informatique depuis 27 ans et s'impose aujourd'hui comme un acteur majeur de la cybersécurité.

En Europe, la société collabore avec les autorités policières tant en France qu'en Allemagne, mettant à disposition son expertise, ses outils analytiques et sa connaissance mondiale des menaces. Partenaire historique d'Interpol, Trend Micro travaille également avec Europol et avec la nouvelle Sous-Direction de Lutte contre la Cybercriminalité de la DCPJ créée en France en 2014, apportant savoir-faire technique, support aux formations et informations stratégiques.

Côté Défense, l'atelier des dernières Assises de la Sécurité de Monaco a été illustré par le témoignage du Ministère de la Défense sur « La sécurité du Cloud en environnement contraint » et le choix des technologies Trend Micro.

Sa présence aux événements nationaux majeurs comme les RIAMs*, organisées par Orange Cyberdéfense, son soutien aux travaux des organisations professionnelles telles que le Cesin ou le Clusif, et son action aujourd'hui dans le cadre des Rencontres Parlementaires, font de Trend Micro un acteur de premier plan dans la stratégie nationale pour la sécurité du numérique présentée le 16 octobre par Manuel Valls, Axelle Lemaire et le SGDSN/ANSSI.

Loïc GUEZO
CyberSecurity Strategist SEUR
Trend Micro France

* Rencontres de l'Identité, de l'Audit et du Management de la sécurité

Les acteurs français et étrangers de la cyberdéfense militaire se sont réunis le 24 septembre à Paris lors du colloque « #CyberDef : le combat numérique au cœur des opérations ». Cet évènement inédit a réuni près de 700 personnes, 3 Ministres et une vingtaine de délégations étrangères. Bien plus qu'un lieu de débats et d'échanges, ce colloque a permis d'initier et de renforcer la coopération entre pays partageant les mêmes enjeux dans le domaine de la cyberdéfense militaire. En effet, l'espace numérique, transverse et sans frontières matérielles, ne peut s'appréhender de manière autarcique. La session 2016 sera organisée à Londres par le ministère de la défense britannique, qui prend ainsi le relais de l'initiative française.

La coopération entre membres d'une même coalition est essentielle pour partager de l'information, échanger les bonnes pratiques, se coordonner face à des ennemis communs. La coopération appuie et renforce également notre souveraineté numérique.

Elle permet notamment d'anticiper la menace, d'améliorer nos capacités en bénéficiant d'échanges fructueux, que ce soit dans le cadre d'exercices conjoints, de formations ou encore d'opérations en coalition, mais aussi de mesurer nos forces et ses faiblesses. Grâce à une montée en puissance en termes de moyens financiers, humains et techniques, la cyberdéfense militaire française a acquis des capacités lui permettant de proposer son savoir-faire et son expertise à des pays désireux de développer leurs capacités cyber militaires, notamment au travers du pôle d'excellence Cyberdéfense récemment constitué avec de nombreux partenaires de la société civile (industriels et universités par exemple).

Conforté par les moyens confiés par la Loi de programmation militaire et sa réactualisation, le ministère de la Défense a opéré une réelle montée en puissance depuis 2010. En 5 ans, un commandement opérationnel de cyberdéfense s'est mis en place au sein de l'état-major des armées, étoffant progressivement ses missions, ses ressources humaines et ses capacités.

Un budget de 350 millions d'euros d'équipements, associés à un budget recherche et développement multiplié par 3 et à un recrutement de plus de mille personnes supplémentaires, sont désormais consacrés à la cyberdéfense, enjeu de souveraineté nationale reconnu par le Livre blanc sur la défense et la sécurité nationale de 2013. Un plan stratégique baptisé « Pacte défense Cyber » met l'ensemble des actions et leur gouvernance en perspectives, mobilisant ainsi tous les acteurs du Ministère vers un objectif commun.

CYBERDÉFENSE MILITAIRE : PLACER LE COMBAT NUMÉRIQUE AU CŒUR DES OPÉRATIONS

Du développement de capacités de lutte informatique défensive à celles de la lutte informatique offensive, en passant par le renseignement d'intérêt de cyberdéfense, le ministère de la Défense entend développer sa compréhension et sa maîtrise de l'espace numérique sur son périmètre de responsabilité, les opérations militaires. Cette maîtrise de l'espace numérique s'étend de la couche technique à la couche informationnelle.

L'espace numérique est aussi un domaine d'action militaire où des attributs spécifiques (menaces, tempo, acteurs…) côtoient des modes d'action conventionnels (maîtrise de l'espace, déception, neutralisation…).

C'est un espace pleinement reconnu comme un milieu à part entière au sein duquel les forces armées évoluent, veillent, défendent, neutralisent, encadrées par un cadre juridique clair et protecteur.

L'intégration de la dimension cyber au cœur des opérations militaires est primordiale. Que ce soit à travers la prise en compte de la menace au travers d'une posture défensive ou la mise en place d'opérations cyber en appui d'opérations cinétiques.

Les forces armées agissent face à des menaces de plus en plus diverses et complexes : attaques ciblées de type APT, attaques de faible ampleur visant à perturber, désinformation…

Confrontés à un domaine militaire à la fois unique et transverse, complexe et reprenant les modes d'action cinétique, un personnel compétent et formé constitue un impératif. Ainsi, l'un des axes particuliers d'effort du ministère de la Défense porte sur le développement d'une filière cyber au sein du ministère et sur l'entraînement permanent des forces à travers des formations, des exercices réguliers.

Les exercices DEFNET organisés chaque année permettent notamment de tester nos capacités de cyberdéfense, nos forces et notre organisation de gestion de crise cyber.

Le combat numérique, à travers ses différentes facettes, capacités humaines et techniques, formation, cadre juridique, renseignement… constitue un véritable enjeu pour le ministère de la Défense : protéger les opérations militaires en défendant ses systèmes et ses réseaux, en anticipant et en neutralisant la menace, en exploitant les vulnérabilités des ennemis de façon combinée avec les actions dans les autres milieux. Le combat numérique s'inscrit désormais pleinement au cœur des opérations militaires.

Vice-amiral Arnaud COUSTILLIERE
Officier général Cyberdéfense,
Etat-major des armées,
Ministère de la Défense

DEUXIÈME ÉDITION DU CONCOURS MONDIALE D'INNOVATION : SOUTENIR LES PROJETS INNOVANTS DANS LE DOMAINE CYBER

Fort de son succès, le concours mondial d'innovation, mis en place par le Président de la République en décembre 2013, a lancé sa deuxième édition en septembre 2015 et le cyber fait désormais partie des secteurs technologiques sélectionnées par la Commission innovation 2030. La Commission innovation 2030, présidée par Anne Lauvergeon co anime ce concours, avec la Banque Publique d'Investissement (BPI), qui permet de soutenir des projets innovants à travers des financements publics. L'objectif est de promouvoir les secteurs et les technologies où la France est susceptible d'occuper des positions de leader à l'horizon 2030, en privilégiant les activités qui répondront aux besoins de la société de demain et créeront la plus grande valeur et le plus d'emplois sur le territoire français.

Les 28 lauréats de la première édition ont déjà reçu un soutien à hauteur de 2 millions d'euros maximum. Cette deuxième édition sera tournée vers un nouvel axe : « sécurité collective et protection contre les attaques malveillantes ». En effet, le Président de la République a souhaité que « *le numérique soit au cœur de ce prochain concours* ». Ainsi, cette nouvelle édition permettra aux acteurs du domaine cyber, des grands groupes aux TPE, de présenter leur projet et promouvoir leurs technologies en France et à l'export.

« CHARTES INFORMATIQUES » : ALLIÉES OU FREINS DE LA SÉCURITÉ DES **SYSTÈMES D'INFORMATION** DE L'ENTREPRISE ?[1]

Toutes les études et enquêtes le montrent, les entreprises sont cyber-agressées de toute part, et ce à un rythme toujours plus important. Les tentatives d'intrusion, de vols d'informations sensibles, de chantage ou encore de destruction de l'activité et des outils industriels des entreprises ne se comptent plus, et les exemples d'actions réussies ont un écho médiatique toujours plus important : indisponibilité des sites internet d'entreprises n'ayant pas cédées au chantage, TV5 Monde coupée d'antenne, virus chiffrant les informations des postes de l'entreprise les rendant inaccessibles sauf au prix du payement de rançons en bitcoins, etc.

Face à ces menaces qui deviennent chaque jour plus tangibles et dont le coût se chiffre en milliards d'euros pour les entreprises, il paraît inutile de revenir ici en détail sur la prise de conscience de cette situation par l'Etat, qui a renforcé fortement les forces et les pouvoirs de l'ANSSI ou encore fait adopter plusieurs textes élargissant le champ des infractions et renforçant les peines théoriquement applicables aux actes de cybercriminalité[2]. La prise de conscience est identique au niveau de l'Union européenne, qui intègre la problématique de manière transversale dans tous les nouveaux textes (directive « cybercrime » du 2013/40/UE, projet de directive « sécurité des réseaux et de l'information », etc.).

Les entreprises se sont quant à elles dotées d'outils, de matériels, de logiciels ou encore de cellules spécialisées et de processus organisationnels internes de nature à leur permettre de protéger leurs systèmes d'information. Les enjeux sont de taille. En effet, outre les risques précédemment évoqués, certains textes précédemment mentionnés mettent à leur charge des obligations de sécurité renforcées assorties de très fortes sanctions et la Cour de cassation a opéré un virage à 180° de sa jurisprudence le 19 mars 2014 pour diminuer le droit à réparation du préjudice de la victime à partir du moment où celle-ci n'aurait pas suffisamment sécurisé son système d'information.

La réalité est toutefois connue de tous : la cybersécurité ne peut, comme dans bien d'autres domaines, être efficace à 100 %, et tout l'enjeu devient donc de mettre en place les moyens d'identifier le plus rapidement les incidents de sécurité, de limiter les surfaces d'attaque et de s'organiser pour y répondre de la façon la plus efficace possible.

Face à cette réalité, l'entreprise doit pouvoir s'appuyer sur ses salariés et collaborateurs qu'elle aura tout particulièrement sensibilisés à cette problématique. Or, comme la stratégie nationale pour la sécurité numérique le précise, les pertes et cyber-risques peuvent aussi être causés par « *le comportement dangereux (...) d'un salarié mélangeant sans précaution vie privée et vie professionnelle* ».

En pratique, nombre d'incidents de sécurité permettent ainsi de remonter, lors des investigations internes, vers le compte attribué à un salarié sur le système d'information de l'employeur. Que celui-ci l'ait réellement utilisé pour commettre un abus sur le système ou que son compte ait été utilisé par un tiers à son préjudice, la problématique est in fine relativement semblable : quel est niveau de contrôle que peut opérer l'employeur sur son salarié grâce aux enregistrements de son système d'information ? Et peut-il effectivement le sanctionner ?

Si ces questions ne se posent qu'à ce moment pour l'entreprise, cela signifie que c'est en réalité déjà trop tard !

Les réponses doivent figurer dans une « charte » dédiée à l'usage du système d'information de l'employeur qui devra être annexée au règlement intérieur et donc avoir fait l'objet de formalités **préalables** à cette occasion (consultation des représentants du personnel, etc.) tout comme auprès de la CNIL (déclaration ou inscription au formulaire du CIL interne s'il existe). Cette inclusion dans le règlement intérieur permet l'opposabilité sans discussion aux salariés, ce qui ne sera pas le cas de la Politique de Sécurité des Systèmes d'Information (PSSI) et autres documents similaires.

Pourtant, ce passage devant les institutions représentatives du personnel, n'étant pas effectué par les personnels dédiés à la sécurité des systèmes d'information de l'entreprise, il est souvent l'occasion de concessions sociales qui n'ont rien de purement rédactionnel et qui sont souvent en opposition complète avec ce que prévoient, si ce n'est la PSSI, du moins les règles basiques de sécurité des systèmes d'information.

Certes, il est évident que la sécurité ne doit pas être l'excuse de l'employeur pour procéder au « flicage » de ses salariés. Mais rassurons-nous, les magistrats y veillent déjà tout particulièrement, et depuis longtemps.

Par contre, ils reconnaissent également la nécessité pour l'employeur d'agir, pour des raisons objectives et particulières de sécurité, sur tous les contenus (fichiers, messages, SMS, etc.), quelle que soit leur nature professionnelle ou extra-professionnelle. Car après tout, l'employeur est tenu de protéger ses données, les données de ses clients ou les données de ses salariés. Le fait que l'employeur accorde un usage privé de son système d'information ne doit pas, dans un retournement de situation kafkaïen, conduire à ce qu'il perde la maîtrise de la sécurité de pans entiers de son infrastructure !

Les chartes ont la particularité d'avoir donné lieu à une quantité très importante de décision ces dernières années, nécessitant d'avoir une vision d'ensemble (elles s'incluent dans l'écosystème des règles de gestion de l'information dans l'entreprise) et en même temps une connaissance très précise des principes posés par les magistrats pour réaliser une véritable cybersécurité « de bout en bout ».

Rappelons en effet que, selon le principe de faveur, si l'employeur s'est limité voire interdit dans son règlement intérieur un type de contrôle (les messages privés de son salarié), c'est ce principe qui trouvera à s'appliquer, indépendamment de la jurisprudence sur le sujet.

Prêter attention à la rédaction précise de ce document est essentiel, car lui seul permet en pratique les contrôles inhérents à la sécurité des systèmes d'information de l'entreprise. Mais suivre l'actualité et agir en conséquence l'est tout autant.

A ce titre, il nous semble essentiel, pour conclure, de mentionner l'article 30 du projet de loi « pour une république numérique ». Prévu pour restreindre l'utilisation par les entreprises offrant des services de messagerie électronique des contenus des messages des utilisateurs, **il ne faudrait pas que ce texte puisse être interprété comme empêchant les entreprises de mettre en place les filtres nécessaires sur les messageries électroniques des salariés visant à empêcher, par exemple, les fuites d'informations confidentielles** (de type *Data Leak Prevention*). Là encore, les magistrats de la Cour de cassation ont posé les règles et permis de tels contrôles pour permettre à l'entreprise d'assurer la protection de son patrimoine informationnel : ne détruisons pas cet équilibre !

François COUPEZ
Avocat à la Cour
Atipic Avocat

[1] Le présent article a été rédigé avant les terribles attentats qui ont endeuillé notre capitale. Toutes nos pensées vont aux victimes, à leurs familles, ainsi qu'aux forces de l'ordre, aux secours et à tous ceux qui ont porté assistance, qui ont ainsi permis, par leurs efforts et leur dévouement, à réduire le nombre de victimes. Fluctuat nec mergitur.

[2] Par la loi du 24 juillet 2015 relative au renseignement

LA NOUVELLE « *RECOMMANDATION DE L'OCDE SUR LA GESTION DU RISQUE DE SÉCURITÉ NUMÉRIQUE* »[1] POSE LES BASES D'UNE APPROCHE DE LA « CYBERSÉCURITÉ » CENTRÉE SUR LA PROSPÉRITÉ ÉCONOMIQUE ET SOCIALE, TANT POUR LES ORGANISATIONS QUE POUR LE DÉVELOPPEMENT DES POLITIQUES PUBLIQUES.

Les technologies de l'information apportent des bénéfices économiques et sociaux considérables, par exemple en termes d'innovation, de gain de productivité et de compétitivité des entreprises, ainsi qu'en matière d'éducation, de santé et de participation démocratique.

En quelques années, l'environnement numérique, et en particulier Internet, est devenu indispensable au développement et au fonctionnement de nos économies. Cependant, son utilisation introduit aussi des incertitudes, et en particulier expose à des menaces de sécurité numérique de plus en plus sophistiquées et à des incidents de plus en plus fréquents.

Dysfonctionnement des opérations, pertes financières, atteinte à la réputation, perte de compétitivité, poursuites judiciaires, perte de confiance des clients, employés, actionnaires et partenaires : de nombreux exemples récents illustrent les conséquences économiques désastreuses que de tels incidents peuvent avoir pour les organisations et pour les individus.

Les incidents sont parfois spectaculaires, comme l'interruption des programmes de TV5Monde pendant plusieurs heures, et les « dégâts physiques massifs » dans une installation industrielle en Allemagne[2]. Certains ont marqué les esprits par leur ampleur, comme le vol de plus de 22 millions de dossiers de fonctionnaires du gouvernement américain[3], de millions de données dans le système de pension Japonais[4] et dans de grandes banques Coréennes[5], ainsi que la fraude à grande échelle dans la chaine de distribution Target aux États-Unis, ou encore l'intrusion dans le système de Sony Pictures Entertainement et la divulgation de dizaines de milliers d'emails internes[6].

Ces incidents ont montré qu'aucune organisation n'est à l'abri et que partout où un dispositif ou processus repose sur le numérique, un risque de sécurité existe, qui peut nuire à la vie privée des individus, mais aussi aux activités des organisations, et qui peut impacter les installations physiques parfois critiques (par ex. énergie, chimie, etc), et même dans certains cas, la vie humaine (ex. hôpitaux, transports).

Ces exemples frappants ne devraient pas masquer les myriades d'incidents moins connus touchant des PME et des individus et ceux qui n'ont jamais été déclarés pour ne pas dégrader l'image de leurs victimes.

En provoquant la démission de certains dirigeants de grandes entreprises (Sony Pictures[7], Target[8], banques Coréennes[9]) et organisations publiques (Office of Personnel Management[10]), ces incidents ont mis en relief le caractère économique et stratégique du problème, au-delà de sa dimension médiatique, juridique et technique.

Ils illustrent la nécessité d'une nouvelle approche fondée sur la reconnaissance que le risque de sécurité numérique est un risque économique et pas seulement technique et de surcroît pour les États, un risque de sécurité nationale et internationale.

Avec sa nouvelle *Recommandation sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale*, l'OCDE appelle les dirigeants et décideurs à prendre leur part de responsabilité dans la gestion de ce risque.

POUR L'OCDE, LE RISQUE DE SÉCURITÉ NUMÉRIQUE EST ÉCONOMIQUE ET SOCIAL

Avec son Document d'accompagnement, la Recommandation rappelle qu'il est impossible de créer un environnement numérique entièrement sûr et sécurisé, où le risque serait entièrement évité, sans renoncer aux bénéfices économiques et sociaux associés à l'ouverture, l'interconnectivité, et au dynamisme de cet environnement. En conséquence, la Recommandation prône la gestion du risque, c'est-à-dire sa réduction à un niveau acceptable, déterminé selon le contexte et les objectives économiques et sociaux en jeu.

A la différence d'une approche purement technique ou centrée sur un objectif isolé de sécurité absolue, la gestion du risque de sécurité numérique permet la sélection de mesures de sécurité appropriées et proportionnées qui ne nuisent ni aux activités économiques qu'elles visent à protéger, ni aux intérêts légitimes d'autrui.

La gestion de ce risque est aussi stratégique que la décision d'utiliser le numérique pour augmenter la compétitivité, améliorer les services, ou faire des économies. Pour l'OCDE, les dirigeants et les décideurs en charge de la réalisation des objectifs économiques sont donc les mieux placés pour fixer les orientations nécessaires pour réduire le risque de sécurité numérique à un niveau acceptable.

Destinée aux dirigeants et décideurs, ainsi qu'à ceux qui les conseillent, la Recommandation brise le mythe d'un monde de la « cybersécurité » qui relève avant tout de la compétence d'experts dont l'action n'est pas forcément en phase avec la réalité et les besoins du métier.

Le risque numérique est un risque comme les autres, et sa gestion doit donc s'insérer dans le cadre plus large de la gestion du risque de l'organisation. Intégrer le risque numérique à la prise de décision économique permet une direction plus stratégique, plus agile et plus efficace de l'organisation. Ceci requiert une coopération accrue entre les composantes métiers et les professionnels des TIC en charge de la conception et de la mise en œuvre de l'environnement numérique.

La Recommandation et son document d'accompagnement clarifient les concepts de risque et de gestion de risque, souvent mal compris. Elle contient huit principes qui permettent aux organisations de développer une politique efficace et cohérente avec les normes opérationnelles de gestion de risque. Elle contient également des recommandations de politique publique pour le développement de stratégies nationales équilibrées et visant à soutenir pleinement l'utilisation du numérique pour la prospérité économique et sociale.

Adoptée après plus de deux ans de discussion entre les représentants des gouvernements, des entreprises, de la société civile et de la communauté technique de l'Internet, elle constitue la troisième génération de Recommandations de l'OCDE sur cette question depuis 1992, et forme, avec les Lignes directrices sur la protection de la vie privée de 1980, révisées en 2013, la base du cadre de l'OCDE pour la confiance dans l'économie numérique.

Laurent BERNAT
Administrateur à la Division des Politiques de l'Economie Numérique
OCDE

[1] OECD, (2015). « Gestion du risqué de sécurité numérique pour la prospérité économique et sociale. Recommandation de l'OCDE et Document d'accompagnement ». http://oe.cd/dsrm-fr
[2] "Hack attack causes 'massive damage' at steel works" www.bbc.com/news/technology-30575104
[3] E. Nakashima (2015), "Hacks of OPM databases compromised 22.1 million people, federal authorities say". www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/
[4] Abel R. (2015), "Japan's national pension fund breach affects 1.25M". www.scmagazine.com/japan-pension-funds-experiences-second-incident-in-less-than-eight-years/article/417985/
[5] Yan, S., Kwon K.J (2014), "Massive data theft hits 40% of South Koreans", http://money.cnn.com/2014/01/21/technology/korea-data-hack/.
[6] Arce, N. (2015), "WikiLeaks Dumps 270,000 Sony Emails, Private Files, Financial Data Into Its Database", www.techtimes.com/articles/62148/20150620/wikileaks-dumps-270-000-sony-emails-private-files-financial-data-into-its-database.htm.
[7] Faughnder, R (2015), "Sony co-chair Amy Pascal steps down after hacking scandal" www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-amy-pascal-stepping-down-20150205-story.html
[8] Riley, M. (2014), "As Data Breach Woes Continue, Target's CEO Resigns" www.bloomberg.com/bw/articles/2014-05-05/as-data-breach-woes-continue-targets-ceo-resigns.
[9] Eha, B. (2014), « 37 South Korean Bank Execs Offer to Resign Over Breach. Should Target Execs Follow Suit? », www.entrepreneur.com/article/230980
[10] Rein, L., Davidson J. (2015), "OPM Director Katherine Archuleta resigns under pressure". www.washingtonpost.com/news/federal-eye/wp/2015/07/10/auto-draft/.

LE RÔLE DE LA BEFTI DANS LE CADRE DES PABX

Créée en 1994, la Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information de la Direction de la Police Judiciaire de la Préfecture de Police de PARIS exerce ses attributions dans le ressort des Tribunaux de Grande Instance de PARIS et de la petite couronne. Elle traite une délinquance complexe, aux conséquences fortement dommageables et procède à des investigations classiques et à des exploitations techniques.

Compétente pour les infractions portant atteinte aux Systèmes de Traitement Automatisé de Données(STAD), elle enquête sur les piratages de commutateurs, appelés génériquement PABX ou IPBX.

Le constat de l'augmentation des préjudices causés par ces piratages l'amène à sensibiliser les professionnels de la sécurité, notamment au sein du Club des Directeurs de Sécurité (CDSE) et de la Fédération des Entreprises du Bureau et du Numérique (EBEN).

Que signifient PABX, IPBX et PABX IP ?

▸ **Private Automatic Branch eXchange** : c'est un commutateur téléphonique dont les circuits sont numériques et sur lequel sont raccordés des postes numériques et des terminaux analogiques

▸ **Internet Protocol Branch eXchange** : c'est l'équivalent d'un PABX, mais utilisé dans un réseau IP et sur lequel sont raccordés des soft-phones et des postes IP

▸ **PABX IP** : système hybride sur lequel on peut raccorder tous les types de postes

Qu'est-ce qu'un piratage de PABX ?

Lorsque l'on écarte le comportement d'un employé qui utilise une ligne téléphonique pour appeler des proches à l'étranger ou des sites surtaxés de jeux en ligne, c'est, le plus souvent, une intrusion au sein d'un commutateur qui permet à son auteur de

- de nuire
- d'espionner
- ou de réaliser une escroquerie dite **phreaking**. Dans cette hypothèse, de nombreux appels surtaxés sont enregistrés à destination de pays étrangers. Les faits se déroulent la nuit, le week-end et les jours fériés.

Pour certaines victimes, le préjudice peut dépasser plusieurs dizaines de milliers d'euros.

Comment s'en protéger ?

L'anticipation et l'application de conseils simples peuvent limiter ces infractions :

- la suppression de mots de passe trop simples tels que 0000 ou 1234 et des mots de passe du constructeur installés par défaut
- le paramétrage des fonctionnalités du commutateur adapté aux besoins de chaque poste et notamment la limitation des appels internationaux, des appels surtaxés, des renvois d'appels et de la messagerie vocale
- la surveillance ou le monitoring par le propriétaire du système et/ou l'info gérant
- des mises à jours régulières des systèmes et de leurs paramétrages

Dans un contexte de maîtrise des dépenses budgétaires, ces conseils présentent l'avantage de ne pas engendrer de coûts supplémentaires.

Qui peut apporter une aide ?

• les installateurs et info-gérants

Le 25 mars 2014, la Cour d'Appel de VERSAILLES a jugé que le défaut de sensibilisation d'un client par le prestataire de maintenance constituait une faute *(en l'espèce, le mot de passe programmé en usine par défaut n'avait pas été changé depuis plusieurs années)*. La jurisprudence attribue à l'utilisateur la responsabilité de gérer la sécurité de son matériel directement ou en la confiant à un prestataire, mais oblige les installateurs et/ou les sociétés de maintenance à informer le client sur cette nécessité et à lui montrer comment procéder.

Les installateurs sérieux d'autocommutateurs assurant cet accompagnement et proposant des contrats de service peuvent s'enorgueillir de ne compter aucune victime parmi leur clientèle.

• les fournisseurs de téléphonie

Des outils de détection de flux existent. En cas de pics inhabituels, ils permettent aux opérateurs d'émettre des alertes auprès de leurs clients. Certains les en avisent et interrompent immédiatement toutes les communications, ce qui permet de limiter considérablement le montant des factures de téléphonie en cas de fraude.

Il est conseillé de faire le point avec son opérateur et de solliciter ce type de réaction immédiate.

Que faire en cas de fraude ?

- Conserver et protéger les journaux d'activité du système
- Déposer plainte auprès du commissariat ou de la gendarmerie

Sylvie SANCHIS
Chef de la BEFTI
Préfecture de Police de Paris

LES CONDITIONS D'APPLICATION DU DISPOSITIVE RAPID ET SES EFFETS

Depuis 2009, le régime d'appui pour l'innovation duale (RAPID) permet aux PME de soumettre spontanément leurs projets technologiques innovants présentant des applications sur les marchés militaires ainsi que des retombées sur les marchés civils. Ce dispositif à fort impact compétitif, qui a été étendu aux entreprises de taille intermédiaire, est mis en œuvre par la DGA conjointement avec le ministère chargé de l'industrie. Dans le cadre du pacte Défense-PME, et afin de renforcer l'accès de ces entreprises aux futurs marchés de défense et de promouvoir leur compétitivité, les crédits consacrés au dispositif RAPID seront de 50 M€ en 2016, comme en 2015, en hausse de 25% par rapport à 2013. Ce dispositif qui permet de financer des projets proposés par des industriels sur des technologies duales est parfaitement adapté au soutien des PME qui souhaitent innover dans le domaine de la cyberdéfense.

Les entreprises pouvant bénéficier du dispositif

Seule ou en consortium avec une entreprise ou un organisme de recherche, toute PME autonome de moins de 250 salariés ou toute entreprise de taille intermédiaire (ETI) autonome de moins de 2 000 salariés peut faire acte de candidature spontanée, pour bénéficier d'une subvention « RAPID ». Le dispositif est conçu pour être extrêmement réactif afin d'accorder un financement des projets sélectionnés par la DGA dans un délai maximum de quatre mois entre le dépôt du dossier et le début des travaux.

Bilan positif et perspectives

Sur les deux dernières années, c'est 12 projets dans le domaine de la cyberdéfense qui ont ainsi été soutenus pour un montant global de 6 millions d'euros avec des retours extrêmement positifs de la part des PME sur l'efficacité du dispositif. Ces projets concernent autant la conception de produits de sécurité innovants comme des sondes de détection d'intrusion ou des produits de visualisation que des outils métiers permettant de tester automatiquement un logiciel ou de détecter les erreurs dans du code. Ces produits restent toutefois très orientés « informatique traditionnelle » et tirent insuffisamment parti des spécificités liées à chaque métier. La DGA au travers de ses projets de S&T a lancé des travaux d'ensemble, comme par exemple la sécurisation des plates-formes navales et va poursuivre cette démarche sur les grandes systèmes militaires mais ce type d'approche qui intéresse autant le domaine militaire que civil pourrait tout à fait faire partie des sujets proposés par des PME dans le cadre de ce dispositif.

ICA Frédéric VALETTE
Responsable du pôle sécurité
des systems d'information
DGA

SÉCURITÉ ET "INSÉCURITÉ ÉCONOMIQUE" DANS LES ENTREPRISES : ÉTAT DES LIEUX ET PISTES DE RÉFLEXION

Si je pouvais m'en passer...

Depuis 12 ans, **l'Enquête sur les pratiques de Veille et d'Intelligence économique (IE) des entreprises bretonnes** a pour objet d'analyser les pratiques de ces dernières dans le domaine de l'IE et ses trois volets : veille, sécurité et influence. Pour sa 8ème édition, les CCI de France ont étendu cette consultation de la Bretagne aux régions Normandie, Bourgogne, Centre et Rhône-Alpes. Les TPE/PME constituaient la grande majorité des répondants. Les premiers résultats se sont avérés comparables dans les régions représentées et se recoupent avec d'autres enquêtes menées en 2015 par les CCI.

Premier enseignement, en termes de pratique : 83% des entreprises considèrent comme importante, voire très importante la recherche d'information, contre 72% pour la protection de l'information et 66% pour l'influence. Tendance confirmée par **la 4ème édition du "Zoom sur l'IE" publié par la CCI de la Drôme en janvier 2015,** centrée sur les entreprises à caractère industrie: sur les sujets d'ateliers demandés par les entreprises, la SSI arrivait en 3ème position (25%), derrière la structuration d'un système d'informations (34%) et la veille (29%).

Second enseignement: seules 44% des entreprises ont une démarche de sécurisation. Une situation fragile car ce choix demeure contraint puisque découlant d'abord d'une fuite d'information (49%), par obligation (44%) après avoir été confrontées à une cyberattaque (26%)... les suites d'une sensibilisation ne concernant que 27% d'entre elles. Même constat lors de **l'étude sur les pratiques et usages du numérique dans les PME/TPE publiée par la CCI de Lyon en septembre 2015** : en termes de préoccupations par rapport au numérique, si 57% environ des TPE/PME souhaitent améliorer leur sécurité informatique, la priorité demeure la visibilité sur internet, l'adaptabilité ou encore la mobilité.

La sécurité ne constitue donc pas une priorité pour une majorité de TPE/PME. Non pas qu'elles s'en désintéressent. Cependant, s'il fallait user d'un discours imagé, l'attitude générale après une sensibilisation à la sécurité économique semble se rapprocher de celle qui suit la vision d'un (bon) film d'horreur : appréhension sur le moment, sommeil perturbé, vie qui reprend son cours le lendemain avec le sentiment rassurant de la faible la probabilité de rencontrer un serial-killer... au final, de la sensibilisation ne nait pas un sentiment "d'insécurité économique".

INSÉCURITÉ ÉCONOMIQUE ?

En effet, si la notion "d'insécurité économique" est parfois **utilisée par les acteurs de la sécurité économique** au sens de menaces sur l'entreprise et d'ingérence, elle ne renvoie pas aux même notions pour le grand public ou les politiques, qui l'assimilent au chômage, à l'instabilité administrative, aux délais de paiement, aux manque de fiabilité des fournisseurs, aux aléas de la mondialisation... bref, "l'insécurité économique" est d'avantage associée à la précarité qu'à la malveillance. Ce qui est exactement l'inverse du sentiment d'insécurité dans notre vie quotidienne...

Dès lors, sauf à démultiplier les piqures de rappel, attendre la prise de conscience une fois que l'entreprise est victime, ou encore "précariser" les auteurs de négligence dans l'entreprise, comment faire naitre un "sentiment persistant" d'insécurité économique amenant chacun à se sentir responsable de la protection de son organisation au quotidien ?

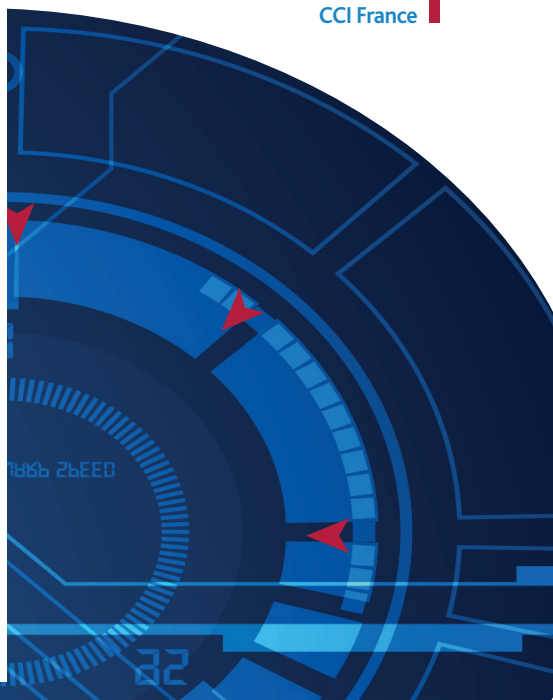
Plusieurs pistes sont à l'étude. La première est de substituer au discours de sécurisation un discours de gestion du risque. C'est l'option choisie par l'OCDE et ses recommandations publiées en novembre 2015 sur "**La gestion du risque de sécurité numérique pour la prospérité économique et sociale**".

Une autre serait d'abandonner l'angle de vue agresseur/agressé, au profit d'une vision de type "business model" : l'auteur de malveillances n'est pas "méchant", il obéit à un business model dont je suis hélas le produit. Une fois compris ce fonctionnement, il ne tient qu'à moi de décider d'être un produit rentable ou non... et à mon détriment. Cette approche "business model" est notamment utilisée par le business game de sensibilisation ***Cyberstategia***, de la Réserve citoyenne cyberdéfense.

Une dernière piste: s'adresser directement à l'imaginaire des employés et dirigeants. Les rendre, de manière ludique, acteurs de la politique de sécurité économique de l'entreprise. Cette piste, CCI France la suit en travaillant sur les "serious games", "jeux sérieux" qui associent une intention "sérieuse" à des ressorts vidéoludiques permettant d'impliquer le joueur dans une thématique donnée, pour créer ce "sentiment persistant". ***Info-Sentinel*** de Getzem, meilleur "Learning Game" d'Europe en 2014, ***Keep it safe*** et ***Mr Travel*** de LayerCake, ***CCI Intelligence Economique*** de la CCI Normandie avec 6 scénettes dédiées à la sécurité économique, ou encore ***Jeu d'influences*** de France 5 sur la gestion de crise médiatique, mais aussi ***2025 exmachina***, pour l'éducation critique à Internet des 12-16 ans... la France est aujourd'hui particulièrement avancée dans le domaine des sérious games en sécurité économique.

Autant de pistes afin de transformer des spectateurs apeurés en acteurs impliqués. Ils vivront alors la sécurité non comme une contrainte, mais comme un facteur de compétitivité et de prospérité de leur organisation, dont ils seront les premiers bénéficiaires.

Thibault RENARD
Responsable intelligence économique
CCI France



CYBERCERCLE

Le club de réflexion sur la sécurité numérique
sous dynamique parlementaire

Rejoignez le CyberCercle

Un cadre privilégié d'accès à l'expertise, d'échanges et de rencontres sur les questions de sécurité numérique

Petits déjeuners débats
Des matinales thématiques
en présence d'experts et de parlementaires

Rencontres Parlementaires de la Cybersécurité
Le rendez-vous institutionnel annuel de la communauté française de la cybersécurité et du numérique

Rencontres Régionales de la Cybersécurité
Des journées d'information
ancrées dans une dynamique locale

Cybersécurité & Parlement
La lettre d'information parlementaire
qui donne la parole aux spécialistes

Rencontres Parlementaires
Cybersécurité & milieu maritime
Une demie-journée d'échanges réunissant les institutionnels français de la cybersécurité et du milieu maritime

CyberCercle Formation
L'offre de formation en droit, management, organisation et gestion de crise sur la cybersécurité

LES FORMATIONS DU CYBERCERCLE

SÉCURITÉ NUMÉRIQUE ET CADRE JURIDIQUE

SMETCJ-1
1 JOURNÉE

Droit de la sécurité des systèmes d'information : point de situation sur les nouvelles règles et évolutions prévisibles

PUBLICS :
Dir. PME-PMI | Dir. juridique | DSI | RSSI

SMETCJ-2
1 JOURNÉE

Protection des données personnelles : de qui parle t'on ? Etat de l'art et règlement européen à venir : se préparer

PUBLICS :
Dir. PME-PMI | Dir. info PME-PMI | DSI | Dir. juridique | Dir. RH | Dir. marketing

SMETCJ-3
1 JOURNÉE

Le RSSI face à ses obligations juridiques

PUBLICS :
Dir. info PME-PMI | Dir. juridique | RSSI

SMETCJ-4
1 À 2 JOURNÉE

Les enjeux de la cybervigilance de l'employeur sur ses collaborateurs : comment se protéger des risques internes ?

PUBLICS :
Dir. info PME-PMI | Dir. juridique | Dir. RH

SMETCJ-5
1 JOURNÉE

Le SystAdmin et le droit : que peut-il faire ? Jusqu'où ne doit-il pas aller ?

PUBLICS :
Dir. juridique | DSI | RSSI | Dir. info PME-PMI

SMETCJ-6
1 JOURNÉE

Failles de sécurité : qu'impose le droit ? Comment réagir ?

PUBLICS :
Dir. info PME-PMI | Dir. juridique | DSI | RSSI

SMETCJ-7
1 JOURNÉE

Agir ou réagir sur les médias et réseaux sociaux : quelles règles juridiques ?

PUBLICS :
Dir. PME-PMI | Dir. communication | Dir. marketing | Dir. juridique

SMETCJ-8
1/2 JOURNÉE

Agir ou réagir sur les médias et réseaux sociaux : quelles règles juridiques ?

PUBLICS :
Dir. PME-PMI | Dir. info PME-PMI | RDI | RSSI

Les formateurs de CyberCercle-Formation sont tous des professionnels, spécialistes de la cybersécurité, que ce soit en termes organisationnels, de gestion de crise ou juridiques, et dotés de qualités de pédadogues qui leur permettent de transmettre leurs savoirs de façon efficiente, en adaptation avec leur auditoire.

Des représentants des institutions viendront également apporter un éclairage sur des sujets définis, permettant aux participants un accès à une expertise particulière et un échange personnalisé.

Les modules de formation ont volontairement des formats courts, d'une ou de deux journées, afin d'éviter de peser trop lourdement sur les agendas. Ils se déroulent au coeur de Paris, dans un lieu facile d'accès par les transports en commun.

SÉCURITÉ NUMÉRIQUE 360°

SM360-1
Transformation numérique et cybersécurité - panorama de la situation et des enjeux

PUBLICS : 1 JOURNÉE
Dirigeants de PME-PMI et cadres dirigeants

SM360-2
Assumer le risque numérique pour une meilleure compétitivité de l'entreprise

PUBLICS : 1 JOURNÉE
Dirigeants de PME-PMI et cadres dirigeants

SM360-3
Quelle politique de l'Etat en matière de cybersécurité ? Quels impacts pour l'entreprise ?

PUBLICS : 1 JOURNÉE
Dirigeants de PME-PMI et cadres dirigeants

SM360-4
Gérer le risque numérique pour optimiser la sécurité de son travail

PUBLICS : 1 JOURNÉE
Dirigeants de PME-PMI et cadres dirigeants

Tél. : 09 83 04 05 37 ● Courriel : contact@cybercercle.com ● Site Internet : www.cybercercle.com

UN SITE INTERNET DE RÉFÉRENCE ET DES RÉSEAUX SOCIAUX ACTIFS

Parallèlement à l'activité menée sur son site internet, le CyberCercle diffuse quotidiennement l'actualité du milieu du numérique par le biais de son compte Twitter. Vous pourrez également y retrouver : des live-tweets à l'occasion des Rencontres et des petits déjeuners débats, des photos, des relais vers des articles rédigés par des experts pour le CyberCercle...

Le CyberCercle sur Twitter*, c'est :
- @CyberCercle
- 1900 abonnés
- 60 mentions @CyberCercle par jour
- des tweets quotidiens et du relai d'information sur l'actualité du secteur du numérique

Notre chaîne YouTube* dédiée :
- 53 vidéos en ligne
- près de 5 000 vues
- les interviews « une question à »
- les CyberTalk
- les vidéos bilan des Rencontres Parlementaires

*Fin 2015

CYBERCERCLE
7, rue Casteja - 92100 Boulogne
Tél. : 09 83 04 05 37
contact@cybercercle.com
www.cyberclercle.com

Cybersécurité & Parlement est édité par le CyberCercle
Directeur de la publication : Bénédicte PILLIET
CyberCercle – 7, rue Casteja - 92100 Boulogne – Tél. : 09 83 04 05 37
contact@cybercercle.com – www.cybercercle.com