7e FORUM INTERNATIONAL DE LA CYBERSÉCURITÉ

Le cyberespace, enjeu de souveraineté et de sécurité

FIC 2015

LES ACTES DU FORUM

AVEC LA COLLABORATION DU CENTRE DE RECHERCHE DE L'ÉCOLE DES OFFICIERS DE LA GENDARMERIE NATIONALE

Mot d'accueil

M. Pierre de SAINTIGNON

Mesdames, Messieurs,

Permettez-moi d'abord de saluer :

Mon cher Général Watin Augouard, sans qui le FIC n'existerait pas !
Notre Cher Préfet Rémy Pautrat, qui contribue aussi au succès de ce Forum,
Monsieur Darason, Président de CEIS, qui co-organise avec la Gendarmerie Nationale ce Forum et que je remercie.
Vous souhaitez d'abord la Bienvenue à Lille, Capitale historique des Flandres et de la Région Nord Pas de Calais, mais surtout, aujourd'hui plus que jamais, Capitale Européenne et Mondiale de la Cybersécurité et de la Confiance Numérique à l'occasion de ce Forum international de la cybersécurité.
Je vous remercie tous très chaleureusement de votre présence si

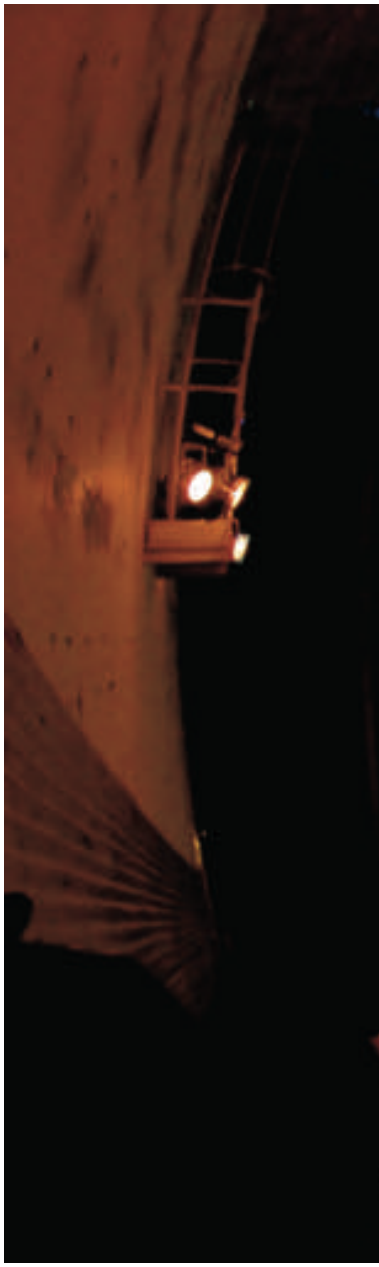
nombreuse aujourd'hui.
Vous êtes plus de 4500 participants, décideurs économiques, universitaires, chercheurs et collectivités représentant 73 nationalités.
Pendant ces deux jours, nous écouterons plus de 320 intervenants de très haut niveau lors des 4 séances plénières, 17 conférences et 20 plateaux TV organisés.
Nous avons également 120 exposants pour animer ce forum avec 140 partenaires publics et privés.
Ce très grand succès de participation augure bien d'ores et déjà de l'intérêt et du haut niveau de cette manifestation.
Nous aurons l'honneur de recevoir :

. Monsieur Bernard CAZENEUVE, Ministre de l'Intérieur,
. Monsieur Jean-Yves LE DRIAN, Ministre de la Défense,
. Madame Axelle LEMAIRE, Secrétaire d'Etat au numérique
. Monsieur Thomas de MAIZIERE Ministère de l'Intérieur de la République Fédérale d'Allemagne

Je souhaite dès à présent à chacun d'entre vous d'excellents travaux au cours de ces deux jours.

Je salue à nouveau le partenariat exemplaire entre le Conseil régional, la Gendarmerie nationale, CEIS, la SPL « Euratechnologies » et la Mission Lille Eurométropole Défense Sécurité.
Je suis heureux que ce partenariat puisse se concrétiser désormais au travers d'une déclaration d'intention entre la Gendarmerie Nationale, CEIS et le Conseil régional, qui renouvelle notre collaboration jusqu'en 2018, et, pour ma part, j'espère bien au-delà !
Le soutien de la Région témoigne de la grande ambition qui m'anime pour conforter le Nord Pas de Calais en tant que référence mondiale en matière de cybersécurité.
C'est une ambition partagée par l'ensemble des acteurs économiques et sociaux de notre région : je rappelle que le Forum International Cybersécurité est partie intégrante de notre Schéma Régional de Développement Economique et de notre Stratégie Régionale d'Intelligence Economique.
Lille est au premier plan des villes européennes, au cœur de l'Europe.
La Région Nord Pas de Calais est la 4ème Région économique de France.
En dépit d'une crise sévère qui continue à frapper fort les salariés et les entreprises, notre région comble peu à peu ses retards et ses handicaps par une politique de développement économique ambitieuse, basée sur l'innovation, la formation professionnelle, l'attractivité de son territoire et sa large ouverture à l'international.
On ne peut pas parler de développement économique sans parler de protection de nos entreprises, d'intelligence économique et donc de cybersécurité et de confiance numérique.
On ne peut pas parler de développement de nouvelles technologies sans parler de protection des données stratégiques si essentielles à notre compétitivité et à notre intelligence collective.
Les cyber-menaces qui nous entourent nous obligent à une capacité d'anticipation et des moyens de riposte. L'année 2014 et ce début d'année 2015 nous l'ont malheureusement que trop montré (piratage de Sony, piratage de données personnelles et bancaires nuisant à la réputation de grands groupes…).
Comme toutes les technologies, celles de l'information et de la communication sont ambivalentes.
Elles offrent des possibilités quasi-infinies en termes d'échanges d'informations, de savoirs, de développement économique et culturel, mais elles posent aussi un grand nombre de problèmes politiques, juridiques, éthiques, sociaux et sociétaux.
C'est la culture de la confiance numérique que nous voulons diffuser, et l'organisation de ce Forum international Cybercriminalité à Lille en est une illustration majeure.
C'est aussi pour toutes ces raisons que le Conseil régional Nord Pas de Calais a confié à Eura-

technologies la création d'un cluster CYBERSECURITE et CONFIANCE NUMERIQUE dont l'ambition est de fédérer l'ensemble des acteurs euro-régionaux autour d'une ambition commune : comprendre les enjeux de la cybersécurité et trouver des leviers de croissance économique grâce à cette thématique.
Depuis un an maintenant, toutes les compétences locales se sont regroupées et travaillent ensemble pour soutenir l'innovation et le développement des compétences de chacun dans le domaine.
Le Cluster accompagne le développement de nouvelles offres performantes, globales et adaptées aux usages et aux métiers.
Interface entre les offreurs et les utilisateurs, le Cluster établit et anime le dialogue au sein de l'écosystème.
Il s'appuie sur le savoir-faire acquis depuis 10 ans par Eura-Technologies pour faire venir des start-up et des projets innovants.
Je vous invite d'ailleurs à découvrir le pavillon du Cluster à l'occasion de ce forum. Près de 30 structures sont présentes. Ce pavillon est un condensé du tissu économique régional. Il accueille des entreprises de toutes tailles, impliquées dans le développement de la filière régionale.
Il est à l'image de l'esprit du Cluster : collaborer pour une meilleure performance collective.
Il me reste à vous souhaiter un bon FIC 2015 ; j'espère que vous prendrez autant de plaisir à y participer que celui que nous avons pris à l'organiser.
Je vous remercie et je cède maintenant la parole au Général Watin Augouard



Mot d'accueil

Général d'armée (2S) Watin-Augouard et M. Pierre de SAINTIGNON

Monsieur le Président,
Mesdames, Messieurs,
Chers amis et, en particulier, chers amis étrangers

Le général d'armée Denis FAVIER, directeur général de la gendarmerie nationale, est en ce moment-même auprès de Bernard CAZENEUVE, notre ministre de l'intérieur, et va accueillir Thomas de MAIZIERE, ministre fédéral allemand de l'intérieur.

En raison de cette contrainte protocolaire, il ne peut être parmi nous à cet instant.
Il m'a demandé de l'excuser auprès de vous et de prononcer, aux côtés du Président Pierre de SAINTIGNON, le mot d'accueil ouvrant le 7eme Forum International de la Cybersécurité
J'accomplis cette mission avec plaisir et satisfaction :
Avec le plaisir d'être à vos côtés, M. le Président, car je sais la part

que la région a prise, sous votre impulsion, au développement du FIC et à son enracinement à Lille, dans la région Nord-Pas-de-Calais ;
Avec le plaisir également de retrouver les participants aux éditions précédentes, dont ceux d'entre vous, fidèles au FIC, depuis sa fondation en 2007. C'est aussi le plaisir d'accueillir près de 1000 nouveaux inscrits.
On vient au FIC pour la première fois par curiosité, on y revient par conviction !

J'éprouve une intense satisfaction en constatant le dynamisme d'un événement qui devient mature. Nous étions 500 en 2007, nous sommes 4500 aujourd'hui, venant de 73 pays du monde. 130 partenaires partagent aujourd'hui notre aventure !
Vous venez parfois de loin. Soyez les bienvenus en France, à Lille, au sein du FIC ! Le cyberespace n'a pas de frontière ; votre participation, chaque année plus nombreuse, en témoigne.
Toute l'équipe, rassemblée autour de Guillaume Tissier, que je remercie chaleureusement, a conçu un programme particulièrement riche, comme vous pouvez le mesurer. Nous avons tenu compte de vos avis, des souhaits émis par nos partenaires.
Notre ambition est de contribuer collectivement à la réflexion et à l'action afin que notre cyberespace soit plus libre et plus sûr. Sécurité et liberté sont deux « sœurs siamoises » indissociables. La sécurité sans liberté, c'est le totalitarisme, la domination sur les esprits, les corps et la matière, la négation de notre vie privée, de notre sphère d'intimité et d'autonomie.
La liberté sans sécurité, c'est un blanc-seing donné aux prédateurs, la loi du plus fort au préjudice du plus faible.
Au regard des événements particulièrement douloureux que nous vivons, cette symbiose sécurité/liberté est plus que jamais une exigence démocratique.

Ensemble, nous allons parler de droit, de technique, de recherche, de projets industriels, d'enquêtes, de forensique, de mesures de prévention, de sécurité et de défense.
N'oublions jamais que toutes ces matières relèvent des modalités, des voies et moyens. Elles répondent à la question « comment ? ».
Leur étude serait vaine, si elle ne s'inscrivait dans la recherche d'une finalité qui réponde à la question « pourquoi ?». Science sans conscience n'est que ruine de l'âme, disait Rabelais.
La transformation numérique serait un échec sans conscience, sans réflexion sociétale qui replace l'Homme au cœur du cyberespace.
Au moment où la « bataille des idées » est engagée sur Internet, comme en témoigne notamment l'explosion des provocations du terrorisme et de son apologie, la quête du sens doit guider notre action et lui conférer sa légitimité.

Le cyberespace doit servir l'humanité, le progrès économique et social. Nous devons le construire ensemble pour un monde plus juste, grâce à la création de valeur, l'accès à la culture, à la santé, à l'éducation, à la démocratie.

Le FIC a l'ambition d'éliminer les cloisons inutiles entre le secteur public et le secteur privé, de favoriser la transversalité au sein même des organisations.
Le FIC est un lieu de partage, de confiance et, ainsi, de solidarité.
Tel est l'esprit qui l'anime, telle est la « FIC Touch » !
Pendant ces deux jours soyons les bâtisseurs d'un cyberespace porteur d'espérance !
Que le FIC 2015 commence !

Forum international de la cybersécurité
Lille – 20 janvier 2015

M. Bernard CAZENEUVE,
Ministre de l'Intérieur

DISCOURS

Monsieur le Ministre,
cher Thomas de Maizière,
Monsieur le Préfet,
Mesdames et Messieurs les élus,
Monsieur le Directeur général de la Gendarmerie nationale,
mon Général,
Mesdames, Messieurs, chers amis,

Je suis très heureux d'ouvrir aujourd'hui les travaux de la 7ème édition du Forum international de la cybersécurité. Un lien naturel et durable unit en effet le ministère de l'Intérieur à cette manifestation, lancée à l'initiative de la Gendarmerie nationale en 2007 et aujourd'hui organisée en partenariat avec le Conseil régional du Nord Pas de Calais et la société CEIS.
La diversité et la qualité des intervenants et des participants à cette nouvelle édition du FIC confirment le haut niveau d'engagement des organisateurs, que je tiens à remercier chaleureusement. Elles soulignent aussi l'intérêt que présente un tel espace de réflexion et d'échanges pour les experts et décideurs que vous êtes.
Je me réjouis également que l'Allemagne soit à l'honneur cette année, et je tiens à saluer la présence parmi nous aujourd'hui de mon homologue et ami allemand, Thomas de MAIZIERE, qui est venu nous apporter son soutien dans cette période difficile où la France fait face à une crise sans précédent.
Le terrorisme frappe sans distinction de pays ni de continent : il est donc nécessaire que notre riposte soit commune, c'est-à-dire européenne et internationale.
Par ailleurs, nous sommes tous confrontés aux mêmes défis et à la même nécessité d'adapter nos réponses sécuritaires aux nouveaux usages numériques – je pense notamment à la lutte contre la propa-

gande et le recrutement terroristes sur Internet, qui est depuis des mois un sujet majeur de réflexion parmi les services européens de renseignement et de sécurité. Il a encore été l'un des grands enjeux dont mes homologues et moi-même avons discuté à l'occasion du G10 des ministres de l'Intérieur, que j'ai réuni en urgence place Beauvau le 11 janvier dernier. Je crois plus que jamais qu'en la matière, une meilleure coordination entre pays européens est un élément décisif de la réponse que nous devons apporter aux terroristes.

La participation du ministre allemand de l'Intérieur à l'inauguration du FIC 2015 illustre bien la dimension internationale de ce salon et des enjeux de cybersécurité. La présence des délégations étrangères de la FIEP (« France Italie Espagne Portugal »), association des gendarmeries euro-méditerranéennes, dont la France a pris récemment la présidence, est également une belle preuve de la dimension internationale que le FIC permet d'approfondir année après année.

La révolution numérique concerne en effet toutes nos sociétés. Elle transforme aussi bien notre vie quotidienne que notre économie et notre modèle de production industrielle. Pour nos organisations, nos entreprises, nos collectivités territoriales ou encore nos administrations, elle représente un véritable levier de performance et un formidable accélérateur d'innovation, offrant des opportunités nouvelles de développement.

Néanmoins, le cyberespace est aussi aujourd'hui un champ sans frontières, où se développent des menaces pour notre société, de même qu'il est un outil susceptible d'être détourné à des fins malveillantes ou criminelles par des individus ou des organisations. Or, sur les territoires numériques comme ailleurs, la responsabilité de l'État est de protéger les citoyens avec détermination, d'anticiper les menaces, et de réprimer – lorsqu'ils surviennent – les actes délictueux.

Nous devons tout faire pour que le cyberespace soit avant tout un lieu où l'exercice des libertés fondamentales et la protection de la vie privée sont garantis.

Garantir la sécurité sur Internet n'est en effet rien d'autre qu'étendre aux territoires numériques – au cyberespace – la protection que nous devons à nos concitoyens, condition essentielle du respect des principes fondateurs de la République, et avant toute chose du respect de l'Etat de droit et des libertés individuelles, en toutes circonstances.

La sécurité dans les espaces numériques doit donc être assurée avec autant de détermination que dans nos villes et dans nos territoires. De même, le droit de vivre de son travail, c'est-à-dire d'innover et de développer une activité économique – ce qui de plus en plus implique une dimension numérique –, doit être garanti.

Une telle responsabilité engage la Nation tout entière. Nous l'assumons pleinement. Ainsi, face à la récente progression des phénomènes de radicalisation violente et d'endoctrinement terroriste sur Internet, aboutissant au départ pour la Syrie et l'Irak de plusieurs centaines de jeunes Français – et au départ, plus généralement, de nombreux jeunes Européens–, le Gouvernement a soumis au Parlement, qui les a adoptées dans la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, des mesures visant spécifiquement la diffusion de contenus illicites sur Internet – notamment des contenus de propagande terroriste et d'apologie du meurtre de masse ou de l'assassinats tels que ceux de notre compatriote Hervé GOURDEL ou de l'Américain Peter KASSIG.

Les attentats que nous avons dû affronter ont eux aussi largement démontré la centralité de ces enjeux de cybersécurité, et par là même l'absolue nécessité qu'il y a aujourd'hui à renforcer notre dispositif de lutte contre les cybermenaces. J'y reviendrai. Comme vous le savez, à la demande du Premier Ministre, nous sommes actuellement en train de finaliser de nouvelles propositions en la matière.

Ministère de l'Etat, ministère de la sécurité, de la prévention et de la gestion des crises, le ministère de l'Intérieur est donc particulièrement concerné par les trois dimensions fondamentales de la cybersécurité.

La cyberdéfense, tout d'abord, vise à protéger les institutions et les intérêts nationaux, conformément aux objectifs définis par le Livre blanc de la défense et de la sécurité nationale. Le ministère de l'Intérieur y participe activement, aux côtés de l'Agence nationale de la Sécurité des systèmes d'information (ANSSI) et du ministère de la Défense notamment.
La sécurité des systèmes d'information est un deuxième enjeu, tout aussi important. Il concerne non seulement les systèmes du ministère de l'Intérieur, mais aussi ceux de l'ensemble des acteurs économiques sur le territoire et des particuliers.

Enfin, la lutte contre la cybercriminalité mobilise aujourd'hui près de 600 enquêteurs spécialisés de la gendarmerie et de la police nationales.
C'est la raison pour laquelle j'ai nommé en décembre dernier un préfet spécifiquement chargé de la lutte contre toutes les cybermenaces, le « préfet cyber », Jean-Yves LATOURNERIE. Directement rattaché à mon cabinet, et en lien permanent avec l'ensemble des directions générales et des directions du ministère qui sont concernées par les enjeux de cybersécurité, ainsi qu'avec les acteurs interministériels compétents, il a pour missions :

- de piloter la montée en puissance du dispositif ministériel, et de proposer le cas échéant des mesures d'organisation adaptées aux enjeux des cybermenaces ;
- de fédérer l'ensemble des énergies et les initiatives des différents acteurs au sein du ministère de l'Intérieur, et de veiller à ce qu'elles s'inscrivent dans le cadre de la stratégie ministérielle de lutte contre les cybermenaces ;
- d'être le point d'entrée identifié pour les acteurs extérieurs au ministère, notamment dans le cadre des travaux, engagés par l'ANSSI, visant à l'actualisation de la stratégie nationale de cybersécurité ;
- enfin, de veiller à la pleine insertion de la démarche stratégique du ministère dans le cadre de la nécessaire coopération européenne et internationale.

Pour accomplir ses missions, le préfet LATOURNERIE bénéficiera bien sûr du concours de l'ensemble des services du ministère de l'Intérieur.

Avant d'évoquer les principaux axes de la stratégie ministérielle, je souhaite vous apporter quelques éléments qui permettront de mieux définir l'état des cybermenaces, tel qu'on peur l'appréhender aujourd'hui. Parmi les tâches confiées au « préfet cyber », figure justement l'élaboration d'un premier rapport ministériel sur l'état de la menace à laquelle nous devons faire face.
Les premiers travaux réalisés en vue de la rédaction de ce rapport permettent d'ores et déjà de dégager trois grandes tendances.
Les différentes menaces que je vais brièvement décrire dans un instant, interviennent dans le contexte d'une société en profonde mutation numérique. Si le développement exponentiel des nouvelles technologies, l'émergence des objets connectés et les facilités offertes par le e-commerce sont de véritables progrès technologiques et sociaux, ils apportent aussi avec eux leur lot de difficultés nouvelles.
Les données numériques structurent en effet toutes les parties et étapes de notre vie personnelle et professionnelle, qu'il s'agisse des démarches administratives, de notre santé, de notre économie ou encore de nos loisirs.

Or, l'utilisation et la gestion de ces données très précieuses exposent aussi parfois leurs propriétaires à des menaces ou des vulnérabilités auxquelles nous nous devons d'apporter des réponses.
La première de ces menaces est le cyberterrorisme, qui consiste à commettre une action destructrice par le vecteur numérique. Comme je vous le disais,

les groupes terroristes qui nous ciblent sont extrêmement actifs sur les réseaux sociaux tels Facebook, Twitter et Youtube, tout en maintenant des canaux de transmissions plus traditionnels comme les forums djihadistes.

Même si les sociétés gestionnaires de ces médias sociaux sont aujourd'hui beaucoup plus soucieuses des contenus postés, l'utilisation d'Internet par les groupes ou organisations terroristes s'est encore amplifiée en 2014. Il apparaît nettement que les groupes islamistes radicaux les plus structurés (notamment Al-Qaida et DAESH) voient en Internet une tribune et un excellent vecteur de recrutement.

A cet égard, entre 2013 et 2014, le nombre de signalements parvenus au ministère de l'Intérieur par le biais de la plateforme PHAROS, créée à cet effet au sein de la Direction centrale de la Police judiciaire, a été multiplié par trois. Le fait que la grande majorité de ces signalements concerne des contenus détectés sur des réseaux américains, ne diminue en rien l'impact de ces actes de propagande sur nos ressortissants ou sur les étrangers résidant habituellement dans notre pays.

Les attentats auxquels nous avons dû faire face il y a une dizaine de jours, nous ont eux aussi démontré, si besoin était, que toute crise majeure – notamment terroriste – comporte désormais une forte dimension de cybersécurité. Ils ont ainsi confirmé la nécessité pour le ministère de l'Intérieur de se préparer à affronter les nouvelles menaces numériques en se dotant des outils et des ressources appropriés. Les réseaux sociaux servant de vecteur de communication aux terroristes, les supports numériques découverts ont été et sont encore exploités et analysés – entre autres par la sous-direction de la police judiciaire à la lutte contre la cybercriminalité – dans les délais très brefs imposés par la gravité et l'urgence de la situation.

Il a fallu ensuite faire face aux cyber-attaques malveillantes, prenant en la circonstance l'aspect d'un phénomène de masse inédit, modifiant les pages d'accueil ou exploitant les fragilités de milliers de sites institutionnels et privés. Plus de 1 300 attaques ont en effet été revendiquées par des équipes de hackers se revendiquant d'organisations islamistes ou saisissant l'opportunité de démontrer leur capacité malfaisante. Nous avons donc dû organiser très rapidement une réponse judiciaire commune que la sous-direction à la lutte contre la cybercriminalité a pilotée. Le réseau des investigateurs spécialisés en cybercriminalité de la police et de la gendarmerie nationales a également été mobilisé.

La plateforme PHAROS, elle-même mise à mal, a, durant la crise, traité en quelques jours plus de 25 000 signalements de contenus illicites sur Internet ; depuis les attentats, elle continue de veiller toujours aussi activement, grâce à la détermination sans faille des opérateurs policiers et gendarmes.

Enfin, une veille sur les réseaux sociaux a également été mise en place, exploitant, dans un tel contexte de crise, les contacts privilégiés noués avec les sociétés de service de l'Internet, plus particulièrement avec Twitter, Facebook, Google et Dailymotion. Un traitement particulier et en urgence a ainsi pu être accordé aux demandes de retrait des vidéos mises en ligne liées aux attaques terroristes. De manière complémentaire, les demandes de gel des données techniques liées aux demandes de retrait des vidéos ont été traitées 24H sur 24H pour le compte de l'ensemble des services de la police et de la gendarmerie nationale.

Le cyberterrorisme est une menace majeure, dont il convient de préserver nos compatriotes, nos institutions et les intérêts nationaux, comme le préconise le Livre blanc de la défense et de la sécurité nationale. Comme je vous le disais, le ministère de l'Intérieur travaille en étroite coopération avec l'ANSSI et le ministère de la Défense, pour mettre en oeuvre notre stratégie de cyberdéfense.

La loi du 13 novembre 2014 a d'ores et déjà permis de renforcer nos moyens de lutte contre le cyberterrorisme.

L'un de ses principaux objectifs est en effet de lutter plus efficacement contre la propagande djihadiste, l'apologie et la provocation du terrorisme en ligne. Pour ce faire, nous avons prévu des dispositions permettant, sous le contrôle d'une personnalité qualifiée et le cas échéant du juge administratif, le blocage et le déréférencement des sites Internet qui mettent en ligne ce type de contenu. Le décret d'application relatif au blocage des sites sera publié dans les prochains jours, après les dernières consultations ; celui relatif au déréférencement suivra rapidement.
La loi comporte également des dispositions moins connues du grand public, mais tout aussi importantes dans la lutte contre la cybercriminalité : l'extension des cyberpatrouilles à l'ensemble des infractions relevant du champ de la criminalité organisée, l'introduction du délit de vol de données informatiques, l'aggravation des peines en matière d'atteinte en bande organisée aux systèmes de traitement automatisées de données de l'Etat et l'application de certaines techniques spéciales d'enquête, la facilitation des perquisitions informatiques et du déchiffrement des données cryptées.

Sans doute notre dispositif législatif doit-il encore être amélioré – et nous allons bientôt faire de nouvelles propositions pour gagner en efficacité dans notre lutte contre le cyberterrorisme –, mais les enquêteurs sont d'ores et déjà mieux armés pour affronter les défis d'aujourd'hui et ceux de demain.
Le deuxième type de menace relève des cyberattaques contre les entreprises, qu'il s'agisse de cyberespionnage industriel ou de cyberescroquerie à grande échelle.
En effet, des attaques de plus en plus sophistiquées touchent principalement les entreprises et visent à leur voler des données stratégiques, parfois en très grande quantité comme certains exemples étrangers ou français l'ont montré ces dernières semaines, ou bien à leur soutirer des sommes importantes d'argent – plusieurs entreprises, parfois des multinationales, ont ainsi été récemment victimes d'escroqueries au faux ordre de virement international (FOVI).
Nous devons donc tout faire pour protéger nos entreprises de telles attaques. Les liens numériques qui unissent les fournisseurs, les vendeurs et les clients sont en effet désormais incontournables, et ne sont plus entravés par les frontières territoriales et politiques. Le patrimoine informationnel des entreprises revêt par ailleurs une importance capitale pour le développement de notre économie et la préservation de nos emplois. Ce patrimoine informationnel englobe très largement les données relatives aux projets liés à la recherche, l'innovation et le développement, les fichiers des clients ou des employés qui permettent de développer ou de préserver une activité économique et plus largement toutes données collectées, stockées et utilisées pour garantir le bon fonctionnement d'une entreprise. Stockées localement ou de manière délocalisée dans le « cloud », ces données sont essentielles pour le développement ou la survie de nos entreprises. Tout comme les locaux physiques, ces données peuvent faire l'objet d'attaque, de vols, de falsification ou de tous autres faits délictueux.
Enfin, le troisième type de menace dont nous devons tenir compte vise les particuliers, particulièrement vulnérables aux escroqueries en tous genres, qui s'accompagnent parfois de chantage sous forme numérique.
Ainsi, les escroqueries représentent actuellement 80% des plaintes cyber traitées par les services de police et de gendarmerie. En 2013, l'usage frauduleux de cartes bancaires dans les transactions sur Internet s'élevait à 155 millions d'euros. Les paiements à distance ne représentent que 11% de la valeur des transactions nationales par carte bancaire, mais comptent pour 65% du montant de la fraude.
Quant aux différentes formes de chantage sur Internet, on observe malheureusement le développement de plusieurs pratiques telles que le chantage suite à des vols

massifs de données internes ou de clients d'entreprise, le chantage à la webcam (sextorsion), ou encore le chantage via l'utilisation de « rançongiciels ».

Là aussi, nous devons tout faire pour protéger nos concitoyens de telles menaces, qui violent par ailleurs leur intimité, ou ciblent leurs activités professionnelles.

Pour affronter ces défis, nous allons lancer un grand plan d'action qui renforcera l'efficacité des services du ministère de l'Intérieur en ce qui concerne la lutte contre les cybermenaces, quelles qu'elles soient.
Je l'ai dit au début de mon propos, la responsabilité de l'Etat, sur les territoires numériques comme ailleurs, est de protéger les citoyens, d'anticiper les menaces, de prévenir et de réprimer les actes malveillants et criminels.
Depuis plus de 20 ans déjà, le ministère de l'Intérieur a intégré les défis nouveaux posés par la cybercriminalité. Mais aujourd'hui, l'ampleur et la variété du phénomène nous obligent à monter en puissance, à adapter notre dispositif de cybersécurité.
Nous devons en effet mobiliser des compétences nouvelles, développer des moyens technologiques spécifiques, proposer des actions de protection et de prévention inédites à l'égard des systèmes et des publics particulièrement ciblés.

Surtout, à l'heure de la transformation numérique de la société, la lutte contre les cybermenaces ne peut plus être réservée à quelques experts : elle doit faire l'objet d'une organisation dédiée qui rendra possible l'amélioration et l'adaptation globales des services du ministère. C'est tout le sens du plan d'action élaboré par l'ensemble des directions du ministère, et dont la mise en oeuvre sera pilotée par le « préfet cyber ».
Ce plan s'organise autour de six axes stratégiques.

Le premier axe consiste à disposer en permanence d'une vision claire et actualisée des cybermenaces.
Outre la production annuelle d'un rapport sur l'état de la menace, il s'agit de construire un appareil statistique adapté, permettant de mesurer les faits constatés dans le domaine de la cybercriminalité, mais aussi de disposer d'autres indicateurs externes ou internes au ministère de l'Intérieur caractérisant l'évolution de la menace. Le service statistique ministériel en sera le maître d'oeuvre.
Le deuxième axe réside dans le renforcement de nos capacités d'analyse et de réponses opérationnelles.
Il s'agit pour ce faire de fédérer les énergies et de favoriser les échanges mutuels entre les divers services et forces de sécurité. La nomination du préfet en charge des cybermenaces contribue ainsi directement à cet objectif. Il s'agit aussi, chaque fois que possible, de mutualiser les efforts consentis au profit des acteurs opérationnels.
Nous disposons à l'échelon national d'un haut niveau d'expertise qui peut ainsi venir compléter et appuyer les dispositifs territoriaux de renseignement et des deux forces de sécurité police et gendarmerie dans le domaine judiciaire. Cet effort suppose une mobilisation générale de l'ensemble des services de renseignement, notamment de la direction générale de la sécurité intérieure (DGSI) et du service central du renseignement territorial (SCRT) dans le domaine cyber. Leur rôle d'anticipation sera également complété par une veille de l'internet, en particulier des réseaux sociaux.
Au sein de la Direction Centrale de la Police Judiciaire (DCPJ) a été créée en avril dernier la Sous-Direction de Lutte contre la cybercriminalité (SDLC). Elle réunit en son sein l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), qui comprend des policiers et des gendarmes, ainsi qu'une division de l'anticipation et de l'analyse. J'ai pu constater personnellement le rôle essentiel qui est le sien en cas de crise, et la réactivité, le savoir-faire et l'engagement de ses personnels.
Au sein de la Gendarmerie na-

tionale, la Division de la Lutte Contre la Cybercriminalité (DLCC), transformée en Centre de Lutte Contre les Criminalités Numériques (C3N) sera rattaché au pôle judiciaire chargé de piloter la communauté des 1800 enquêteurs et correspondants « Technologies numériques de la gendarmerie ». Ce centre développera également ses capacités d'investigations d'initiative sur Internet.

Parallèlement, au sein des sections de recherches de la gendarmerie, des groupes cyber seront créés pour consolider les capacités d'investigations de haut niveau, y compris au plan territorial, et poursuivre les responsables de trafics de haut niveau, ou d'escroqueries en bande organisée. L'adaptation des moyens consacrés au forces de sécurité, pour se moderniser et faire face aux cybermenaces tout en s'adaptant à la transformation numérique de la société, fait également l'objet de démarches mutualisées et communes aux deux forces . Ainsi l'organisation, sous le pilotage du préfet chargé de la lutte contre les cybermenaces, d'une veille juridique cyber à disposition de l'ensemble des services du Ministère, procède de cette démarche. Il en va de même en matière de formation à la lutte contre les cybermenaces pour l'ensemble des policiers et gendarmes, ou de la définition d'un schéma de mutualisation des formations des enquêteurs et investigateurs spécialisés dans ce domaine, qui associeront DGGN, DGPN et Préfecture de Police.

Plus largement, la lutte contre les cybermenaces s'inscrit dans le plan ministériel de modernisation, qui implique l'ensemble des services du ministère et permettra de consacrer sur le triennal 2015-2017 un budget total de 108 millions d'euros pour doter à court terme les forces de sécurité intérieure de moyens modernes et d''augmenter leurs capacités d'action, leur mobilité et leur sécurité. Ce plan vise à offrir dans le même temps de meilleurs services, notamment numériques, à la population pour une plus grande proximité des services. Il contribuera enfin directement à modernisation et la sécurisation des réseaux informatiques du ministère de l'Intérieur. Il s'agit pour nous de rester en mesure de faire face, y compris en situation de crise importante, aux exigences que nécessitent ses missions régaliennes

Le troisième axe porte sur la politique de sensibilisation et de prévention des publics.

En effet le ministère de l'Intérieur, du fait de sa présence sur l'ensemble des territoires, peut contribuer à améliorer significativement le niveau de vigilance des particuliers, des acteurs économiques et des collectivités territoriales. Les réseaux territoriaux de la DGSI, de la DGGN et de la DGPN sont déjà particulièrement mobilisés par ces objectifs. La DGSI intervient directement auprès des opérateurs d'importance vitale et des entreprises les plus stratégiques. La gendarmerie concentre ses efforts sur les entreprises PME-PMI et a intégré les nouvelles menaces cyber dans ses actions de sensibilisation. Ces actions devront être encore amplifiées.

La prévention auprès des jeunes publics constitue également une priorité pour le ministère. Après les expérimentations conduites par la gendarmerie, l'ensemble des forces de la police, de la préfecture de police et de la gendarmerie s'engagent désormais dans l'opération "Permis Internet" auprès des élèves de CM2. Des initiatives particulièrement intéressantes ont été prises dans cette région, par la brigade de prévention de la délinquance juvénile du groupement de gendarmerie du Pas-de-Calais qui organise aujourd'hui même une opération à destination de sourds et malentendants ; un gendarme a ainsi été spécialement formé à la langue des signes.

Le quatrième axe concerne la recherche et développement.

Il est essentiel pour nous de disposer d'un tissu industriel solide, qui soit à même de proposer des solutions de cybersécurité éprouvées et qui préservent la souveraineté nationale. C'est pourquoi j'ai souhaité rencontrer dans quelques instants des représentants des entreprises françaises de cy-

bersécurité. Je les rencontrerai accompagné de Jean-Yves Latournerie et de Thierry Delville, délégué ministériel aux industries de sécurité. Ma volonté est faire en sorte que l'Etat et les entreprises nouent une relation durable et solide, permettant à chacun de contribuer à l'amélioration du niveau de cybersécurité de la France. Le ministère de l'Intérieur devra donc jouer pleinement son rôle dans l'affirmation d'une politique industrielle de cybersécurité. Dans le prolongement des actions engagées par l'ANSSI au titre du plan 33 de la « Nouvelle France Industrielle » et dans le cadre des travaux menés au sein du comité de filière des industries de sécurité, le ministère de l'intérieur veillera à mobiliser toutes les énergies en faveur de l'émergence d'une offre française, mais aussi européenne, de cybersécurité.

Dans le domaine de la formation, le partenariat noué entre la gendarmerie nationale et l'Université Technologie de Troyes pour la formation des « Enquêteurs technologies Numériques » illustre la qualité de ces échanges avec le monde de la recherche et de l'industrie. C'est pourquoi j'ai tenu à remettre leurs diplômes aux lauréats de la dernière promotion en compagnie du directeur de l'université M. Pierre Koch.

Le cinquième axe vise à renforcer encore le niveau de sécurité des systèmes d'information du ministère.

Dans ce domaine, le Ministère de l'Intérieur se doit évidemment d'être exemplaire. C'est pourquoi il nous faut à la fois actualiser régulièrement la liste des éléments essentiels de notre patrimoine opérationnel et conduire les audits de sécurité appropriés. Nous devons veiller à sensibiliser l'ensemble des personnels aux enjeux de la sécurité des systèmes d'information. Et nous devons bien entendu mettre à leur disposition des outils et systèmes qualifiés protégés, en particulier pour les usages mobiles.

Je souhaite également que l'offre de services du Centre national de gestion de la sécurité des systèmes d'information soit actualisée. Il s'agit, là encore, de veiller à l'utilisation optimale des moyens importants que ce ministère consacre aux fonctions de veille, d'alerte et de réaction face aux incidents de sécurité informatique et de cyberattaques.

Le sixième axe consiste enfin à promouvoir l'action internationale du ministère dans le domaine de la lutte contre les cybermenaces.

Face à des cybermenaces qui se jouent des frontières, la coopération avec nos partenaires étrangers revêt un caractère fondamental. La Direction de la Coopération Internationale (DCI) est résolument impliquée dans cette ambition et son réseau international s'est mobilisé afin d'appuyer au quotidien l'activité des acteurs opérationnels, (SDLC, C3N, PP..) hors de notre territoire.

La coopération judiciaire doit bénéficier de législations internationales adaptées à des besoins opérationnels qui restent souvent conditionnés par l'urgence. C'est pourquoi j'ai demandé au préfet chargé de la lutte contre les cybermenaces de s'assurer de la cohérence des travaux d'élaboration de la doctrine internationale en la matière.

A cet effet l'ensemble des directions travaille à améliorer le dispositif au niveau de l'Union européenne, du Conseil de l'Europe et dans d'autres enceintes de négociation. En effet, la sécurité de l'espace cyber demeure une sécurité collective. De ce fait, elle repose sur l'échange de compétences entre les professionnels des forces de l'ordre. En 2014, près de 300 partenaires étrangers ont bénéficié de ce partage de compétence de la part de nos services. Ce sont ces partenaires qui, ayant noué de solides relations de confiance mutuelle, contribueront demain aux succès des enquêtes internationales.

Dans le même esprit, j'invite également nos partenaires étrangers à développer leurs contacts avec les 280 policiers et gendarmes des 84 représentations du ministère de l'Intérieur qui se trouvent au sein de nos

ambassades à l'étranger. Je les remercie aussi pour le soutien qu'ils pourront nous apporter dans le cadre des négociations visant à établir des cadres juridiques qui répondent mieux aux attentes des enquêteurs.

Enfin, je voudrais souligner que la lutte contre les cybermenaces ne peut se concevoir au sein du seul ministère de l'Intérieur. Notre approche doit être globale et transversale et elle a donc vocation à s'inscrire plus largement dans un contexte interministériel. De nombreux autres départements sont mobilisés par ce sujet, à commencer par celui de la Défense et par celui de l'Economie et des Finances. C'est pourquoi je me félicite de la venue demain ici même, à l'occasion de la clôture de ce Forum, de mes collègues Axelle Lemaire et Jean-Yves Le Drian.
C'est dans le même esprit que je vous souhaite donc de profiter pleinement de cette occasion exceptionnelle que constitue ce Forum pour dialoguer et échanger avec de nombreux experts et décideurs, issus des entreprises, des administrations ou de l'Université, venus de France ou de pays étrangers, afin de confronter nos visions respectives de la transformation numérique qui est à l'œuvre au sein de nos sociétés.

Je vous donne d'ores et déjà rendez-vous pour la prochaine édition de Forum en 2016. Vous pourrez compter naturellement sur l'engagement du ministère de l'intérieur, et au sein de celui-ci sur celui de la gendarmerie nationale dont je tiens à saluer la remarquable et persévérante contribution à cette initiative.

Enfin je voudrais conclure sur un petit mot qui tient à l'actualité. Nous venons de vivre des heures extraordinairement douloureuses, qui témoignent de la réalité de la menace terroriste en France et en Europe. La France a été frappée, mais elle n'est pas la seule. L'Australie, le Canada, la Grande-Bretagne l'ont été aussi, la Belgique à travers les monstrueux assassinats commis par Mehdi Nemmouche. La France est plus forte lorsqu'elle regarde en face la réalité de la menace. Et lorsqu'elle regarde en face la réalité de la menace en puisant sa force dans les valeurs qui fondent la République et qui ont conduit la France à tenir aux peuples du monde le message que les peuples du monde ont appris à aimer d'elle, alors la France est plus forte. Elle est plus forte d'elle-même, elle est plus forte de ce qu'elle représente, des valeurs universelles qu'elle a portées. Ceux qui ont cherché à nous atteindre en frappant lâchement, ignoblement des journalistes qui incarnent la liberté de la presse jusqu'à l'impertinence, des policiers qui représentent le droit, la force du droit, l'amour de l'état de droit, qui est consubstantiel à la République, et des Français de confession juive, parce que l'antisémitisme existe en France, ceux qui ont frappé ainsi doivent savoir que nous les combattrons avec les armes de la République et de la démocratie, que nous ne les laisserons pas, par l'effroi qu'ils prétendent semer, remettre en cause les libertés fondamentales auxquelles nous tenons et que nous nous armerons face à eux en mobilisant tous les moyens dans la conformité, encore une fois, aux principes du droit pour que la République, debout, puisse demeurer telle qu'en elle-même, forte et belle, rassemblée autour de ses valeurs.
Je vous remercie.

Forum international de la cybersécurité
Lille – 20 janvier 2015

M. Thomas de MAIZIÈRE
Ministre fédéral Allemand de l'Intérieur

DISCOURS

Lieber Herr Kollege Cazeneuve, lieber Bernard, Herr Präfekt,

vielen Dank für die freundliche Begrüßung. Ich bin sehr gerne hierhergekommen, um erneut zu zeigen, dass Frankreich und Deutschland auf vielen Gebieten eng zusammenarbeiten.

Sie werden heute und morgen wichtige Themen der digitalen Welt besprechen. Wenn das Internet international ist, muss die Antwort Cybersicherheit auch international sein. Natürlich steht diese Veranstaltung auch im Schatten der schrecklichen Anschläge und Attentate in Paris. All das hat nicht nur Frankreich bewegt sondern auch uns im Kabinett aber auch das deutsche Volk. Wir standen und stehen fest an der Seite Frankreichs, und ich will gerne auch wiederholen, dass auch aus meiner Sicht und aus der Sicht der deutschen Öffentlichkeit die ganze Regierung, auch die Opposition, aber insbesondere auch der französische Innenminister, Du, Bernard, durch Deine Art und Haltung Dich in diesen Tagen großartig bewährt hast.

Das waren Anschläge auf den Kern unserer Demokratie und Grundwerte, die nicht nur in Frankreich gelten, sondern auch in Deutschland und in Europa.

Für das globale Problem Terrorismus gibt es keine einfachen Erklärungen und damit auch keine schnellen und einfachen Lösungen. Sie haben Auswirkungen auf Frankreich, auf Deutschland, auf Europa und darüber hinaus. Die Ereignisse in Paris verdeutlichen einmal mehr, dass wir gemeinsam handeln müssen, und zwar nicht nur im Bereich der so genannten „realen" Welt. Das Handeln krimineller und terroris-

tischer Bestrebungen findet genauso in der „virtuellen“ Welt statt, wobei ich mir die Bemerkung erlaube, dass ich den Begriff der „virtuellen Welt“ nicht besonders mag, auch wenn er in Ihrer Community verbreitet ist. Ich glaube, es gibt keine „virtuelle“ Welt. Was im Internet stattfindet, ist höchst real und wir sollten nicht so tun, als hätte es mit der realen Welt durch die Beschreibung, es sei virtuell, wenig zu tun.

Wir haben das Internet als Ort der Freiheit, der persönlichen Entfaltung, des Handels, der Vernetzung erlebt und schätzen gelernt. Das soll auch so bleiben. Damit das Internet aber nicht für kriminelle und terroristische Zwecke missbraucht wird, muss es genauso geschützt werden wie andere Infrastrukturen, wie Strom und Wasser.

Was können wir tun, was können Frankreich und Deutschland beitragen, um das Internet sicherer zu machen?
Um unsere Gesellschaft zu schützen?
Um unsere kritischen Infrastrukturen zu sichern?
Um Cyber-Terrorismus und Cyber-Jihadismus zu bekämpfen, aber auch Kinderpornografie und Formen von Wirtschaftskriminalität, die nur im Internet stattfinden kann?

Dazu bedarf es natürlich zu allererst nationaler Strategien. Frankreich hat eine solche Strategie - der Innenminister hat sie eben vorgetragen mit ihren sechs Achsen, und alles, was ich eben gehört habe, finde ich klug und überzeugend. Sicher ist aber auch, dass wir alleine mit nationalen Strategien nicht weiterkommen. Wir brauchen auch gemeinsam mit unseren Partnern, gemeinsam mit der EU und wir brauchen weltweit Anstrengungen. Das war ja auch die sechste Achse der französischen Strategie. Auch das haben wir bei dem Treffen vor neun Tagen, an dem berühmten Sonntag auf Einladung von Herrn Bernard Cazeneuve besprochen und - einige Wochen zuvor - auf einem G6-Treffen lange vor dem Anschlag diese Bedeutung unterstrichen.

An unseren Grundwerten, an den Regeln unseres gesellschaftlichen Zusammenlebens ändert sich prinzipiell auch durch das Internet nichts. Bestehende Regelungen gelten auch im digitalen Zeitalter. Aber natürlich ist nicht alles eins-zu-eins übertragbar, man muss genau hinsehen und Manches an die anderen Rahmenbedingungen anpassen. Neue Technologien können neue Herausforderungen mit sich bringen, an die Gesetzgebung, an unsere Sicherheitsbehörden und an die Sicherheitsbehörden.

Einiges ist bereits auch in Deutschland - und darüber will ich berichten - auf einem guten Weg:
Wir haben zum Beispiel seit einigen Jahren einen Lagebericht, den Cyber-Sicherheitsbericht, den das Bundesamt für Sicherheit in der Informationstechnik (BSI), eine Institution die ganz ähnlich funktioniert wie das französische ANSSI, jedes Jahr vorlegt. Im letzten Jahr habe ich zum ersten Mal selbst gemeinsam mit dem Präsidenten des BSI diesen Jahresbericht vorgestellt. Dort tragen wir der Öffentlichkeit vor, wie viele Angriffe es gegeben hat, z.B. auf die Regierungsnetze, auf die Wirtschaft und welche Maßnahmen ergriffen worden sind, welche Schutzmöglichkeiten der einzelne Bürger hat, und vieles andere mehr. Also ein solcher Lagebericht ist für die Bewusstseinsbildung der Bevölkerung sehr wichtig.

Zweitens: Die EU-Kommission beispielsweise parallel zur Europäischen Cybersicherheitsstrategie Anfang 2013 einen Richtlinienentwurf vorgestellt, um die Netzwerk- und Informationssystemsicherheit (NIS) in der EU zu verbessern. Private Betreiber von Netzwerk- und Informationssystemen werden dort stärker in die Pflicht genommen. Wir unterstützen sehr die Kommission, dass es hier schnell zu einer Verabschiedung kommt.
Auch beim Schutz kritischer Infrastrukturen, also der für unsere Gesellschaft so bedeutsamen Ein-

richtungen wie Strom-, Wasser- und Energieversorgung, das Funktionieren der Bankensysteme, der Versicherungssysteme, besteht auch in Europa Handlungsbedarf. Drittens: In Deutschland haben wir einen Umsetzungsplan Kritische Infrastrukturen entwickelt und haben eine öffentlich-private Kooperation zwischen den Betreibern Kritischer Infrastrukturen, deren Verbänden und den zuständigen staatlichen Stellen aufgebaut.

Viertens: Wir haben im Dezember letzten Jahres im Kabinett ein so genanntes IT-Sicherheitsgesetz beschlossen. Das wird jetzt im Parlament beraten. Damit wollen wir einen Mindeststandard an IT-Sicherheit etablieren, und insbesondere die Betreiber Kritischer Infrastrukturen müssen hohe Anforderungen an Cyber-Sicherheit erfüllen. Dazu gehört auch, dass die Betreiber Kritischer Infrastrukturen erhebliche IT-Sicherheitsfälle künftig an unser BSI melden müssen, nicht immer öffentlich, oft vertraulich. Denn wenn ein Unternehmen angegriffen wird, spricht viel dafür, dass auch andere gleichartige Unternehmen angegriffen werden, insbesondere bei Strukturangriffen, und das wollen wir verhindern. Wir wollen dann auch durch das BSI entsprechende Unternehmen warnen, um sie zu schützen.

Meine Damen und Herren,

Freiheit und Sicherheit bedingen sich. Freiheit gibt es nicht ohne Sicherheit, und Sicherheit ohne Freiheit ist nichts wert. Wir müssen immer beide Perspektiven einnehmen und sorgfältig abwägen.

Das zeigt sich zum Beispiel bei der Kryptographie:
Einerseits möchten die deutschen Kryptostrategen unsere Bürger und die Wirtschaft im Internet schützen, z.B. durch Verschlüsselungstechnologien für alle, z.B. durch Ende-zu-Ende-Verschlüsselung. Deshalb erklärt z.B. unser BSI für Laien verständlich auf seiner Webseite, welche Verschlüsselungstechniken es gibt und wie man sie richtig einsetzt und diese Entwicklung geht weiter.
Andererseits aber sollen natürlich auch unsere Sicherheitsbehörden unter strengen Voraussetzungen – rechtsstaatlichen Voraussetzungen – befugt und in der Lage sein, verschlüsselte Kommunikation zu entschlüsseln, wenn dies für Ihre Arbeit und zum Schutz der Bevölkerung notwendig ist. Also: Der eine Teil der staatlichen Verwaltung berät, wie man sich am besten sicher im Internet bewegt und der andere Teil der öffentlichen Verwaltung versucht, trotzdem unter rechtsstaatlichen Bedingungen diese Sicherheitsvorkehrungen gegebenenfalls bei Straftätern zu überwinden. Das wirkt vielleicht wie ein Widerspruch, aber wir kennen das natürlich auch aus der so genannten „realen" Welt, beim Schutz des Hauses, beim Schutz des Autos. Überall raten wir zu Sicherheit: Man soll sein Haus verschließen, man soll eine Alarmanlage einbauen, man soll ein sicheres Auto kaufen, und trotzdem hat die Polizei selbstverständlich das Recht, unter bestimmten rechtsstaatlichen Voraussetzungen in ein Haus einzudringen und vieles andere mehr. Also: Den Konflikt, den viele jetzt als neu darstellen, den kennen wir längst aus der Abwägung von Freiheit und Sicherheit. Effektive Ermittlungen zur Strafverfolgung müssen auch im Cyberraum möglich sein. Der Staat – das ist meine Überzeugung – braucht nicht mehr, aber auch nicht weniger Reche im Cyberraum als sonst, nur weil die Art der Kommunikation anders ist.

Verschlüsselte Internetkommunikation – und das ist nur ein Beispiel von vielen – macht an Landesgrenzen nicht halt. Deshalb sind der Schutz des Internets, die Gewährleistung bestmöglicher Cybersicherheit, wie auch die Bekämpfung von Cyberkriminalität, Cyberspionage und Cyberterrorismus Herausforderungen, die nur mit guter internationaler Zusammenarbeit bewältigt werden können.

In vielen Bereichen arbeiten wir

bereits sehr gut zusammen. Ein schönes Beispiel ist das Projekt „Lorgnette“, über das Sie hier auf der Konferenz auch noch mehr erfahren können. Aus einer mehrmonatigen Hospitation eines französischen Gendarmen im deutschen Bundeskriminalamt entwickelte sich eine dauerhafte grenzüberschreitende Zusammenarbeit auf dem Gebiet der Zahlungskartenkriminalität. Diese intensive persönliche Kooperation bildete die Grundlage für erfolgreiche Ermittlungen, die schließlich zur Zerschlagung eines internationalen Netzwerks von Zahlungskartenbetrügern führte – mit 42 Festnahmen in Kanada, Frankreich und Deutschland.

Ebenso gut arbeiten die Agence nationale de la sécurité des systèmes d'information (ANSSI) und unser BSI zusammen. Es heißt oft, vielleicht auch gerade zwischen Deutschland und Frankreich, dass in solchen sensiblen Bereichen wie der Informationstechnologie nicht umfassend zusammengearbeitet werden könne. Das sehe ich nicht so, auch wenn natürlich jedes stolze Land einen nationalen Kern von Souveränität hat. Der bleibt auch für Zugang mal verschlossen - das ist normal. Aber wir können weit mehr tun als bisher und tun viel, wir müssen es tun und wir wollen es tun mit engen Partnern. ANSSI und BSI leben dies vor.

Gute Zusammenarbeit erfordert Vertrauen, und um sich zu vertrauen, muss man sich kennen. Deshalb sollten wir nicht nach bestimmten Ereignissen und nach tragischen Ereignissen, sondern strategisch und langfristig zusammenarbeiten. Uns austauschen und noch besser kennenlernen und weiteres Vertrauen aufbauen. Das gilt nicht nur für staatliche Akteure untereinander, sondern auch für Kooperationen mit und zwischen der Wirtschaft, der Wissenschaft und der Zivilgesellschaft. Wir tragen gemeinsam eine Verantwortung für unsere Welt, online wie offline.

Wer, wenn nicht Frankreich und Deutschland, sollten so eng wie irgend möglich zusammenarbeiten in Europa. Dazu sind wir fest entschlossen.

Diese Konferenz bietet eine gute Gelegenheit für den persönlichen Austausch, gemeinsame Projekte und neues Vertrauen, und in diesem Sinne wünsche ich dieser Veranstaltung einen erfolgreichen Verlauf. Vielen Dank!


ternational de la Cybersécurité
LE - Mardi 20 janvier 2015
7e Forum International de la Cybersécurité
LILLE - Mardi 20 janvier 2015

Forum international de la cybersécurité
Lille – 20 janvier 2015

M. Jean-Marc Todeschini,
Secrétaire d'Etat auprès du Ministre de la Défense
chargé des Anciens combattants et de la Mémoire

DISCOURS

Mesdames et Messieurs les élus,
Messieurs les officiers généraux,
Mesdames et Messieurs,

Pour ma première participation au Forum international de la cybersécurité, où je représente le ministre de la défense, nous nous retrouvons dans un contexte de crise exceptionnelle, après les attentats terroristes qui ont frappé notre pays. Parmi toutes les analyses qui ont été faites de ces actes odieux, je retiens, pour ce qui nous rassemble aujourd'hui, qu'Internet en a constitué l'un des terreaux évidents.

Internet est source de richesses ; il engendre de nouveaux modèles économiques ; il raccourcit les distances ; il rapproche les hommes et les femmes. Mais Internet permet donc aussi– avec les mêmes caractéristiques – à des individus malfaisants de préparer des actes terroristes, de désinformer, de leurrer, de voler voire de détruire.

La multiplication des cyberattaques que nous constatons à l'heure actuelle confirme plus que jamais la dimension stratégique de la cybersécurité et de la cyberdéfense. Comme vous le savez, depuis les tragiques événements du 7 janvier dernier, des milliers de sites internet en France – de tout type – ont fait l'objet d'une d'attaque informatique. Les sites institutionnels ont été peu affectés par ces attaques. De faible ampleur et souvent de faible technicité, ces incidents n'ont pas eu d'impacts opérationnels. Mais ces attaques sont revendiquées par différents groupes qui affichent leur soutien à Daesh. Nous sommes ainsi au cœur d'un nouvel espace de conflictualité, de confrontation directe.

Le ministère de la défense considère cette nouvelle donne avec la plus

grande attention. En premier lieu parce que le nombre d'attaques subies par le ministère est très important : 756 recensées en 2014. Ce volume est comparable à celui de 2013, mais il convient de noter que les attaques ciblées ont presque doublé, pour passer de 64 en 2013 à 112 en 2014.

Au vu des événements de début janvier, le ministre de la défense a immédiatement pris la décision de mettre en place une structure de crise, qui est dirigée par le vice-amiral Coustillière, et qui s'appuie sur les compétences de tous les organismes du ministère. Les armées en effet, comme les forces de l'ordre, sont engagées dans le combat contre le terrorisme ; elles constituent aussi une cible pour les attaques informatiques. D'ailleurs, si cette cellule de crise a été si rapidement opérationnelle, c'est grâce au travail préparatoire mené notamment lors de l'exercice DEFNET en octobre dernier – j'y reviendrai.

Priorité nationale, enjeu de souveraineté bien identifié par le Livre blanc, la cyberdéfense est donc plus que jamais au cœur de notre action. Devant une menace croissante, que nous pouvons mesurer au quotidien, l'enjeu est de placer le combat numérique au cœur des opérations militaires.

Notre doctrine d'action dans le domaine cyber s'organise désormais autour de quatre grandes fonctions, qui visent à nous protéger, nous défendre, nous renseigner, et agir.

La protection suppose des produits et services de confiance, mais aussi une conception rigoureuse des systèmes. La défense repose quant à elle sur la chaîne opérationnelle de cyberdéfense, qui agit en temps réel pour la sécurité de nos systèmes. Le renseignement, de son côté, nous permet d'anticiper les menaces, d'adapter nos systèmes de défense et de caractériser l'adversaire. L'action, enfin, ce que l'on appelle la « lutte informatique offensive », vient en appui des opérations militaires, dans un cadre juridique qui a été clarifié par la loi de programmation militaire.

Voilà le cadre de l'action que nous menons en matière de cyberdéfense. Je voudrais à présent vous en décrire les modalités concrètes.

Lors du précédent Forum, Jean-Yves Le Drian avait annoncé mettre en place un ensemble de mesures fortes dans le domaine. C'est dans cette perspective qu'il a lancé, en février 2014, le Pacte Défense Cyber. Ce sont « 50 mesures pour changer d'échelle ». C'est le symbole et l'outil d'un projet politique majeur, portée par la loi de programmation militaire 2014-2019, qui consacre – je veux le rappeler ici – plus d'un milliard d'euros à la cyberdéfense.

Les différents axes de ce Pacte sont maintenant bien connus : durcissement du niveau de sécurité des systèmes du ministère ; recrutement de personnels et définition de parcours professionnels adaptés ; renforcement de la communauté nationale de cyberdéfense, en s'appuyant sur un cercle de partenaires et sur les réseaux de la réserve ; enfin, intensification de l'effort de recherche et de formation, avec la création du pôle d'excellence cyber en région Bretagne.

Près d'un an après, toutes ces mesures sont mises en œuvre, et certaines ont déjà trouvé leur aboutissement.

Je tiens d'abord à souligner que le domaine de la cyberdéfense, au sein des armées et du ministère, a atteint un haut degré de maturité et un volume en personnel très significatif. Cette capacité, qui repose sur une expertise technique particulièrement exigeante, tire toute son efficacité des ressources humaines qui lui sont associées, tant en termes de volume que de qualification.

L'entraînement des hommes tient ainsi une place essentielle dans

la montée en puissance de la cyberdéfense. En un an, on constate des efforts considérables et des progrès qui sont remarquables. Je voudrais vous en donner un exemple.

Le premier exercice de la cyberdéfense, l'exercice DEFNET 2014, a eu lieu en octobre dernier aux Ecoles de Saint Cyr Coëtquidan. Ce creuset historique de la formation au combat a ainsi conforté sa place de pilier du pôle d'excellence cyber, pour les entraînements opérationnels de grande ampleur et la gestion de crise. Coëtquidan a montré au passage, avec DEFNET 2014, sa grande capacité d'adaptation et de prise en compte des enjeux nouveaux.

Cet exercice était important, parce qu'il était le premier à jouer, de manière coordonnée, le déploiement de trois groupes d'intervention rapide cyber et l'activation d'une cellule de crise.

Ce modèle d'exercice pourra être reproduit, notamment dans le cadre des futures formations prévues par le Pacte « Défense cyber », en liaison avec le groupe Défense Conseil International, avec qui nous avons signé – cet après-midi même – une convention-cadre relative à la formation et à l'entraînement dans le domaine cyber. Nous pourrons ainsi mieux contribuer à former nos partenaires étrangers. Il y a là un enjeu de sécurité essentiel pour l'avenir.

Il y aura un DEFNET 2015, au mois de mars, qui sera plus ambitieux encore et synchronisé avec PIRATNET 2015, l'exercice gouvernemental du SGDSN qui est conduit par l'ANSSI.

Mais cette formation à la gestion de crise n'est que l'une des facettes du pôle d'excellence que nous sommes en train de bâtir autour de Rennes. La défense a en effet souhaité construire un véritable partenariat entre organismes du ministère, écoles, universités, industriels, et acteurs locaux. Ce partenariat est en train de prendre forme. Le ministre a signé, il y a une semaine, treize conventions avec nos partenaires industriels. Et il y en aura d'autres.

Grâce à ces démarches que nous avons engagées, l'offre de formation va fortement croître. C'est là un chantier essentiel. Les PDG des sociétés concernées disent tous à quel point il est aujourd'hui difficile de trouver des personnels au bon niveau de formation. Des écoles existent, certaines sont présentes ici comme l'EPITA, et l'enseignement délivré y est reconnu comme étant de grande qualité. Mais la demande dépasse largement l'offre. Dans ce contexte, le ministère de la défense apportera sa contribution. Dès la rentrée 2015 un master consacré à la conduite des opérations et à la gestion de crise de cyberdéfense sera ouvert. Il s'appuiera notamment sur le type de mise en situation que nous avons évoqué avec DEFNET. Il sera bien entendu ouvert aux militaires et aux civils de la Défense, mais aussi à des civils d'autres administrations et d'organismes d'intérêt vital. Il s'appuiera sur un socle technique solide, à la pointe de l'expertise nationale, grâce à la collaboration avec la DGA/MI.

En ajoutant les formations délivrées à Sciences Po Rennes, à l'université de Bretagne Sud, au CNAM de Saint Brieux, à l'ENSTA Bretagne, et bien d'autres, c'est donc une offre complète de formation, à la fois cohérente et exhaustive, que nous sommes en train de créer autour de Rennes. Avec l'ambition de toucher l'ensemble de la France.

Former les personnels pour qu'ils soient rapidement opérationnels est donc un enjeu essentiel. Mais il faut savoir également leur offrir des parcours professionnels intéressants. C'est largement le cas au sein du ministère de la défense. Vous me permettrez de le rappeler ici : la variété des métiers offerts par le ministère dans ce domaine est exceptionnelle, depuis la défense de nos systèmes en métropole, jusqu'à l'élaboration des manœuvres cyber les

plus complexes sur les théâtres d'opérations. Sachez-le : en 2015, 41 postes d'ingénieurs sont ainsi créés sur le périmètre de la DGA, et 57 postes supplémentaires de militaires rallieront la capacité de cyberdéfense des armées.

Mais je souhaite que nous allions plus loin, en créant des passerelles entre ministères, avec aussi les industriels et les organismes d'intérêt vital. Je crois que nous avons tous intérêt à ces allers retours, qui sont autant d'enrichissements mutuels. Car nous formons désormais, une même communauté, celle des enjeux cyber.

Je veux d'ailleurs saluer en particulier l'un des acteurs de cette communauté, qui est le Réseau de la réserve citoyenne cyber. Cette réserve, très active, est portée par l'ANSSI, la gendarmerie et l'état-major des armées. Elle incarne le dynamisme d'hommes et de femmes qui s'engagent pleinement au service de la cyberdéfense en apportant leurs compétences et leurs relais aux travaux que nous menons. Mais le ministre va aussi prochainement créer une réserve à vocation opérationnelle. Son volume devrait concerner près de 4500 personnes, qui seront mobilisables en cas de crise majeure en particulier.

Mesdames et Messieurs, les hommes et des femmes, civils et militaires, qui incarnent aujourd'hui la cyberdéfense – qu'ils soient acteurs du combat numérique, de la recherche et développement, de la formation, ou de la réserve citoyenne – participent tous à ce qui est déjà l'une des grandes batailles de ce siècle : la protection informatique des intérêts vitaux de la Nation.

Conscient de ces enjeux, Jean-Yves Le Drian a souhaité que soit mieux reconnu le très haut niveau d'engagement de ce personnel, qui sert sans relâche, souvent dans l'ombre. C'est pourquoi a été prise la décision de créer une nouvelle agrafe « cyber » pour la médaille de la défense nationale qui sera attribuée aux personnels civils et militaires, ainsi qu'aux gendarmes.

Parce que la cyberdéfense est une composante essentielle de la souveraineté nationale, elle appelle une mobilisation collective. Fort du continuum entre la lutte contre la cybercriminalité, la cybersécurité et la cyberdéfense, c'est ensemble, acteurs institutionnels, industriels et citoyens, que nous pouvons aujourd'hui conforter le développement de la communauté nationale cyber, à la hauteur des enjeux qui se présentent à nous.

Comme l'a écrit Saint-Exupéry, « dans la vie, il n'y a pas de solutions, il y a des forces en marche : il suffit de les créer pour que les solutions suivent ». C'est bien le rôle du FIC de mettre ces forces en marche, et je suis heureux que le ministère de la défense y contribue pleinement.

Je vous remercie.

Forum international de la cybersécurité
Lille – 20 janvier 2015

Mme Axelle LEMAIRE,
Secrétaire d'Etat au Numérique

DISCOURS

Je voudrais tout d'abord remercier les organisateurs du Forum International de la Cybersécurité de m'avoir invitée aujourd'hui : la Gendarmerie Nationale, la Région Nord-Pas-de-Calais, le pôle Eura-technologies que je connais bien et la société CEIS.
Je sais l'importance qu'a prise ce rendez-vous :
-en devenant un rendez-vous européen de plus en plus incontournable avec une croissance du nombre de participants assez spectaculaire ; 600 visiteurs en 2008 à Marcq en Baroeul, puis 1000, 1500, 2400, 3000, jusqu'à 4000 aujourd'hui : cette année, vous mettez l'Allemagne à l'honneur
-en devenant un événement qui dépasse la seule sphère régalienne, comme le montre ma présence ce matin en devenant au-delà de la dimension souveraineté qui reste essentielle, un événement économique majeur, et c'est pourquoi je suis au milieu de vous ce matin.

C'est un sujet important car, comme on l'entend souvent, « même les paranoïaques ont de vrais ennemis ». Plus sérieusement, quelques chiffres récents sur le secteur montrent les enjeux auxquels nous faisons face :
-depuis les attaques des 7, 8 et 9 janvier, 1300 attaques[1] ont porté sur 25000 sites français, en lien avec les attentats. Vous savez comme moi que les OIV n'ont pas été touchés et que dans 95% des cas il s'est agi d'alarmer les esprits mais pas vraiment les systèmes d'information. Ces phénomènes sont cependant une piqûre de rappel sur l'importance des dispositifs de sécurité et l'actualisation et la maintenance notamment pour les acteurs publics souvent visés. Il faut plus redouter le vol de données per-

sonnelles ou c'est tout le sens qu'il faut donner aux attaques des organes de presse, surtout en ce moment : bloquer l'accès à un site de journal ou à un compte twitter. Le Monde encore piraté hier soir, Rue89 qui fait l'objet d'intenses pressions depuis de longs mois, c'est porter atteinte à la liberté d'expression.
-en 2014, les attaques ayant pour objectif le cyberespionnage ont augmenté de 200%[2].
-13 milliards d'euros, c'est le poids des acteurs français de la confiance numérique3 sur un marché mondial total de 80 milliards d'euros. C'est dire à quel point nos industries pèsent lourd en ce domaine, et je vais vous dire ce que nous faisons pour les accompagner afin d'aller plus loin encore.

C'est un sujet de souveraineté, de sécurité et défense nationale, et c'est aujourd'hui aussi un sujet économique, pour chaque entreprise française et, de plus en plus, un sujet politique quand des organisations tentent de nuire à nos infrastructures et nos entreprises à cause des idées que notre pays défend.

C'est pourquoi j'ai souhaité venir aujourd'hui vous livrer ma perception de ce sujet. Ces dernières années, la sécurité informatique a été présentée comme une contrainte, un frein à l'innovation et au développement économique. Les discours traitant de ce thème sont parfois encore anxiogènes. Ils font régulièrement référence à l'espionnage, au sabotage, à une cyberguerre hypothétique. Si certains de ces éléments correspondent à une réalité, les nouvelles révélations de documents Snowden il y a quelques jours par la presse allemande nous le rappellent, ils ne sont qu'une partie des raisons pour lesquelles il est nécessaire d'atteindre un niveau suffisant de sécurité informatique.

Si nous voulons entraîner l'adhésion de tous vers cet objectif, il nous faut surtout parler de confiance. Il faut de la confiance dans les infrastructures, dans les produits et les services proposés aux citoyens, aux entreprises ou aux collectivités territoriales pour réussir la transition numérique que nous avons engagée. La confiance doit être un pilier de la République numérique.

Elle repose sur l'ensemble des acteurs du numérique : les chercheurs qui imaginent les objets numériques du futur et doivent donc prendre en compte les questions de sécurité d'usage, les entreprises qui les produisent, l'Etat qui la garantit et sur nous tous qui les utilisons.

Il est de la responsabilité du politique de créer les conditions de la confiance. Vous le savez, des dispositions importantes ont été prises par le Gouvernement pour améliorer la sécurité des systèmes d'information des opérateurs d'importance vitale. Il y a quelques jours je rencontrais mon homologue allemande, Brigitte ZYPRIES. Nous avons décidé de travailler ensemble à la création d'une zone de confiance d'abord binationale puis européenne, pour l'hébergement sécurisé de nos données, « Cloud Secure ». Ces avancées nationales ou bilatérales seront complétées par des orientations européennes portées notamment par la directive « network Information security » (NIS) qui devrait être adoptée d'ici la fin de l'année.

On voit bien que l'attente vis-à-vis du politique est forte. Le Président Obama a, par exemple, récemment exposé les objectifs visés par sa « Cyberbill ». Harmonisation, nodifications des

1- http://ecrans.liberation.fr/ecrans/2015/01/19/plus-de-1-300-cyberattaques-en-france-depuis-les-attentats_1184136
2- http://business.lesechos.fr/directions-numeriques/la-cybersecurite-2014-en-chiffre-63825.php
3- http://dge-et-vous.entreprises.gouv.fr/

failles de sécurité (délais, formats).

Enfin, pour que nos concitoyens et les entreprises aient confiance dans la société numérique, il faut qu'ils soient accompagnés lorsqu'ils sont victimes de malveillances informatiques aux conséquences parfois graves.

C'est pour toutes ces raisons que le premier volet de notre action, c'est le plan cybersécurité, mené par le Directeur général de l'ANSSI, autour de 4 axes principaux, dans le cadre des 34 plans de la Nouvelle France Industrielle :
-Primo, clarifier l'offre en identifiant mieux les prestataires de confiance ;
-Secondo, renforcer certaines offres spécifiques : plusieurs appels à projets ont permis le développement de technologies spécifiques ces dernières années et la cybersécurité reste une priorité des investissements d'avenir ;
-Tertio, améliorer les performances à l'export : ce Forum international en est une belle illustration ;
-Quatrièmement enfin, consolider et soutenir le secteur pour multiplier les champions français – la croissance et le développement des PME innovantes et des start-ups est une dimension essentielle de ma politique économique. Confiance aussi dans les entreprises nouvelles qui cherchent à collaborer avec les ministères ou de plus grosses entreprises.

Ce plan avance, grâce à l'implication des industriels, de l'ANSSI et de la DGE et je veux remercier à nouveau toutes les personnes qui travaillent au quotidien pour faire vivre ce sujet et ce plan industriel.

C'est pourquoi je suis heureuse de pouvoir remettre aujourd'hui les premiers labels France Cybersecurity aux 17 premières entreprises pour contribuer à structurer l'offre de services et de produits de confiance. Cette action, demandée par les industriels comme par les pouvoirs publics, va permettre de valoriser l'offre de produits de confiance.
C'est une démarche saine, qui inclut très largement tous les acteurs de l'écosystème, y compris les associations représentantes des utilisateurs. Ce label est destiné à s'imposer comme une référence reconnue : un gage d'authenticité et une garantie de qualité et de performance des produits et services aussi labélisés.

Maintenant que ce label existe, il est vraiment important de faire sortir la question de la cybersécurité des cercles d'experts du sujet En effet, la protection face aux attaques informatiques est l'affaire de tous : aucune entreprise n'est épargnée par les attaques informatiques (PME, grand groupe), aucune administration. Les menaces sont diverses et les réponses également : comme toujours en matière de sécurité, il faut suivre des procédures rigoureuses pour évaluer les besoins et définir les réponses les plus adaptées et cela exige une diffusion de la culture de sécurité informatique. C'est un domaine qui demande une formation et une sensibilisation de tous les acteurs de l'entreprise : employés, patrons, fournisseurs, clients. Ce label mais également les travaux menés par plusieurs institutions françaises au premier rang desquelles l'ANNSI, permettront d'améliorer, petit à petit, la prise de conscience.

L'enjeu pour vous, industriels et professionnels de la cybersécurité, c'est de parvenir à parler le langage des entreprises et des utilisateurs « normaux », de comprendre leurs contraintes et leurs besoins pour apporter les réponses les plus simples et les plus complètes.

Nous avons lancé plusieurs initiatives en ce sens :
-Le quatrième appel à projets des investissements d'avenir sur la cybersécurité comprend le thème « offre intégrée de sécurité pour les PME » : l'objectif est d'encourager l'industrie à se mobiliser pour pouvoir mettre à la disposition des PME des dispositifs de sécurité clés en main ergonomiques et simples d'uti-

lisation, afin que la sécurité soit discrète ;

-De même, il faut mieux intégrer les questions de cybersécurité aux initiatives nationales de diffusion du numérique ou de soutien à l'écosystème, pour que la question soit systématiquement prise en compte :
La French Tech, comme le montre la présence d'Euratechnologies dans l'organisation de cet événement
L'An II de la French Tech qui vise à rapprocher start-ups et grands groupes, pour lesquels les enjeux de sécurité sont souvent essentiels.

Au-delà de ce besoin évident de sensibilisation, le ministère du numérique et plus largement le gouvernement soutiennent le développement de produits et de services en matière de cybersécurité :
-La cybersécurité est l'un des thèmes forts du CoFIS (comité de filière sécurité) installé par le Premier ministre en octobre 2013 ;
-L'Etat soutient activement le développement de solutions, notamment au travers du programme d'investissements d'avenir : trois appels dédiés à cette thématique ont d'ores et déjà été lancés et ont permis de soutenir environ 20 projets pour un montant total de 100 M€ (dont 30 M€ de financement étatique).

Un quatrième appel à projet est actuellement ouvert, j'en ai déjà parlé.

Puisque vous avez mis l'Allemagne à l'honneur, comme en matière de sécurité des systèmes d'information, nous devons être dans une démarche d'amélioration continue de nos pratiques et je crois que les échanges que nous engageons avec nos partenaires allemands vont contribuer à cette amélioration mutuelle.

Il est de plus essentiel que l'Europe porte un discours ambitieux sur la cybersécurité, pour protéger non seulement nos infrastructures mais également nos valeurs. La stratégie européenne sur le numérique qui sera présenté en mai doit y faire une large place, en commençant par l'adoption de la directive NIS.

Je vous remercie.

Forum international de la cybersécurité
Lille – 20 janvier 2015

M.
Major général Richard Lizurey

DISCOURS

Je veux tout d'abord remercier la région de nous accueillir dans ses locaux, des locaux à l'image du domaine cyber qui nous réunit aujourd'hui : modernes, innovants, lumineux, connectés avec ses nouvelles technologies d'information VDI (Voies-Données-Images / réseau de communication intégrant plusieurs flux : téléphone, TV, internet), au sein d'un quartier de Lille central, en plein développement, en perpétuel aménagement. Je veux ensuite remercier l'ensemble des participants – institutionnels, décideurs et professionnels de confiance numérique - à cette 7e édition du Forum International de la Cybersécurité. C'est votre présence, vos échanges, vos partages et retours d'expériences qui font d'ores et déjà, de cette nouvelle édition un succès.

La 7e édition, c'est, dit-on, l'âge de raison.
Oui, et nous pouvons être fier du chemin parcouru en 7 ans, de la maturité du FIC. Nous sommes partis d'une volonté initiale, portée par la gendarmerie nationale, de développer dès 2007 un espace d'échanges entre les différents acteurs de la cybersécurité ; nous avons développé une relation particulière, durable, forte, entre les trois organisateurs de ce forum : la gendarmerie nationale, la société CEIS et la région Nord Pas de Calais. Grâce à la mobilisation forte et inchangée de ces partenaires, le FIC prend d'année en année une dimension plus importante.
… et non ce n'est pas tout à fait l'âge de raison, car 7 ans, c'est aussi le moment où l'imaginaire, qui laisse croire que tout est possible, laisse la place au rationnel. Et nous ne savons que trop que le domaine cyber reste le domaine de tous les possibles, qui n'ont que fi des barrières technologiques, des frontières physiques...

Le monde de la cybersécurité n'est pas seulement national, il est européen, il est international. Et je veux saluer le formidable rayonnement national, européen et international de cette 7e édition du FIC. Je veux notamment souligner la participation au FIC de nombreuses délégations étrangères. Je veux en particulier saluer les représentants des délégations de l'association des gendarmeries euro-méditerranéennes, la FIEP, dont le directeur général jordanien, le général de division Ahmad Ali AL SWEILMEEN ;
La gendarmerie, qui assure cette année la présidence de la FIEP, a en effet souhaité concentrer en 2015 ses travaux sur les défis de la transformation numérique. Chaque jour, des possibilités nouvelles sont ouvertes, qui constituent autant de défis pour nos institutions, tant la technologie transforme la manière d'agir sur le terrain.

« Cybersécurité et Transformation numérique», c'est le thème de cette 7e édition du FIC qui devrait réunir sur les deux jours près de 4 000 cadres et décideurs du domaine de la cybersécurité. La révolution numérique bouleverse notre société toute entière. Elle transforme notre quotidien et notre économie. La transformation numérique constitue également pour nos organisations, entreprises, collectivités ou administrations, un véritable levier de performance. Elle constitue en effet un véritable catalyseur d'innovation ouvrant de nombreuses potentialités et de formidables opportunités comme j'ai pu le mesurer lors de ma visite des divers stands du salon.
La gendarmerie nationale participe activement à ce mouvement en 2015 avec son projet « équipement numérique du gendarme ». Ce projet est mené dans le cadre du plan ministériel de modernisation et en liens étroits avec les divers services du ministère, en particulier la police nationale. Il s'agit, à terme, de doter chaque gendarme d'un équipement numérique mobile afin non seulement d'augmenter ses capacités d'action et sa mobilité, en lui évitant notamment de revenir à la brigade, mais aussi de rechercher dans le même temps davantage de proximité avec la population avec une offre étendue et adaptée ainsi que de nouveaux services.
C'est donc, bien au-delà d'un nouvel outil, le développement de nouveaux modes d'action, d'une nouvelle façon de faire notre métier : l'outil qui sera développé a ainsi d'abord été imaginé, en co-construction, par ses usages ;
C'est naturellement au sein de la région Nord Pas de Calais et plus précisément sur le département du Nord que se déroulera, dès le deuxième semestre 2015, l'expérimentation d'un déploiement pilote de plus de 1 200 équipements au profit des gendarmes de ce groupement.

Ce projet intégrera, dès le début, les problématiques de cybersécurité. Car la transformation numérique ne peut plus être conduite indépendamment de la cybersécurité. C'est le thème de ce 7e FIC et c'est un impératif, une exigence. L'augmentation des cyberattaques visant les entreprises et les ministères régaliens en témoigne, tout comme la forte dimension cyber que revêt désormais toute crise majeure, à l'instar des attentats récents qui ont frappé notre pays.
Pour répondre à ces exigences – lutte contre le cyberterrorisme / cyberdélinquance – et garantir l'état de droit dans le cyberespace, le ministre de l'Intérieur, comme il l'a évoqué ce matin, développe, dans le cadre interministériel fixé par le gouvernement, une politique ambitieuse de lutte contre les cybermenaces.
Il a ainsi confié au préfet Jean-Yves LATOURNERIE – que je salue - la lutte contre les cybermenaces. Coordinateur ministériel, il a pour mission de structurer la montée en puissance du dispositif ministériel, de s'assurer de la mobilisation de l'ensemble des directions, au service de nos concitoyens et de nos entreprises.
A son niveau, la gendarmerie s'est mise en ordre de bataille en

structurant son dispositif et ses capacités existantes. Ce dispositif s'appuie sur des capacités techniques de haut niveau telles que le Centre de lutte Contre les Criminalités numériques (C3N) intégré au sein du Pôle Judiciaire de la Gendarmerie Nationale(PJGN), qui est actuellement en cours de transfert vers la nouvelle caserne de Pontoise.

Le PJGN bénéficiera ainsi de locaux modernes et adaptés, un écrin technologique à la hauteur des défis du XXIe siècle à relever dans les domaines de la police judiciaire et des nouvelles technologies.

Ce niveau d'expertise est complété par un dispositif territorial cohérent et divers partenariats pour répondre localement sur l'ensemble du territoire aux phénomènes liés aux cybermenaces. Je pense notamment à la mise en place de groupes cyber au sein des sections de recherches de gendarmerie implantées au chef-lieu de JIRS. Ce sera ainsi le cas à la SR de Lille dès cet été.

Avec ce dispositif structuré, la gendarmerie est donc en mesure d'agir, de manière graduée, globale et continue de l'échelon local au niveau national, pour assurer la sécurité de nos concitoyens en général et en particulier dans les trois domaines : anticipation, prévention et lutte contre la cybercriminalité.

Un dispositif structuré, mais assurément pas isolé : la gendarmerie n'agit pas seule mais avec un ensemble de partenaires ou de services, notamment la police nationale. Car c'est bien la coordination et les liens, entretenus par les échanges et les contacts réguliers, qui garantissent une meilleure réactivité et une plus grande efficacité en temps de crise. Tous les dispositifs et toutes les structures ne remplaceront jamais la richesse de la relation humaine, des échanges et des contacts. Cette mise en relation, cette réunion des décideurs et des professionnels de confiance numérique pour décloisonner le débat sur la cybersécurité, confronter les points de vue et les retours d'expérience, c'est tout l'enjeu et l'objectif du FIC. Je souhaite donc que cette 7ème édition du FIC offre un cadre d'échanges favorable à la mise en mouvement coordonnée de l'ensemble des acteurs, publics et privés, face à un enjeu majeur tel que la cybersécurité.

Et comme le partenariat unissant les organisateurs du FIC a vocation à s'inscrire dans la durée, je vous donne d'ores et déjà rendez-vous pour la prochaine édition.


MINISTÈRE DE L'INTÉRIEUR
GENDARMERIE
GENDARMERIE NATIONALE
LUTTE CONTRE LA CRIMINALITÉ LIÉE AUX TECHNOLOGIES NUMÉRIQUES
60
260
1000
20
PERMIS INTERNET

P1
Faut-il réinventer la sécurité ?

Animateur :
Michel Picot, journaliste, BFM Business
Intervenants :
Alain Bouillé, président du CESIN
Bruno Brocheton, vice-président du CIGREF
Jacques Marzin, directeur de la DISIC
Michel Van Den Berghe, directeur général de Orange Cyberdefense,
Loïc Guezo, directeur du développement chez Trend Micro

Problématique :
Avant l'émergence du cyberespace, jamais les attaquants n'avaient eu autant l'avantage sur les défenseurs. Nos modèles de défense traditionnels ont donc volé en éclats et se révèlent inadaptés aux évolutions techniques récentes, qu'il s'agisse de la mobilité, de l'informatique en nuage ou de l'internet des objets. On ne parle d'ailleurs plus uniquement de sécurité des systèmes d'information mais de cybersécurité. Simple effet de mode ou véritable changement ? De fait, la protection ne suffit plus. On parle maintenant de défense dans la profondeur, de détection, de réaction aux incidents, mais aussi de résilience grâce à la « sécurité by design » et au « secure coding ». S'agit-il des bases d'un nouveau modèle de sécurité ? Quels en seraient les points clés ? Alors que la complexité des réseaux et systèmes d'information est toujours plus difficile à maîtriser, quelle serait la place de l'humain par rapport aux technologies dans ce nouveau modèle ?

Michel PICOT : Bonjour, l'année dernière j'avais déjà eu le plaisir d'animer cette plénière d'ouverture. Déjà, nous avions constaté la hausse spectaculaire du nombre de cyberattaques dans le monde. Si on parle de cybercriminalité économique, il faut parler de millions, de milliards de dollars de dommages. Dans ce contexte, faut-il réinventer la sécurité ? Faisons un petit tour de table pour commencer. Guillaume POUPARD, vous êtes directeur de l'Agence Nationale de la Sécurité des Systèmes d'Information.

Guillaume POUPARD : Faut-il la réinventer ? Il faut simplement que la sécurité suive l'évolution des usages. La courbe que l'on vient de voir montre que le monde qui

nous entoure est un monde en constante évolution. On a une explosion du numérique, c'est une évidence que de le dire.
La sécurité est là pour permettre l'évolution du numérique, elle n'est pas là pour l'empêcher, bien au contraire. C'est une invention permanente. C'est une évolution très rapide.

Gérard BERRY : Il ne faut pas la réinventer, il faut la comprendre. On a eu un énorme problème en France, un problème historique, qui est que la pensée des gens est vraiment organisée autour des matières et de l'énergie. Toute l'industrie française a été organisée autour des matières et de l'énergie. L'information et l'informatique ont été très largement ignorées au XXème siècle dans notre pays. Or l'information est un levier extraordinaire. Moi, je pensais, quand j'étais petit, qu'en termes de sécurité, il y avait la guerre froide. On nous parlait de mégatonnes de TNT. Je me disais que quelle que soit la puissance de la bombe, de toute façon il ne faut que trois bits pour la lancer et pas plus ! Donc, le levier de trois bits est de toute façon plus important que le levier physique. C'est ce qu'il faut comprendre.
Hormis des domaines comme le renseignement dans les armées, l'information n'est pas du tout quelque chose qui est dans la mentalité des gens. Je travaille avec des parlementaires sur des problèmes de sécurité. Ce sont des gens d'une extrême bonne volonté mais qui n'ont aucune culture, ou dont la culture sur le sujet est proche de zéro.

Michel PICOT : Cela veut-il dire qu'il y a encore un énorme travail à faire en matière de sensibilisation, d'explication selon vous ?

Gérard BERRY : Oui. Cela veut dire que si l'on transpose les raisonnements que l'on fait ailleurs, par exemple dans le domaine de l'énergie, dans le domaine de l'informatique et de sa sécurité, eh bien il ne sont pas valables. Donc, il faut les changer.

Michel PICOT : Nous allons voir comment les changer. Poursuivons ce tour de table avec Jean-Michel OROZCO, président d'Airbus Defense & Space Security. Faut-il réinventer cette sécurité ?

Jean-Michel OROZCO : Non, je ne le crois pas. Ce qui est important, c'est de coller à l'évolution de la menace. C'est à dire qu'il faut être en perpétuelle adaptation. Il ne s'agit pas de mon point de vue de faire un big bang en matière d'invention. Par contre, ce qui s'impose à nous, c'est une adaptation perpétuelle et rapide. Il faut être force d'innovation dans ce domaine-là si l'on veut être capable de suivre l'évolution de la menace. On a affaire à des développements technologiques qui sont exponentiels en nombre d'objets connectés. Nous sommes dans un monde qui évolue et qui sera de plus en plus à l'avantage des attaquants. Alors, il y a peut être quelque chose qu'il faut inventer : c'est le financement.
Je pense qu'il y a une prise de conscience sur le sujet de la sécurité. Mais cela ne veut pas dire qu'il y a mise en place des financements notamment dans les industries, chez les opérateurs d'importance vitale et dans les organisations publiques. Il n'y a pas de free lunch comme disent les anglais. On a compris l'enjeu mais on a n'a pas encore pris les bonnes décisions.

Michel PICOT : Même question pour Franck GREVERIE, directeur général des activités cybersécurité chez Sogeti : faut-il réinventer la sécurité ?

Franck GREVERIE : Je ne pense pas qu'on a réinventé la cybersécurité, mais je pense qu'on l'a sérieusement adaptée ces dernières années. J'aurai donc un point de vue un peu différent. Il faut se rendre compte qu'une évolution profonde des systèmes I.T . et des systèmes industriels s'est produite. Nous ne sommes plus du tout dans le

même monde. Au cours des trois dernières années, il y a eu tellement d'évolutions dans les systèmes IT qu'on ne peut plus faire de la cybersécurité comme on la faisait il y a cinq ans. Cela n'a plus rien à voir en termes d'architecture, en termes d'approches. Je pense qu'il y a un véritable changement dans ce domaine.
Il y a un deuxième changement qui me semble fondamental par rapport à ce que l'on a connu, c'est le fait que les attaques sont de plus en plus sophistiquées. Il y a surtout de la part des hackers une connaissance des systèmes cibles. Une fois qu'ils sont rentrés dans le système, ils ont une capacité à remonter et à naviguer dedans qui est beaucoup plus forte que ce que nous constations il y a quelques années. On doit donc avoir une action dans le domaine de la sécurité, une fois que la personne malveillante est au sein du système. C'est un vrai changement.

Michel PICOT : A vous entendre, il semble qu'il y ait une part de techno et une part de comportement. J'aimerais que l'on essaie de trouver le juste équilibre.
Pour vous, Guy Philippe GOLDSTEIN, consultant, écrivain, je vais essayer de compléter la question initiale, sans rentrer dans des termes anxiogènes. La presse titrait récemment « sommes nous à l'aube d'une troisième guerre technologique ? » Ces derniers jours, on a parlé d'une vague de cyberattaques sans précédent en France. Je participe depuis des années à de nombreuses conférences et j'ai l'impression que cela progresse toujours.

Guy Philippe GOLDSTEIN : Oui, effectivement cela progresse. Juste sur la question des cyberattaques, il faut faire très attention aux termes que l'on utilise. Au cours d'une guerre, il y a un nombre significatif de morts, de destructions industrielles importantes. En revanche lorsqu'il y a des effets de cyberdjihadisme comme on vient de le voir avec des défacements de sites web on est vite très loin de ces destructions. Il faut faire très attention à ne pas s'emballer, il faut bien choisir les termes.
Pour rebondir sur ce qui a été dit précédemment, il est vrai que la technologie évolue extrêmement rapidement, on est dans des effets d'accélération, avec des vagues nouvelles qui vont arriver, en particulier, autour des objets connectés autonomes, à savoir la robotisation de la société. Cela risque d'ailleurs probablement de réduire le coût de réalisation des attaques dites cyberphysiques. Par ailleurs, cela pose des questions en termes doctrinaux de réinvention de la manière de penser la cyberdéfense. On a évoqué au cours de la guerre froide les doctrines de destructions mutuelles assurées. Elles sont malheureusement a priori inopérantes lorsque l'on parle de ce domaine cyberphysique, tout simplement parce que lorsque l'on envoie un missile nucléaire, on sait a priori qui l'envoie et on arrive à en comprendre les effets. Ce n'est pas du tout le cas dans une attaque cyberphysique. Il se pose dans ce dernier cas des questions fondamentales : qui attaque ? Et quel est l'objectif ?

Michel PICOT : Pour rebondir sur ce que vous venez de dire, je m'adresse à Guillaume POUPARD. Le ministre de la Défense avait annoncé la création d'une quatrième armée pour lutter contre les cyberattaques. Il ne s'agit pas de rentrer dans des termes guerriers, mais ce terme est assez fort. Il y a donc une prise de conscience au niveau de l'État ?

Guillaume POUPARD : Ce n'est pas à moi de commenter ce terme. En revanche, cela traduit quelque chose d'important. Tout ce qui est cyberespace devient une réalité y compris pour les forces armées. On ne peut plus conduire d'opérations sans prendre en compte le cyber, pour s'en protéger et éventuellement pour l'utiliser à notre avantage et c'est exactement cela que le ministre promeut. Cela me paraît être du bon sens. Est-ce que la

troisième guerre mondiale est déclenchée ? Je suis également assez prudent sur ces termes là. Une guerre, c'est quelque chose de grave, c'est quelque chose où il y a des morts. Nous n'y sommes pas aujourd'hui. S'il y a une guerre déjà engagée, ce n'est certainement pas celle avec les cyberdjihadistes qui défacent des sites non protégés. On n'est pas dans un non événement mais on n'est certainement pas non plus dans ce que certains médias ont pu avancer.
En revanche, pour élargir le débat, cette guerre est probablement ouverte en termes de maîtrise des données, de maîtrise de l'information, de maîtrise des données personnelles, qui est un sujet extrêmement grave sur lequel il ne faudrait pas se réveiller en se rendant compte qu'on a loupé quelque chose.

Michel PICOT : En parlant de réinventer, on parlait de l'aspect humain. Sur ce tweet qui apparaît à l'écran, le thème de la formation universitaire est abordé. Gérard BERRY, vous avez évoqué la cyberculture. Il serait peut être intéressant de commencer dès l'université pour sensibiliser les jeunes, qui utilisent les réseaux sociaux, dans le cadre de leur formation et de leur faire comprendre les risques qu'ils encourent. N'est-ce pas cela aussi « réinventer la sécurité ? »

Gérard BERRY : Ce n'est pas valable que pour la cybersécurité. C'est valable pour tout ce qui est cyber. A l'heure actuelle, un étudiant arrive au bac en ayant suivi zéro seconde de cours d'informatique, ce qui est peu par rapport aux besoins de sa vie future. Il passera en effet sa vie à être connecté à l'informatique mais aussi au cyber. J'insiste beaucoup sur les objets cyber-physiques parce que ce sont des choses très importantes. J'ai beaucoup travaillé dessus. Nous ne sommes pas seulement dans la sécurité des données, nous sommes également dans la sécurité des personnes, directement. Par exemple, une faculté américaine a démontré qu'il était possible, avec une simple télécommande, de prendre le pouvoir sur 50 % des pacemakers aux États-Unis. Prendre le pouvoir sur un pacemaker cela signifie que l'on prend le pouvoir, assez violemment, sur le physique des gens.
Cette formation intellectuelle est donc indispensable. La plupart des dirigeants français ne savent pas comment fonctionne un système cyber quel qu'il soit. Il y a autre chose de fondamental, c'est le lien entre sûreté et sécurité. Les trous de sécurité sont la plupart du temps de petits bugs apparemment anodins dans des systèmes. Les gens qui fabriquent les systèmes et les utilisent ne s'y intéressent pas. C'est bien par ces bugs que les hackers rentrent. Cela peut être extrêmement violent. Certains personnes pensent que des marques de machine peuvent être mieux protégées que d'autres, mais pas du tout. Les bugs sont partout et les hackers sont très forts. La grande différence entre la sûreté et la sécurité, c'est que pour la sûreté, il s'agit de montrer qu'il n'y a pas de bug, et pour la sécurité il s'agit d'être en capacité de faire face à une attaque.

Michel PICOT : Nous sommes tous acteurs et responsables de cette sécurité, qu'en pensez-vous Guillaume POUPARD ?

Guillaume POUPARD : C'est absolument essentiel. Ce qu'il faut, c'est apporter le bon niveau de maîtrise aux bonnes personnes. Il est hors de question de transformer tout le monde en expert de la cybersécurité. Je suis d'accord sur le constat que quelqu'un qui a un bac+5 dans le domaine du numérique puisse actuellement ne pas avoir eu un seul cours sur la sécurité tout au long de son cursus. C'est anormal. A l'autre échelle, on voit nos enfants qui sont particulièrement à l'aise avec le numérique, c'est intuitif pour eux. En revanche, je ne pense pas que la sécurité soit un élément intuitif. Si le bon niveau n'est pas donné aux bonnes personnes, effectivement on arrive aux difficultés que l'on rencontre aujourd'hui.

Michel PICOT : Sur cet aspect humain y-a-t-il d'autres réactions, Guy Philippe GOLDSTEIN ?

Guy Philippe GOLDSTEIN : Oui effectivement l'importance de la prise de conscience au plus haut niveau est indispensable. Nous avons un exemple extraordinaire avec ce qui s'est passé avec Target aux États-Unis l'année dernière. Une attaque a été initiée sur un objectif qui disposait des équipements, il y avait le logiciel, il y avait Fireeye qui avait bien identifié l'attaque mais la direction générale de l'entreprise s'est endormie au volant. Elle a perdu 150 millions de dollars, le CTO a été viré et un peu plus tard le CO également. On voit donc bien que même lorsque les outils sont là, sans orchestration, sans politique de sécurité au plus haut niveau, cela ne marche pas. D'où l'importance du facteur humain.

Michel PICOT : Il y a donc le facteur humain. Il y a également le facteur technologique. L'idée est de pouvoir les combiner dans un juste équilibre. Il n'empêche que le nombre d'actes de cybercriminalité ne fait que progresser. Je m'interroge quand même. Malgré toutes les technologies déployées, malgré toutes les actions de sensibilisation, il semble que cela n'avance pas. Sans parler d'échec, on a l'impression qu'il y a un coup d'avance chez les hackers.

Franck GREVERIE : Je pense que lorsqu'il y a un véritable échec sur la protection d'une entreprise ou d'une administration, c'est justement parce que le triptyque entre la technologie, les hommes et les processus n'est pas mis en œuvre au moment où apparaît une grosse faille. Ce que vous mentionniez, c'était certes un sujet d'hommes mais surtout en fait un sujet de processus. Sans processus mis en place, il ne faut pas compter sur le seul comportement d'un décideur. Si le processus n'est pas en place, il n'y aura pas de bonne décision. Je pense que c'est avec ce triptyque que la sécurité se renforcera dans les années à venir. Je souhaiterais revenir sur le sujet de la guerre. Moi, je pense que le mot guerre est trop fort. En revanche, la guerre de l'information est un terme plus adapté. Il suffit de se rendre sur le darkweb et de constater ce qui traîne comme information dans cet espace du web. C'est absolument impressionnant en termes de contenus sur l'ensemble des entreprises qui sont dans cette salle. Il est certain que la guerre de l'information a commencé.

Gérard BERRY : Il ne faut pas oublier que nous avons vécu dans une absence de prévention. Par exemple, à la fin du XXème siècle, la plupart des systèmes ont été construits dans la précipitation. C'était une époque où l'on se souciait peu des bugs et des trous de sécurité. Ces systèmes l'ont payé très cher par la suite. Ils sont toujours là. Il suffit de constater le coût de la remise en forme d'Internet explorer, et je ne sais même pas si c'est achevé. Il y avait en effet des points d'accès multiples pour les hackers. Tous les systèmes réalisés dans la précipitation et peu testés sont des opportunités pour les hackers. Dans l'industrie, cela se voit également ; l'exemple de Stuxnet est éloquent. Les systèmes qui sont en place et commandent des usines ont été conçus sans se préoccuper de la sécurité, ils cachent des bugs dont se réjouissent les hackers. Il ne faudrait tout de même pas aider les gens qui souhaitent pénétrer dans les systèmes.

Michel PICOT : Cela veut-il dire que les producteurs de logiciels produisent trop rapidement peut-être ?

Gérard BERRY : Bien évidemment que le producteur a besoin d'agir rapidement. Si vous regardez les applications de téléphones, en quelques années nous sommes parvenus à en produire une centaine de milliers. Cela veut tout simplement dire que dans cette masse de produits, certaines applications ne valent

pas un clou en matière de sécurité !

Franck GREVERIE : Juste un point sur la qualité des logiciels. Je suis frappé par les appels d'offres qui sont proposés. Sur les douze derniers mois, dans deux sociétés différentes, 60 % des appels d'offre avaient des exigences de sécurité. Je trouve que les 40 % qui n'en demandent pas sont très inquiétants. On a donc des clients qui demandent de coder des applications sans exigences de sécurité. On le leur propose en option certes, mais cela veut dire que ce n'est pas rentré systématiquement dans les habitudes. Cela rejoint ce que disait Jean-Michel OROZCO, il faut passer à l'action. C'est bien d'être conscient mais il faudrait aujourd'hui que dans 100 % des appels d'offres, il y ait des exigences de sécurité. Ma deuxième remarque est que la plupart des attaques ont lieu sur les applications. Pendant des années, on s'est focalisé sur la protection des data centers mais 80 % des attaques sont réalisées via des applications. Il faut donc coder correctement et tester ces applications.

Jean-Michel OROZCO : Le constat que nous faisons aujourd'hui trouve ses racines dans les décennies précédentes. Nous sommes aujourd'hui dans une situation où la plupart des industries sont insuffisamment protégées. Dans certains cas on en est à une certaine prise de conscience. Pour certaines industries, on a déjà mis en place des plans, des investissements pour installer des systèmes de sécurité. Pour la plupart des industries on en est encore aux balbutiements de ces plans. Les gens ont conscience qu'il faut faire quelque chose mais ne sont pas encore passés à l'acte. Je crois, pour en revenir à la première question, qu'il faut passer à l'action.

Michel PICOT : Est-ce propre à la France ?

Jean-Michel OROZCO : Non, pour notre part nous travaillons essentiellement en Europe et c'est une problématique que nous retrouvons un peu partout. Les pays anglo-saxons, notamment les États-Unis, sont partis avant nous. Mais je dirais que tout le monde se réveille face à un problème relativement important à traiter.

Michel PICOT : Peut-on prononcer le mot « échec » comme nous le suggère un membre de l'assistance via un tweet ?

Jean-Michel OROZCO : Non, il ne faut pas parler d'échec. Quand on regarde ce que l'on a fait depuis trois ans, on a énormément progressé. Quand je me présentais dans de grandes entreprises, les gens découvraient le principe des cyberattaques. Aujourd'hui, il est rare de trouver des gens totalement vierges de connaissances sur le sujet. Donc, non, il n'y a pas d'échec. Au contraire, on est en mouvement, on progresse, on innove. Mais il y a encore beaucoup à faire. Nous sommes au début d'une histoire qui va durer longtemps. Je reviens sur le caractère exponentiel des développements technologiques, ce sera une lutte sans fin.

Guy Philippe GOLDSTEIN : Échec ou réussite ? Si on regarde simplement les chiffres qui ont été établis sur le SAS sur le coût de la cybercriminalité, on serait autour de 300 à 500 millions de dollars US. C'est un petit peu inférieur à 0,5 % du PNB mondial, c'est certes énorme mais toujours moins que le marché des produits stupéfiants. Il y a certes un problème mais il n'est pas catastrophique. Il faut faire attention.

Sommes nous capables de sortir un logiciel qui a été correctement testé ? Il y a des vraies questions systémiques. Il y a toujours un nombre incompressible d'erreurs. Il y a des programmeurs qui sont capables d'insérer des Easter eggs. On a du logiciel qui communique avec d'autres logiciels et on voit apparaître des comportements auxquels on ne

s'attendait pas : par exemple, le Flashcrash de mai 2010 sur la bourse de New York au cours duquel d'un seul coup des systèmes de trading automatique commencent à se battre entre eux et la bourse perd 10 % en quelques minutes. Il y a une nature du logiciel qui peut être particulière et que d'un point de vue scientifique on a du mal à évaluer aujourd'hui.

Michel PICOT : Gérard BERRY, vous qui travaillez sur ce domaine de la protection, pouvez-vous nous dire s'il y a des solutions technologiques qui vont arriver sur le marché ?

Gérard BERRY : Oui, il y a plusieurs choses. D'abord, la notion de nombre d'erreurs incompressibles par ligne de codes n'est pas vraie. On sait faire autrement. Il existe des compilateurs qui n'ont pas de bugs par construction et c'est mathématiquement prouvé. Il existe des systèmes opératoires qui sont prouvés fiables par rapport à leur fonctionnement. Il existe une très grande recherche en sécurité à travers le monde. Elle a deux grandes composantes. La première c'est la cryptographie, qui est un sujet très ancien, ce sont des mathématiques arbitrairement compliquées. La deuxième qui est moins connue mais plus importante en pratique, ce sont les protocoles de sécurité. Ce sont des protocoles qui permettent de discuter en toute sécurité entre deux machines. Nous avons l'exemple de SSL, bien connu. Ces protocoles sont prouvés dans le principe mais pas en pratique. L'attaque, par exemple, par le virus Heartbleed portait sur une application SSL jugée excellente. On travaille sur des méthodes qui permettent de prouver la théorie, sur des méthodes un peu abstraites. En France, on est assez leader sur ce domaine. On travaille de plus en plus à entrer dans la véritable implémentation. Cette situation n'empêche nullement qu'il y a de bons hackers, ces gens-là sont vraiment très importants. Ces gens-là peuvent être de très bons scientifiques, comme par exemple Adi Shamir, l'inventeur de RSA, qui est un grand intellectuel des maths de la sécurité mais qui a aussi réalisé des attaques extraordinaires, comme le fait d'avoir cassé RSA 4096 bits, une très grande clé, en écoutant le bruit de l'alimentation de l'ordinateur avec un téléphone portable posé à 50 centimètres. Cela lui a suffi à casser la clé RSA ! Il n'y a pas que des mauvais hackers, il y a aussi de bons hackers qui sont extrêmement importants dans les domaines de sûreté. Et c'est du hack tout à fait scientifique, il y en a aussi à l'ENS, nous sommes très bons aussi en France sur ce sujet. Les bons hackers sont essentiels pour trouver ce que les mauvais hackers pourraient faire, et ils sont aussi performants que ces derniers, soyez rassurés.

Michel PICOT : Faut-il considérer la sécurité comme un atout dans la qualité des produits ? La sécurité ne serait-elle pas une sorte de label de qualité, soulignant que le concepteur a misé sur ce domaine ?

Franck GREVERIE : Dans le domaine des logiciels, si vous regardez le Magic-quadrant Gardner, SOGETI est leader mondial du test des logiciels. C'est par la recherche de qualité que cela a commencé. On a associé les tests de sécurité des logiciels à la fois dans les phases de conception et puis également quand les logiciels sont terminés, juste avant l'implémentation dans le système. Donc, le lien entre la qualité et la sécurité est total. La sécurité est une extension du concept de la qualité. Tout cela part d'une même suite logicielle de tests. SOGETI a mis cela en œuvre est c'est essentiel pour le futur de notre industrie.

Michel PICOT : Il semblerait, enfin j'en ai le sentiment, que les entreprises ne souhaitent pas parler de la sécurité, par peur d'être mises en cause. Quand cela va bien, on le dit mais quand cela va moins bien, on se tait.

Guillaume POUPARD : Ça c'est une bonne remarque et je

reviens sur la sécurité des logiciels. Pendant des siècles, on a fait la sécurité par l'obscurantisme, c'est à dire que le but était de cacher les méthodes et d'avoir les choses les plus secrètes possibles. Au début des années 70, on s'est rendu compte qu'il fallait faire exactement l'inverse. Il fallait publier ses méthodes et concentrer le secret dans quelque chose de bien identifié, ce que l'on appelle les clés cryptographiques. Ça, c'est une preuve de maturité. Les gens qui cachent encore la copie sont des gens qui ne sont pas prêts et ils pensent limiter la casse en cachant les choses. Évidemment, il ne faut pas s'arrêter là, il faut aller carrément plus loin.

Je reviens sur les logiciels et sur un tweet, qui évoque la sécurité by design. C'est un terme barbare. La sécurité cela se pense au départ. Rajouter la sécurité par le biais de la sur-couche ou du petit machin qui va permettre la sécurité, cela ne marche pas. Toute la difficulté aujourd'hui est de faire en sorte que les gens qui conçoivent les systèmes, les logiciels, le matériel, les architectures, pensent bien la sécurité dès le départ et ce même si leur métier n'est pas de faire de la cybersécurité. Les objets connectés ont été mentionnés, on a des start-up formidables, en France, qui développent des produits vraiment très innovants. Ce ne sont pas des experts en sécurité, ce n'est d'ailleurs pas ce que l'on attend d'eux. Cependant, nous les alertons en leur disant : « attention, si dans la conception même de ce que vous faites vous ne prenez pas en compte la sécurité, tout ce que vous faites risque alors in fine d'être complètement ruiné ». C'est donc extrêmement dangereux. Ça c'est la première chose. L'autre élément repose sur des tests qui permettent de garantir et d'introduire de la sécurité dans les développements. On a des langages qui sont prouvés, différentes méthodes, des règles de codages qui sont importantes à suivre. Nous disposons également du processus d'évaluation qui permet d'avoir des produits avec de vrais labels pour le coup, des labels de sécurité qui soient reconnus, y compris au niveau international, notamment avec nos amis allemands qui sont présents aujourd'hui. Cela permet à des non spécialistes de la sécurité d'apporter des garanties relativement fortes sur la sécurité produite ou portée par un système.

Michel PICOT : Le général WATIN-AUGOUARD évoquait le débat entre la sécurité et la liberté. Cela nous renvoie à ce que certains nomment le patriot act à la française. Certains le défendent, d'autres disent non. Je voudrais savoir si réinventer la sécurité passe aussi par une nouvelle réglementation ou une nouvelle régulation des libertés sur le web ?

Jean-Michel OROZCO : Je pense qu'on ne peut et ne doit pas restreindre les libertés, c'est évident. La cybersécurité doit prendre en compte ce concept de base qui est non négociable. Quel est l'avenir de la cybersécurité ? Ce n'est pas tant écouter les gens normaux, ce n'est pas tant de tout savoir sur les gens normaux ! La clé de l'avenir, c'est de bien connaître son ennemi. Il s'agit d'être capable d'appréhender ce qu'on appelle les patterns d'attaques, les schémas offensifs, la façon dont un ennemi va attaquer, la façon dont ils font évoluer leurs attaques. La prise de renseignement, ce qu'on appelle en anglais le fret intelligence, est de mon point de vue fondamental pour combattre efficacement des gens qui, par définition, sont là pour vous surprendre et qui ont tout le temps devant eux pour y parvenir.

Michel PICOT : Je crois me rappeler que le président Obama avait demandé aux entreprises victimes d'attaques des notifications d'incidents, d'attaques dans le mois qui suivait leur survenue afin de les répertorier.

Jean-Michel OROZCO : Connaître les attaques existantes constitue un pré-requis. C'est fondamental. Ce qu'il faut parvenir à réaliser, c'est réellement d'être en capacité d'anticiper sur les évolutions. Il s'agit d'être en

capacité de détecter des signaux faibles de nouveaux patterns d'attaque. Cela doit permettre d'être en mesure d'arrêter l'attaque et d'homegainer toutes les défenses que vous pouvez avoir chez vos clients quand vous êtes un fournisseur de systèmes de sécurité.

Guillaume POUPARD : Juste une parenthèse pour rappeler qu'en France, depuis décembre 2013, la loi impose aux opérateurs d'importance vitale, c'est à dire aux opérateurs les plus critiques dans les domaines du transport, de l'énergie et des finances, de notifier ces attaques au Premier ministre, en pratique à l'ANSSI. Le but n'est pas de compter les victimes, on n'en est pas là. Il 'agit de comprendre ce qui s'est passé, de s'assurer que les gens sont capables de répondre aux attaques qui se sont produites, de les aider à qualifier la gravité de ces attaques. Il s'agit également d'organiser une défense collective. Quand on a la chance d'identifier une victime, ce serait dommage de ne pas aller vérifier que d'autres opérateurs ne sont pas eux aussi victimes de cette attaque. Ça, c'est dans la loi française. Contrairement à d'autres pays, nous ne sommes pas dans l'incantation. Il faut noter que nous sommes en tête vis-à-vis de ces opérateurs critiques.

Jean-Michel PICOT : Ces derniers temps, vous devez être plus vigilant. C'est bien ce travail que vous réalisez actuellement ?

Guillaume POUPARD : Notre travail est clairement d'identifier les attaques graves. Le défacement d'un site web, encore une fois, ce n'est pas une attaque grave. C'est un graffiti sur un mur. C'est certes désagréable, cela pose des problématiques de communication mais ce n'est pas grave. En revanche, il ne faudrait surtout pas que ce bruit généré par ces attaques de faible importance masque finalement des attaques beaucoup plus sérieuses qui viseraient à exfiltrer de l'information sensible ou pire, qui viserait à saboter des systèmes industriels qui sont technologiquement potentiellement très vulnérables aujourd'hui.

Michel PICOT : « La création d'un ministère du cyberespace n'est-elle pas désormais une exigence d'État ? » C'est une question posée par tweet. Qu'est-ce que cela vous inspire ?

Guillaume POUPARD : On a un ministère de la Défense, on a un ministère de l'Intérieur, on a un secrétaire d'État au numérique, je pense que nous sommes très bien armés. On a une agence interministérielle qui est là justement pour organiser tous ces travaux. On a beaucoup de personnes de bonne volonté, je pense que nous avons toute la structure nécessaire, il n'y a peut être pas besoin d'un ministère. Charge à nous d'être efficaces face aux nouvelles menaces.

Jean-Michel PICOT : Franck GREVERIE vous voulez réagir !

Franck GREVERIE : Sur l'évolution de la cybersécurité. Il y a deux thèmes sur lesquels je travaille actuellement. Tout d'abord, celui des menaces externes. Il s'agit de travailler sur la création de pièges. Nous partons du principe que le hacker, à un moment, va rentrer dans le système et je cherche à faire en sorte qu'il passe par un endroit précis.
Sur les menaces internes ensuite, nous travaillons sur la détection des comportements anormaux. Il s'agit ici de l'équilibre entre liberté et sécurité. Détecter les comportements anormaux des administrateurs, par exemple, est assez intéressant.

Guy Philippe GOLDSTEIN : Sur le sujet « liberté-sécurité », il y a plusieurs questions. Il s'agit tout d'abord de la liberté d'expression, évidement. Moi, je suis citoyen français et dans les règles de droit que l'on utilise en France, il y a les lois Pleven, Gayssot. J'aimerais que dans l'es-

pace de communication qui est utilisé a minima par le monde français, on n'applique pas les règles américaines mais les règles françaises.

Jean-Michel PICOT : Il y a des textes, mais ne faut-il pas les adapter ? Comment voyez-vous les choses ?

Guy Philippe GOLDSTEIN : Cela veut dire simplement qu'il y a des droits et des principes qui ont été établis par le législateur. Internet est un espace de communication et d'information comme tous les autres espaces de communication et d'information. Les lois et principes qui ont été posés sur les autres espaces, que ce soit les livres, les publications ou autres, doivent également s'appliquer sur Internet.

Jean-Michel PICOT : Internet se joue des lois et frontières nationales, c'est donc peut être un peu plus compliqué ?

Guy Philippe GOLDSTEIN : C'est là effectivement qu'il y a des éléments de friction. Les opérateurs de médias, pour ne pas dire autre chose, qui ne sont pas établis en droit français doivent être pris en compte. Il faut parvenir à faire respecter ce qui est a minima les choses les plus essentielles et qui correspondent aussi à nos valeurs.

Jean-Michel PICOT : Selon vous, il n'est pas nécessaire d'ajouter une dose de réglementation supplémentaire ?

Guy Philippe GOLDSTEIN : Il faut qu'a minima on applique les lois Pleven et Gayssot.

Jean-Michel PICOT : Gérard BERRY, qu'en pensez-vous ? Faut-il ajouter une couche de réglementation ?

Gérard BERRY : Le droit évolue toujours en suivant les faits. On peut faire la comparaison avec le droit maritime. Là aussi, il n'y a pas de frontière. Les lois locales sont donc difficilement opérantes. C'est une des grandes difficultés du domaine, ça c'est certain.
Pour revenir sur un autre sujet, quand on dit que la sécurité est stable, je pense moi que cela n'est pas vrai. En effet, aujourd'hui on ne peut rien supposer sur l'attaquant. Aussi, la notion de test, qui suppose que l'on envisage l'attaquant, n'est pas réalisable. Il faut faire certes de son mieux pour tester la sécurité mais on ne pourra jamais aller au bout. Je pense que les fabricants d'ordinateurs testent leurs matériels de façon fantastique. Cependant, récemment, chez un grand fabriquant d'ordinateur, on a trouvé que, grâce à un nouveau port entrée/sortie, on pouvait casser définitivement la ROM de base et la remplacer par autre chose. Or la ROM de base, c'est celle qui fait démarrer l'ordinateur. En s'y attaquant, on touche aux clés de cryptage de façon irréversible.

Franck GREVERIE : Le sujet, c'était le test de sécurité des applications par rapport à ce que Guillaume a mentionné, c'est-à-dire respecter les règles de codage. En fait, on se rend compte chez les développeurs que les règles de codage sont des règles de sécurité. Mais ces règles sont en fait rarement respectées. Aussi, n'allons pas tout de suite chercher les attaques très sophistiquées. Je prends l'exemple d'un test de sécurité que nous avons réalisé sur une application qui a été compromise dans une grande banque il y a quelques semaines. Les tests ont révélé 32 vulnérabilités critiques des règles de base de codage. En fait, assurons nous déjà, lorsque l'on développe des applications, que les règles de base soient respectées.

Jean-Michel PICOT : Quelles sont les solutions pour améliorer la sécurité ?

Guy Philippe GOLDSTEIN : Il y a encore des questions de prise de conscience et la manière de faire vivre cette prise de conscience qui peut être réalisée par des tests, des simulations, des exercices de wargaming au plus

haut niveau. Il s'agit aussi des moyens de mise en place de ce que l'on appelle la cyber-hygiène pour l'ensemble des citoyens. In fine, nous voyons bien qu'il s'agit de menaces qui nous concernent tous. Ça, ce serait pour la partie cybersécurité. Il y a aussi la cyber défense et on touche ici à des questions doctrinales qui ne sont pas encore tranchées. Il y a aussi des questions qui touchent à la compréhension de la cyberpuissance. On voit bien avec l'épisode du hack de Sony que la capacité à être crédible dans la désignation d'un adversaire, de poser cette vérité là, est une capacité politique extrêmement forte et donc militaire d'une certaine façon. Il y a là une réflexion à poser pour savoir s'il est possible de faire une attribution crédible et qui sera comprise par l'ensemble de la communauté d'une part et d'autre part, il existe une question encore plus complexe : que faire, par exemple, dans le cas de l'attaque sur JP Morgan qui concernait 83 millions de comptes bancaires ? C'est une question importante, une question de stratégie. Thomas SCHILLING parlait des lignes rouge comme étant des éléments de grammaire dans le dialogue de la violence entre les États. Si on ne comprend pas ces éléments de grammaire, alors on est perdu. Si on est perdu, soit on ne fait rien, ce qui a été la stratégie américaine jusqu'aux événements récents avec la Corée du Nord, soit au contraire on risque l'escalade et là c'est un vrai danger.

Jean Michel PICOT : J'aime beaucoup ce terme de « bonne hygiène cyber ». Qu'est ce que cela veut dire ? La bonne hygiène, c'est se prendre en main et surtout sensibiliser les gens à le faire.

Jean-Michel OROZCO : Oui, je crois que vous avez raison. Je pense que l'on a ainsi la réponse à la cyber menace. La réponse est double. Elle est technologique et elle est dans les comportements. Il faut sensibiliser les gens et leur dire de ne pas utiliser comme mot de passe le prénom de leurs enfants. Oui, effectivement, cela existe encore ! C'est la prise de conscience du grand public, des utilisateurs. Je pense qu'il y a également la prise de conscience des décideurs. Il est de mon point de vue extrêmement important d'adopter une démarche pédagogique vis à vis des décideurs des grandes entreprises parce que, à la fin, vous ne décidez pas d'investir dans un problème que vous ne comprenez pas. Il faut donc passer du temps à expliquer avec des mots simples ce dont on parle aux décideurs des grandes d'entreprises.

Jean Michel PICOT : Franck GREVERIE, on a évoqué la partie technologique. La sensibilisation est-elle un travail en plus à réaliser pour améliorer la sécurité ?

Franck GREVERIE : S'agissant des décideurs, je pense qu'ils sont sensibilisés. La question, évoquée par Jean-Michel tout à l'heure, c'est qu'ils doivent passer à l'action. En fait, ils ne passent à l'action que lorsqu'ils ont compris. Ce n'est donc pas parce qu'ils sont sensibilisés qu'ils ont compris. Quand ils ont compris les conséquences que cela peut avoir, alors on peut espérer avoir un budget d'investissement. Moi je fais une grande différence entre sensibilisation et passage à l'action. Ce n'est pas du tout la même chose et on le voit avec les clients que l'on rencontre tous les jours.
Pour ce qui relève de l'évolution des technologies, je porte beaucoup d'intérêt à la détection des signaux faibles, c'est un sujet important. J'insiste également sur la détection des comportements anormaux. La menace ne vient pas que de l'extérieur, elle peut venir de l'intérieur et c'est important de travailler là-dessus.

Jean-Michel PICOT : Faut-il mettre en interne une organisation particulière pour que cela puisse continuer à fonctionner en cas d'attaque ?

Franck GREVERIE : Dans une politique de sécurité, il faut expliquer ce que l'on attend des

gens qui utilisent le système et ce que l'on attend d'un comportement que l'on qualifie de normal. A partir du moment où on a défini ce qu'est le comportement normal attendu de la part des utilisateurs, on peut détecter un comportement dit anormal. Cela doit faire partie des politiques de sécurité de l'entreprise.

Michel PICOT : Est-ce compatible avec le respect de l'anonymat de l'utilisateur ? Quelle est la ligne à ne pas franchir à ce niveau-là ?

Franck GREVERIE : Pour ce qui est des comportements anormaux, travaillons tout d'abord sur les administrateurs IT. Dans une grande entreprise, il y a en moyenne 250 administrateurs IT. On donne à ces administrateurs, répartis dans le monde entier, un certain nombre de privilèges dans les systèmes d'information. Ce n'est pas pour cela qu'il faut les laisser faire n'importe quoi. Il faut donc regarder ce qu'ils font par rapport au système. C'est vital parce qu'on leur donne les clés, la crypto. C'est donc une question importante.

Guillaume POUPARD : Oui, je pense qu'il ne faut pas tout mélanger. Il y a des cas où l'anonymat est fondamental. Là, ce dont on parle, c'est de la sécurité de l'entreprise, l'administration de groupe. Quand vous êtes chef d'entreprise, vos employés ne sont pas anonymes. Déjà pour se connecter, il y a un mot de passe. Le fait de pousser une sécurité basée notamment sur une gestion d'identité propre, des choses de ce type, ce n'est absolument pas contraire à un droit fondamental. On peut sortir de l'entreprise, mais ça c'est un autre sujet. Défendons déjà les bons périmètres.

Michel PICOT : Gérard BERRY, pourriez-vous être plus concret sur la première question de cette table ronde. On a évoqué la sensibilisation, l'organisation. Quel est votre regard sur ces questions ?

Gérard BERRY : La sécurité a toujours été constituée de facteurs humains mélangés à des facteurs techniques. Ce n'est pas nouveau. Ce que peut faire la science dans mon cas, c'est que l'infrastructure soit solide. Il faut comprendre, en termes de sécurité, que si l'infrastructure n'est pas solide, c'est terrifiant. Ainsi, si on fait un code cryptographique cassable, alors c'est le désastre. Il faut donc que l'informatique soit solide. Pour être honnête, tout n'est pas encore fait. Ainsi, certains protocoles de réseaux sur Internet ne sont pas solides. Si vous prenez les réseaux utilisés par les objets cyber-physiques, par exemple dans les voitures, je serais étonné que les protocoles soient solides. Attaquer une voiture, ce n'est pas si compliqué que cela. Une université américaine a montré que l'on pouvait prendre le pouvoir sur les freins et les désarmer facilement, par exemple. Il est important que l'infrastructure soit très solide, elle ne peut pas être laissée aux ingénieurs standards. Il est aussi important de diminuer le nombre d'administrateurs. Il n'est pas logique qu'il y ait autant de gens avec autant de pouvoirs. Par exemple, la crypto à clé publique fait qu'il n'y a pas besoin d'administrateur de clé. Il faut lancer des recherches pour comprendre comment améliorer la technique, notamment celle à grande échelle, pour la rendre plus sûre. Avec les objets, cela va être très sérieux car il y a un coût, les calculs de sécurité coûtent cher et dans les parties qui dépensent très peu d'énergie, ce sera compliqué à faire.

Michel PICOT : On parle de 50 milliards d'objets connectés à l'horizon 2020. Va-ton pouvoir sécuriser tous ces objets ? Le facteur humain sera essentiel. La santé aussi pourra être un enjeu.

Gérard BERRY : Il ne faudra peut-être pas sécuriser tous ces objets . On parle à l'heure actuelle de mettre la santé sur le téléphone portable. Ce n'est pas sur le téléphone portable que se trouve la meilleure sécurité.

Michel PICOT : Que faut-il faire pour que les décideurs comprennent ce qu'est la sécurité de l'information ?

Jean-Michel OROZCO : Si je puis me permettre, pour répondre à cette question, je pense qu'il faut déjà aller les voir. Il faut leur expliquer avec des mots qu'ils peuvent comprendre. Il ne faut pas hésiter à faire des démonstrations. Sur le plan technique, la plupart des fournisseurs de solutions sont en capacité de faire des démonstrations qui ressemblent à un scanner, tout comme lorsque vous allez chez le médecin. Cette démarche peut aider à la prise de conscience. Lorsque vous allez chez un décideur et que vous lui montrez que sa boîte mail est ouverte à tous les vents, il commence généralement à prendre conscience de la gravité du problème.

Michel PICOT : S'il n'y a pas de démonstration, y-a-t-il des mots forts ? Il y a quand même des entreprises qui tombent à cause de problèmes de sécurité, il faut le dire.

Jean-Michel OROZCO : Oui, je crois qu'il y a des sociétés qui ont périclité du fait d'un espionnage économique persistant. Je crois qu'il faut porter à la connaissance des décideurs tous ces cas pour qu'ils réalisent qu'il y a quelque chose à faire dans leur entreprise ou dans leur organisation en général.

Michel PICOT : Le seul hic est qu'il faut investir !

Jean-Michel OROZCO : Oui, il n'y a rien de gratuit. Il faut être conscient que lorsque vous êtes espionné, vous ne sentez pas la douleur tout de suite. La douleur, vous allez la voir arriver dans 2, 3 ou 4 ans. Cela dépend un peu de votre business model. Si vous êtes un vendeur sur internet, la douleur, vous allez la ressentir immédiatement. Si vous êtes une grande entreprise qui a des produits issus d'investissements en recherche et développement, vous ne sentirez pas la douleur tout de suite. On a souvent une vision de court terme. Il faut combattre cette vision. Il faut être bien conscient qu'il s'agit du patrimoine industriel et d'une façon générale du patrimoine étatique. Pour revenir sur le terme de guerre, nous ne sommes pas dans une guerre au sens traditionnel, mais nous sommes dans une guerre économique.

Michel PICOT : Ça c'est clair. Mais quand quelqu'un va voir son décideur pour lui demander de l'argent pour développer, le décideur peut hésiter. C'est compliqué.

Guy Philippe GOLDSTEIN : Juste un point complémentaire. Ce qui fait réagir un décideur, ce peut être également le coût de l'investissement dans la sécurité par rapport aux risques.

Guillaume POUPARD : Un petit témoignage sur ces décideurs que l'on présente souvent comme des responsables. Je rencontre pas mal de PDG. Ils ne se posent pas la question de savoir s'il y a une menace, ils savent qu'elle existe. Ils veulent savoir comment ils peuvent se défendre. La question de mise en doute de la menace est une question qui se posait il y a quelques années. Aujourd'hui, il faut vivre dans une grotte pour ne pas voir qu'il y a une menace. Ces décideurs l'ont très bien compris.

Michel PICOT : Je vous propose de passer à la conclusion de cette table ronde. Mais auparavant pouvez nous dire pourquoi un téléphone portable serait moins sécurisé qu'un PC domestique ?

Gérard BERRY : Le téléphone portable est un appareil récent. Sur les téléphones portables, de nombreuses applications ont été lancées rapidement. Elles vous prennent vos données personnelles. En fait, ces données sont collectées à d'autres fins que l'application en elle-même, pour la publicité par exemple. Les gens sont extrêmement tolérants par ailleurs. Au final, sur les PC,

on a eu le temps de développer la sécurité alors que sur les téléphones portables les application prennent des droits invraisemblables. Le dernier point est que les gens acceptent beaucoup de choses.

Michel PICOT : Un mot de la fin, si l'on doit garder une idée forte, qu'est-ce que vous diriez ?

Jean-Michel OROZCO : Il faut passer à l'action, encore passer à l'action, toujours passer à action et aller vite, plus vite, encore plus vite.

Franck GREVERIE : Il y a quand même une note positive, on a énormément progressé ces dernières années. Il y a dix ans, sur les sujets de sécurité, on était vraiment au niveau zéro. On a fait énormément de progrès. Aujourd'hui dans 60% des appels à projets il y a des exigences de sécurité. On est au début de l'histoire.

Guy Philippe GOLDSTEIN : Je remets la casquette de l'écrivain. Accélération fulgurante avec une question qui est ouverte : un porte-avions a une durée de vie de quarante ans, dans quarante ans nous ne savons pas dans quel environnement logiciel nous serons. Cela ouvre énormément de questions.

Guillaume POUPARD : Oui, je dirais la même chose avec d'autres chiffres. Regardons dix ans en arrière, cela rend extrêmement modeste. En même temps, je suis très optimiste en considérant la dynamique et l'élan en cours avec des acteurs qui travaillent différemment de ce que l'on fait d'habitude, avec des acteurs privés, des acteurs étatiques, des acteurs étrangers. Tout cela me rend optimiste dans un contexte où la menace est très forte.

Gérard BERRY : Oui, très simplement, les gens n'aiment pas investir dans la prévention. Quand les gens sont mordus, ils réagissent très vite et comme ils vont se faire mordre, cela va fonctionner.

Michel PICOT : Je vous remercie beaucoup, nous allons laisser la place à Monsieur le ministre de l'Intérieur.

P2

Quel rôle pour la cybersécurité dans la transformation numérique ?

Animateur :
Michel Picot, journaliste, BFM Business
Intervenants :
Alain Bouillé, président du CESIN
Bruno Brocheton, vice-président du Cigref
Jacques Marzin, directeur de la DISIC
Michel Van Den Berghe, directeur général de Orange Cyberdefense,
Loïc Guezo, directeur du développement chez Trend Micro

Michel Picot : Bonsoir, merci d'être avec nous pour cette deuxième plénière de la journée : « quel rôle pour la cybersécurité dans la transformation numérique ? ». La transformation numérique modifie en profondeur nos modes de vie, nos entreprises et même nos organisations, je ne vous apprends rien. Le monde physique et le monde numérique se superposent quelles que soient la taille et l'activité de l'entreprise. Je tiens à le souligner, car je suis journaliste sur BFM Business, je rencontre beaucoup de chefs d'entreprise. Même les petites entreprises ont enclenché un processus de transformation numérique parce qu'elles ont compris qu'il y a de nouveaux business et qu'elles sont encore fragiles. Il faut peut-être aussi les conseiller et les accompagner. Cette transformation numérique exige toujours plus de sécurité pour créer ce cadre de confiance nécessaire dans les nouveaux usages, tant par les utilisateurs que par les clients. Alors, quel rôle pour la cybersécurité dans cette transformation numérique ? Elle est souvent perçue comme un frein au progrès. Ne pourrait-elle pas au contraire jouer un rôle d'accélérateur et de facilitateur dans cette transformation ? Elle pourrait aussi, peut-être, instaurer une vraie confiance, qui est la base de tout business.
On va en parler en compagnie de nos invités.
Jacques Marzin, bonsoir, vous êtes le directeur de la Direction Interministérielle des Systèmes d'Information et de Communication (DISIC). Je peux dire, en quelque sorte, le DSI de l'État ? On vous le dit souvent...

Jacques Marzin : Oui, tout à fait, c'est plus simple.

Michel Picot : Quand on parle de

transformation, on pense aux entreprises mais l'État est aussi en pleine transformation numérique. Je crois même que Thierry Mondon souhaite une accélération de cette transformation. Où en êtes-vous actuellement ?

Jacques Marzin : Effectivement, il n'y a pas beaucoup de discours d'où la transition numérique et son accélération soient absentes. Nos hommes politiques ont bien compris que, comme tous les champs de l'activité des relations humaines, l'administration ne pouvait pas échapper à cette généralisation. Aujourd'hui, on a posé des actes forts d'affirmation de l'existence d'un unique système d'information de l'État et non plus de n systèmes d'information ministériels juxtaposés. On a jeté les fondements d'une architecture intentionnelle unificatrice sur ce champ. On est à l'écoute de toutes les actions politiques menées dans le domaine de la simplification puisque c'est, bien évidemment, cela qu'attendent avant tout nos concitoyens et les entreprises, que les procédures administratives soient simplifiées et que nous soyons au service de la satisfaction de leurs besoins en masquant la réalité de la complexité de notre organisation, assez incontournable compte tenu de la taille et du champ des activités de l'État. Il n'y a pas d'échéance fixée. C'est le problème de ces transitions : je me méfie beaucoup de l'annonce des grands soirs d'une transformation. On assiste en fait à l'enclenchement d'une amélioration continue et permanente. Ce n'est pas dans le domaine de la sécurité qu'on pourra dire le contraire. Imaginer qu'un effort de cette importance a une fin serait totalement illusoire. Elle a un ensemble d'échéances courtes, chantier par chantier, sujet par sujet, et non pas un horizon de transformation. La demie-vie de nos applications, au sein de l'État, est de 20 ans. Je parle bien de la demie-vie. On ne va pas annoncer le moment où tout aura été refait, ce n'est pas possible et c'est totalement déraisonnable compte tenu de l'équation économique du pays.

Michel Picot : On parlera tout à l'heure ensemble de la cybersécurité ô combien importante dans la transformation numérique de l'État.
Nous sommes également avec Bruno Brocheton, vice président du Cigref. Votre mission : promouvoir la culture numérique comme source d'innovation et de performance. La transformation numérique est réellement en marche dans notre pays. On voit déjà de nouveaux modèles d'affaire voir le jour...

Bruno Brocheton : Tout à fait. Le Cigref, jusqu'en 2010, visait à promouvoir l'usage des systèmes d'information comme source de création de valeur et d'innovation pour les entreprises. Vous avez vu que nous avons changé « usage des systèmes d'information » avec « culture numérique » et que nous avons enlevé le mot « entreprise » à la fin pour reconnaître le coté sociétal. Nous ne sommes plus le club informatique des grandes entreprises françaises mais un réseau de grandes entreprises, les entreprises étant complètement globales. Nous avons publié plusieurs ouvrages, le premier intitulé « Entreprises numériques », puis d'autres. L'entreprise numérique a une stratégie et un plan d'action dans tous les domaines de son modèle d'affaire, que ce soit le mode opératoire ou la proposition de valeur (le quoi et le comment). Culture numérique, car on a parlé de confiance et d'ouverture. Aujourd'hui, les entreprises doivent être ouvertes sur leur écosystème et la société. Récemment, nous avons publié les neuf tendances, enjeux et défis à l'horizon 2020. Nous travaillons sur des plans stratégiques 2010-2015, 2015-2020 et nous avons une fondation de recherche. Ce que nous avions lancé en 2010 avec une vision 2020 se trouve aujourd'hui beaucoup plus avancé que ce que nous avions prévu dans certains domaines (la mobilité notamment).
Il y a plusieurs façons de parler de la transformation numérique.

La première est très classique. C'est la façon dont on appréhende et dont on tire parti de toutes les nouvelles tendances du marché, des technologies et des usages. Classiquement, il s'agit de la mobilité, du big data, des analytics, de l'Internet des objets, des objets connectés, etc. Plus récemment, si vous allez sur le site Cigref.fr, nous avons essayé de décomposer en offres, enjeux et défis à l'horizon 2020. Il s'agit d'abord de réinventer les modèles d'affaires pour ne pas disparaître. Ensuite, il faut multiplier les partenariats et enfin repenser l'organisation pour innover. Nous avons commencé par trois éléments importants, vous le voyez. Le neuvième élément a été abordé récemment par un cabinet de conseil au sujet de la France et du numérique, il s'agit du e-leadership des dirigeants.

Michel Picot : J'aime beaucoup « réinventer le modèle d'affaire ou disparaître ». En préparant ce rendez-vous, je me suis dit qu'on n'allait peut-être pas parler des entreprises qui n'ont pas entamé cette transformation numérique car elles ne seraient plus là l'année prochaine...

Bruno Brocheton : Cela dépasse le cadre de l'entreprise. Ce sont des questions que l'on se pose aussi dans les services publics. Se sentir menacé dans ses missions les plus fondamentales est aussi un facteur de progrès. Je fais partie de ceux qui considèrent qu'il y a peu de missions régaliennes qui échapperont aux barbares numériques, avec des conséquences sociétales plus lourdes que la disparition d'une entreprise recréée à coté avec un modèle différent. Ce sont des choses qui doivent être prises au sérieux, y compris dans la sphère publique. Je suis assez peu écouté. Des pans entiers de l'administration vivent encore, comme General Motors sans doute, de l'illusion que le navire amiral est absolument indestructible. Il faut que nous soyons vigilants : dans le domaine de la santé, on voit l'Iphone 6 avec sa partie santé embarquée qui montre que ces gens-là n'ont peur de rien. Ils auraient bien tort de se gêner...

Michel Picot : Alain Bouillé, bonsoir, vous êtes le président du Club des Experts de la Sécurité Informatique et du Numérique (CESIN). Vous me disiez en préparant ce rendez-vous : « la transformation numérique, quel vaste sujet... ». De quoi parle-t-on exactement, du numérique au service des utilisateurs, des clients, des usagers ? Pour qu'une transformation numérique soit réussie, par quoi doit-elle passer selon vous ? Par cette brique de sécurité qui inspire confiance ?

Alain Bouillé : D'abord, je vais dire quelques mots sur le CESIN. On n'a pas voulu s'appeler « club des RSSI » mais c'est tout comme. Nous réunissons au sein de notre club presque 200 RSSI d'entreprises et c'est en leur nom que je m'exprime ce soir.
S'agissant de transformation numérique, il faut savoir de quoi on parle. On rencontre de tout dans ce « jargonnage » de transformation numérique. On a tous connu la grande ère des dématérialisations où se posaient les questions de sécurité, de valeur probante de ce que nous faisions dans le monde numérique par rapport à ce que nous faisions dans le monde papier. Cela ne nous rajeunit pas d'en parler, nous faisions déjà de la transformation numérique mais nous l'ignorions. Maintenant, ce que l'on voit apparaître comme phénomène, c'est un mode de transformation numérique du sol au plafond. Ça touche les utilisateurs qui poussent le DSI car ils veulent évidemment utiliser des outils modernes alors que l'entreprise ne peut pas financer des outils aussi performants que ceux qu'ils utilisent à la maison. Je passe sur le sujet des BOYD. Les utilisateurs veulent une transformation de leur mode de travail. Les clients, quand on s'adresse à eux, demandent toujours plus d'accès à de l'information, partout, avec n'importe

quel appareil, 24 heures sur 24 et 7 jours sur 7. Un autre phénomène apparaît parmi les entreprises présentes au club. Ces entreprises se transforment elles-mêmes. Elles ne vont plus nécessairement faire le même métier que dans le monde traditionnel. Il y a une vraie question à se poser pour les entreprises, les DSI, les chefs d'entreprises : quelle est l'entreprise de demain dans ce monde numérique qui n'est pas seulement une question basique de dématérialisation ?

Michel Picot : On verra ce volet cybersécurité qui est une brique incontournable dans cette transformation numérique. Michel Van den Berghe, bonsoir, vous êtes le directeur général d'Orange-Cyberdéfense. Vous avez déclaré dans le Journal du Net : « la cécité en matière de sécurité est très préjudiciable ». Cette phrase est simple et tellement vraie. Est-ce votre travail que d'éclairer les dirigeants dans cette transformation numérique, en les avertissant sur l'importance de cette brique de la cybersécurité ?

Michel Van den Berghe : Nous, acteurs de la cybersécurité, avons la chance formidable, avec la transformation digitale, d'arrêter d'être dans l'après-coup. On nous demande très souvent d'agir après que le phénomène soit passé. Il y a eu le phénomène de la consumérisation, du cloud computing. A chaque fois, on nous a demandé de sécuriser les systèmes une fois le phénomène passé. Aujourd'hui on peut être un acteur au centre de la transformation digitale de nos clients et je pense que la sécurité peut être un facteur différenciateur fort. Quelqu'un qui mettra en place une application dans laquelle il a pris en compte les problématiques de cybersécurité pourra le faire valoir auprès de ses clients. On le voit chez Orange, le grand public commence à s'intéresser à ces questions, de la gestion des données personnelles aux données recueillies sur Internet. On voit qu'aujourd'hui la transformation digitale impose un changement de culture et qu'on a la possibilité, pour une fois, nous, acteurs de la cybersécurité, de participer à cette formidable promesse de la transformation digitale.

Michel Picot : On évoquait ce matin certaines entreprises qui traînent encore des pieds pour investir dans la sécurité. Selon vous, cette sécurité n'est pas maltraitée. Est-elle vraiment prise en considération aujourd'hui ?

Michel Van den Berghe : Je crois qu'il n'y a plus de grand dirigeant qui aujourd'hui se pose la question de la cybersécurité. L'actualité a fait ce qu'il fallait pour sensibiliser à cette question. Les grands dirigeants en sont conscients et dans tous les programmes de transformation digitale, la cybersécurité est prise en compte. De la même manière qu'aucune voiture n'est mise sur le marché sans crash-test, les applications, qu'elles soient dans le domaine de la santé, de la mobilité ou autre, passent par une sorte de crash-test.

Michel Picot : Je vais donner la parole à Loïc Guezo, directeur du développement Europe du Sud chez Trend Micro.

Loïc Guezo : Trend Micro est un éditeur de solutions de sécurité qui accompagne les clients ou les fournisseurs de service dans cette transformation numérique en apportant les briques de cybersécurité qui sont nécessaires. On est un éditeur japonais de sécurité, c'est plutôt positif comme aspect aujourd'hui parce qu'il y a, dans l'ère post-Snowden, un discours de confiance. Les cartes sont redistribuées, brouillées dans certains domaines. Trend Micro existe depuis 26 ans sur cette activité. La transformation numérique a aussi impacté Trend Micro. Historiquement, nous étions une entreprise connue comme fournisseur d'anti-virus. Nous avons accompagné les premières installations de systèmes de messagerie, d'exposition sur le web des entreprises et nous avons transformé toute notre

offre pour accompagner cette mutation vers le cloud computing ou les data centers mutualisés. La chasse aux barbares numériques, tout ce qui est identification des contenus très malveillants, des attaques très ciblées, le partage d'information avec les organismes de gendarmerie ou de police (Interpol, Europol, la DCPJ en France par exemple), ce sont des choses que nous pratiquons. Nous sommes partenaires stratégiques au niveau mondial avec Interpol.

Michel Picot : Depuis l'affaire Snowden, de nombreux efforts ont été faits pour expliquer et rassurer mais il plane toujours quelque chose au dessus de nous, un doute sur la fiabilité des systèmes de sécurisation…

Loïc Guezo : Je suis aussi membre de l'ARCSI (Association des Réservistes du Chiffre et des Systèmes d'Information). Nous sommes dans l'ère post-Snowden. Beaucoup d'informations filtrent, sont rendues publiques et on ne peut que constater l'impact de la NSA sur l'ambiance générale du confort, du bien-être des uns et des autres dans cette transformation numérique.

Michel Picot : Merci pour ce tour de table qui nous a exposé votre approche de la transformation numérique. Maintenant, nous allons nous intéresser à la question, centrale dans cette plénière, du rôle de la cybersécurité dans la transformation numérique. Jacques Marzin, quel est le rôle de la cybersécurité dans la transformation de l'État ? Pas question de dévoiler ici des stratégies secrètes, évidemment… La question est double. Elle est celle de la sécurité pour les utilisateurs (les administrations) mais aussi celle des usagers. Comment abordez-vous cela ?

Jacques Marzin : La question de la sécurité des informations du citoyen, des entreprises ou interne entre les administrations ne se pose pas. S'il n'y a pas de confiance, de sécurisation de ces informations, il n'y a pas de service public. Vous avez sans doute en mémoire le bug de l'administration fiscale, à laquelle j'appartenais alors, l'année où l'on a envoyé la page de gauche de l'avis d'imposition au voisin dans la rue. C'était très localisé et ne touchait que peu de personnes, et nous étions dans l'ère de l'édition papier, mais il s'agissait d'une erreur informatique. A l'heure où chacun veut protéger ses données de santé, ses données fiscales (protégées par la loi), il n'est pas question de lésiner sur la place de la sécurité des systèmes d'information. La question ne se pose pas et l'on investit lourdement, massivement, autour de l'ANSSI, des réseaux de fonctionnaires de sécurité des systèmes d'information dans tous les ministères… On peut dire que la préoccupation est permanente et constante. L'énorme difficulté que nous rencontrons est la mise en équation de cette exigence fondamentale, dans un domaine où on n'en fait jamais assez, avec d'une part la vitesse de la transformation et de la satisfaction de la demande sociale de simplification des services publics, d'autre part avec l'équation économique. Parallèlement, on me demande de faire entre 20 et 40 % d'économies sur la dépense des systèmes d'information de l'État en trois à cinq ans. Je pense que c'est une question à laquelle seront confrontés tous les DSI qui sont dans la salle, comme tous les responsables de la sécurité. Où est le point d'équilibre entre la nécessité de donner confiance à ceux que l'on sert, que ce soit marchand ou pas, et ce que ça représente dans le business model en termes de coûts ? Si c'est pour en arriver à un coût qui n'est plus du tout compétitif par rapport à tous ses concurrent, une entreprise ne fera pas tous ces investissements complémentaires. La difficulté dans la sphère publique est que l'on n'a pas cet étalonnage de parangonnage externe, puisqu'on est un peu seul dans notre genre et qu'on n'a pas de valeur de marché, de marge, de coûts de revient qui sont au cœur des discussions. Selon moi, il est assez simple de

revenir sur une idée, quitte à être iconoclaste dans cette assemblée, que l'usage est quand même au cœur du problème, avant la sécurité. Ça me paraît une question fondamentale, on pourrait prendre des exemples. Il ne faut pas perdre les fondamentaux sur la valeur éminente de l'usage et sur la juste analyse de risque plutôt que le réflexe technologique de l'application d'une solution sécuritaire.

Michel Picot : C'est intéressant. Puisque l'on parle de transformation numérique, il faut bien entendu des usages. On verra comment vous abordez cette question mais Alain Bouillé, vous voulez réagir, ainsi que Bruno Brocheton.

Alain Bouillé : Je pense qu'il y a un sujet important. Cela a été dit ce matin, on a parlé de security by design mais je parlerais de security inside. Ce qui change et doit changer c'est la manière dont on appréhende le problème. Il n'est plus question de bricoler de la sécurité une fois que l'application est à la veille de la mise en production. On fait maintenant de la sécurité , c'est en tout cas ce que je prône dans mon entreprise et c'est ce que nous prônons au CESIN, pensée dès le départ et dans la stratégie numérique de l'entreprise. Nous avons un nouvel ami, le chief digital officer, qui va focaliser tous ces sujets. Il est clair que, dans tous les projets de digitalisation que nous voyons aujourd'hui apparaître dans l'entreprise, la sécurité est prise en compte dès le départ. Nous ne faisons plus, dans l'entreprise qui me paie, une seule livraison d'un applicatif exposé sur le Web sans qu'il ne passe des audits de code, des tests d'intrusion etc. On livre maintenant une sécurité complètement intégrée et c'est un gros travail car il faut former les développeur, que ceux-ci développent proprement. Évidemment, on continue à acheter des boîtiers à tous les marchands présents ici pour palier les failles qui ne manqueront pas d'apparaître. Cependant, on construit « sécurité » désormais. Je voulais juste raconter une petite anecdote qui m'est arrivée la semaine dernière lors d'une discussion budgétaire sur la sécurisation d'un système. Nous étions chez le directeur du budget de l'entreprise et le patron métier couinait car il manquait de moyens pour adresser tous ses problèmes de sécurité. Le directeur budgétaire lui a répondu : « c'est pas mon problème. Si tu n'as pas les moyens de sécuriser ton système, tu arrêtes ton business ! ».

Michel Picot : On a évoqué le terme de cyberculture ce matin, cela veut dire que la sensibilisation a été faite.

Bruno Brocheton : S'agissant de votre question, on considère aujourd'hui que l'avantage compétitif, c'est le management et la valorisation de l'information. Souvent, on écrit que l'information est l'or noir des entreprises. Il faut donc absolument protéger cet actif stratégique sous peine de simplement avoir une énorme crise à la fois de compétitivité et d'image. Je ne vais pas citer un studio de cinéma qui a été attaqué, mais cela a été assez désastreux. Aujourd'hui, les systèmes d'information et les technologues numériques sont dans toutes les fonctions de l'entreprise sans exception. Bien sûr, les processus sont dématérialisés mais cela va au-delà de ça. Les éléments principaux de la propriété intellectuelle sont tous sous forme numérique. Moi, si je suis CIO d'une entreprise leader mondial de l'entertainment, de la télé, etc, je constate que tous les actifs, les films qui sortiront en décembre 2015, que les schémas 3D des parcs d'attraction qui sortiront à Shanghai sont tous en format numérique… Le numérique est aussi une source de risques en lui-même. On ne peut pas avoir un stratégique d'entreprise et un plan numérique, c'est une seule et même chose. Dans le plan numérique, dans les investissements, on ne doit faire aucun compromis. Jacques Marzin le rappelait tout à l'heure, l'actualité est malheureusement

une formidable corde de rappel pour les dirigeants.

Michel Picot : Jacques Marzin demandait aussi quel est le juste équilibre dans les investissements dans la sécurité.

Bruno Brocheton : Comme toutes les entreprises, nous avons une mission, des valeurs et, affichée très clairement, il en est une qui s'appelle « trust and transparency », confiance et transparence en bon français. C'est à dire que l'on ne vend plus seulement du produit, du service, on vend une expérience client qui passe par une personnalisation, laquelle passe par une collecte de données sur le client. On commence à avoir vraiment le coté éthique : qu'est-ce que vous faites de mes données, les protégez-vous réellement bien ? Ca commence à être un élément concurrentiel, différenciant fort. Prouver au client qu'on garantit cette sécurité est un élément aujourd'hui essentiel.

Michel Van den Berghe : Je voudrais réagir car on ne parle pas assez aussi de l'utilisateur. N'oublions pas que ceux qui utilisent nos systèmes d'information sont les enfants de la génération Y, nés dans le numérique dès le départ. Aujourd'hui, dans nos entreprises, nous sommes un peu les sachants, regardez l'âge de ceux qui interviennent sur cette scène. Ceux qui sont derrière les claviers n'ont pas le même âge que nous, on ne peut pas leur raconter la même chose qu'aux anciens utilisateurs. C'est impossible, c'est trop dangereux. Ils sont nés avec le numérique, ils sont avec Facebook, ils sont connectés tout le temps avec le numérique… Si on ne les accompagne pas, ils nous laisseront de coté. Notre rôle de sachant est de les accompagner sur la bonne voie. Le changement ne touche pas seulement la partie logistique et applications, c'est aussi le changement des usagers qui, maintenant, demandent à pouvoir accéder à l'information partout et avec n'importe quel type d'appareil. Il faut réellement le prendre en compte.

Loïc Guezo : La partie technique est très importante. Il y a beaucoup de challenge dans ce que l'on doit faire pour rester au niveau des attaquants. C'est notre métier. Une transformation numérique, c'est majoritairement les usages et les utilisateurs qui sont en face. C'est beaucoup plus difficile d'anticiper et de mettre en place les bons investissements au bon niveau, en technologie mais aussi et surtout en sensibilisation, en transformation des usages. C'est là qu'est la vraie difficulté. Du coté des attaquants, c'est toujours le même discours, c'est facile pour eux de court-circuiter les usages et d'aller taper n'importe où, voler la donnée qui est l'or noir. C'est ce que l'on voit dans notre quotidien. En permanence, 24/24 et 7/7, avec en quelque sorte une dénationalisation des adversaires, la complexité est vraiment dans la mise au carré de ces deux problématiques, la technologie (on y arrive à peu près) et les usages et accélération des techniques d'attaque. C'est de l'humain en quelque sorte.

Alain Bouillé : S'agissant de la question du « combien on investit dans la sécurité », Michel a eu la délicatesse de rappeler notre grande maturité, notre expérience. On a appris depuis toujours qu'il fallait faire des analyses de risques, les classifier… On le fait toujours, on sait où sont les bijoux de la couronne et où il faut mettre de l'argent. Regardons aujourd'hui les motivations des attaquants, avec ce que l'on a vécu ces derniers jours et des motivations relativement inattendues. On peut considérer, comme Monsieur Poupard ce matin, que du défacement de site Web n'est pas grave et que c'est juste un graffiti sur la vitrine. Je suis pas d'accord. Quand une entreprise se fait défacer, et on parlera tout à l'heure de confiance, la confiance est quand même un peu égratignée. Je ne parle pas des petits sites ici ou là, développés à moindre frais et pour simplement présenter tel ou tel organisme ou association.

Je parle des vrais sites marchands. Quand vous vous faites défacer, que vous avez pignon sur rue sur le Web, il est compliqué de remonter la pente. Si on fait de la classification d'information, celle qui est publiée sur le site est par définition non classifiée, publique, ouverte aux quatre milliards d'internautes. Il faut bien quand même, par rapport à cette information, si l'on ne souhaite pas se faire défacer, mettre l'argent qu'il faut pour empêcher les attaquants de venir esquinter le site. La problématique de l'argent à engager, comme je le dis toujours à mon comité de direction, c'est qu'une mauvaise nouvelle coûte cette année beaucoup plus cher que l'an dernier. L'information est de plus en plus dispersée, sans parler du shadow IT et de ce que l'on pourrait évoquer en matière de dispersion de l'information. Si l'on veut effectivement une protection correcte de cette information, il faut mettre de l'argent sur la table.

Loïc Guezo : Je voudrais juste citer une anecdote sur les nouveaux usages et les choses surprenantes. Le mot-clef « FIC 2015 » est monté très haut dans les tendances de Twitter ce matin, notamment pendant l'allocution des ministres. En même temps, il a été utilisé dans des Twitts de pro-djihadistes simplement pour se donner une meilleure visibilité. Ce matin, pendant que les ministres parlaient, ce hashtag « FIC 2015 » était utilisé juste comme annotation pour être associé à l'événement. C'est une exposition publique, on ne peut pas empêcher l'utilisation d'un Twitt mais cette perturbation parallèle est un graffiti d'un nouveau genre. Si vous suivez le fil « FIC 2015 », vous trouvez tout-à-coup des revendications anti-France.

Bruno Brocheton : L'entreprise 2020 à l'ère du numérique doit développer une culture numérique, éviter les fractures, accompagner les nouvelles pratiques, accueillir les nouveaux arrivants, jeunes ou pas. C'est essentiel, cette notion de culture. S'agissant du défacement, je n'étais pas là ce matin mais un site web défacé, et des entreprises dont le plus gros actif est immatériel, j'en connais quelques unes, c'est quelque chose que l'on ne peut pas se permettre. Pour le point d'équilibre, dans toute stratégie, il y a une certaine prise de risque. Il faut par conséquent prendre les risques à l'aune de cette stratégie. Je vais redire très vite les quatre premiers enjeux et défis : réinventer le modèle d'affaire, multiplier les partenariats, repenser l'organisation pour mieux innover et valoriser les données, créer la confiance. Il ne s'agit que d'ouverture du système d'information, que de l'agilité. Si on prend l'aspect budgétaire, il faut faire du privacy by design, du security by design. Je ne sais pas ce qu'est un chief digital officer mais si c'est quelqu'un qui fait du test and learn, du test and adjust et qui, derrière, s'appuie sur des professionnels pour faire tout ce qui est sécurité, ça va. Si c'est quelqu'un qui fait du quick and dirty, il n'a pas sa place dans l'entreprise. C'est un vrai sujet. Il y a des jeunes générations, des gens issus du monde du marketing qui pensent qu'ils peuvent faire comme ils veulent et que Dropbox c'est très bien.

Michel Picot : Jacques Marzin, comment les agents de l'État réagissent-ils à cette double ambition de sécurité et de simplification ? Est-ce compatible ?

Jacques Marzin : Ils sont en première ligne sur ces sujets-là, particulièrement ceux qui sont aux guichets. Ils sont très sensibilisés à ces deux questions, plus aux questions de l'usage que de la sécurité d'ailleurs. Ils vivent quotidiennement la sécurité, plutôt par la voie physique, avec des usagers qui viennent hurler l'insatisfaction qu'ils ont par rapport aux services publics… La difficulté que l'on a le plus, c'est la problématique de la transformation des usages et des systèmes. Il y a une grande attente de leur part pour qu'il y ait davantage de continuité entre ce que font les internautes en matière de

transactions publiques et la visibilité qu'ils en ont au niveau du guichet. Nous avons aujourd'hui, je crois, deux transactions sur trois qui n'aboutissent pas sur mon.service-public.fr parce que c'est trop compliqué sur la dernière page. L'usager va alors à un guichet mais doit tout recommencer depuis le début. Par ailleurs, dans des lieux qui deviennent de plus en plus polyvalents, notamment dans les zones de déprise humaine où les usagers se font aussi rares que les services publics, comment des généralistes peuvent-ils faire face à la complexité sans avoir des systèmes d'information qui les rassurent sur le conseil qu'ils s'apprêtent à donner et qui est souvent pris par le citoyen comme un rescrit, un engagement de l'État. Or il s'agit de choses qui ne sont pas d'un degré de simplicité biblique. C'est donc plus du côté de la transformation que se pose le problème vis-à-vis des agents que du côté de la sécurité.

Michel Picot : Quelles initiatives de l'État pour pousser les PME vers la cybersécurité et qui en a la mission ?

Jacques Marzin : C'est une question à poser à l'ANSSI. L'Agence Nationale pour la Sécurité des Systèmes d'Information a une mission très large au niveau du territoire national sur ces sujets-là. Cela rentre dans les préoccupations des structures régionales mises en place par Mme Lemaire, qui sera là demain. Je leur laisse le soin de répondre à cette question. Je voudrais revenir sur les usages pour noter deux choses. On a l'habitude d'intégrer assez facilement la sécurité dans les grandes cathédrales informatiques. Cela ne pose pas trop de problèmes. Ce n'est jamais pris suffisamment en amont et on découvre un peu tardivement des choses. En revanche, on a plus de mal dans les organisations géantes, comme les nôtres, à accompagner les mouvements d'hyper rapidité. Les mouvements d'hyper rapidité, c'est parfois un texte de loi voté la nuit, sans que nous ne demandions rien à personne. Il faut que l'évolution du système, pas très idéal parfois, soit présente pour le citoyen à une date donnée. On ne va pas poser la pelle pour faire autre chose. On fait du quick and dirty dans un cadre expérimental, hé oui. Pour nous, la difficulté, quand on parle de production, c'est que cela coûte tout de suite dix millions. Un cadre expérimental, ça peut être territorial. Effectivement, la difficulté est alors de réinventer les méthodes d'accompagnement qui font que le sujet sécurité est bien adressé depuis le début. On tâtonne là-dessus. Nous avons des équipes hyper agiles qui font ce genre de chose et nous nous attachons à travailler en hamac derrière elles. Mais derrière elles car elles ne vont pas se laisser perturber par ce type de choses. Leur problème est de régler la question du non-accès au droit. L'accès au RSA-activité, 80 % des demandeurs renoncent à le demander tellement c'est compliqué de l'avoir… On a trouvé, avec l'ANSSI, une organisation pour suivre à la trace ces vigognes du numérique moderne et on essaie de mettre la sécurité au niveau qui correspond à la sensibilité du sujet traité. Je vous assure que la personne qui est en situation sociale extrêmement difficile et qui n'arrive pas à obtenir son droit n'a pas franchement comme priorité la protection de ses données personnelles. Ensuite, il s'agit d'adapter au niveau d'expérimentation qui est en cours puis de l'accompagner progressivement dans la progression du chantier. Ça demande une disponibilité plus continue. On n'est plus dans le domaine cadencé des études effectuées puis discutées dans des comités assez complexes. Le traitement de ces sujets compliqués devient une affaire d'homme dans l'accompagnement permanent, avec ses excès et ses incompréhensions comme dans toute affaire d'homme. Ce que je note, c'est que plus on a cette complexité, plus l'état-major doit s'emparer de ces sujets de régulation, de cette intelligence de la prise en compte des solutions pour faire en sorte que cela dé-

bouche. Quand je dis que ça débouche, c'est-à-dire que l'on ne s'aperçoive pas au bout du compte que les règles que l'on voulait appliquer ne l'on pas été ou ont été ardemment contournées avec toutes les bonnes excuses du monde pour le faire.

Michel Picot : Je comprends bien cette approche. Michel Van den Berghe, dans les solutions que vous apportez, partez-vous du constat que vient de nous exposer Jacques Marzin ? On comprendra mieux le rôle de la cybersécurité dans cette transformation numérique. Simplification, usage, il faut que cela marche, cette cybersécurité ne doit pas être un frein, il faut qu'elle fonctionne, qu'elle donne confiance. Loïc Guezo ?

Loïc Guezo : La cybersécurité, elle doit être un frein, mais pas au sens d'un limitateur, au sens des freins sur une voiture qui permettent de rouler vite en confiance. C'est l'ambiguïté du sujet, du mot. La cybersécurité doit permettre d'ouvrir en confiance et de fermer très vite quand on a détecté quelque chose d'anormal. Dans les usages, aujourd'hui, il y a un socle qui est la généralisation de l'emploi de la cryptographie par exemple. Une cryptographie, c'est important, mais un usage qui deviendrait trop complexe pour la mettre en place, c'est impossible. Il y a vraiment des travaux de fond à faire pour intégrer dans les usages, par exemples, les applications, le recours transparent mais efficace à la cryptographie. C'est un exemple parmi d'autres.

Michel Van den Berghe : C'est un peu ce que l'on essaie de faire aujourd'hui. On a beaucoup parlé de la donnée, devenue le nouvel or noir. La donnée, lorsqu'elle est dans l'entreprise, au sein du data center de l'entreprise, est bien protégée. Quand elle est dans les data centers du code computing, là aussi elle est bien protégée. C'est le transport de cette donnée qui est important aujourd'hui. La donnée est fragile quand elle se promène sur les réseaux. Orange a des choses importantes à apporter au marché en protégeant, en créant ce cercle de confiance. Il n'y a pas de big data sans « big confiance ». C'est pour que la donnée soit protégée à tout moment, quand elle est à l'intérieur du système d'information mais aussi quand elle se promène au niveau d'Internet où les portes sont grandes ouvertes et où tout le monde peut s'insérer dans cette promesse de transformation digitale.

Alain Bouillé : Ceci dit, on traîne un lourd fardeau en matière de sécurité car cela fait quelques décennies que, au fur et à mesure des évolutions des menaces et des attaques, on a joyeusement empilé dans nos data centers des couches de sécurité. Maintenant, je ne comprends plus les schémas réseaux mais quand je les comprenais encore, je me demandais comment les données légitimes passaient au travers de tout ça. Je me disais, ce n'est pas possible, à un moment donné ils doivent débrancher quelque chose pour que ça passe… Trêve de plaisanterie, je pense que nous avons un vrai problème d'intégration. C'est ça notre image de marque aussi, qui est un peu ternie par cette complexité. Je fais appel pour le coup à ces messieurs, il faut absolument que l'on simplifie cette sécurité. Ce sont des travaux qu'un certain nombre de membres du club ont mené. Il est très intéressant de voir que, finalement, on peut faire une meilleure sécurité avec des choses beaucoup plus intégrées. Beaucoup d'éditeurs proposent du tout-en-un. Je n'étais initialement pas trop pour, je considérais que c'était du bricolage de trucs recollés avec une colle à peine sèche. Il n'empêche que l'on n'a pas nécessairement besoin partout de la Rolls Royce. Je me souviens que, lorsque a eu lieu la migration des postes de travail dans mon entreprise, j'ai mis au défi le DSI. Je lui ai assuré que la sécurité des postes de travail, une fois la migration sous le nouveau système d'exploitation effectuée, lui coûterait moins cher. C'est ce

que nous avons fait. Nous avions effectivement quatre ou cinq couches de sécurité embarquées sur le poste de travail, qui faisaient tout. Évidemment, on ne prenait qu'un service par marque et on avait le meilleur du meilleur partout. Quand on a fait ce travail-là, on a simplifié considérablement la sécurité du poste de travail mais on l'a aussi augmentée car on a pris le meilleur parti de cette solution intégrée. On s'attaque aux réseaux et ce ne sera pas simple. On n'est pas condamné à empiler les couches année après année. Je crois qu'il faut aussi s'atteler à ça, c'est un vrai enjeu. On ne peut pas dire d'un coté security by design, security inside si effectivement cette architecture de sécurité nécessite cinquante spécialistes pour être comprise.

Michel Van den Berghe : Je suis d'accord avec Alain mais c'est une question de moyens. Un utilisateur, aujourd'hui, accède à une quinzaine d'applications pour faire son travail. On lui demande un mot de passe différent pour chaque application, mot de passe qu'il doit changer tous les quinze jours, qui doit faire au moins dix-huit caractères...Mettez-vous aujourd'hui à la place du pauvre utilisateur, c'est impossible à gérer. En revanche, quand on est une grande entreprise, qu'on a 100.000 utilisateurs et qu'on décide de mettre en place un programme de gestion du single sign-on, les coûts sont tout de suite exorbitants. C'est tout ce rapport entre la simplification de l'accès à l'information et les coûts engendrés qui est très compliqué pour l'entreprise. Allez demander à votre DGE de mettre plusieurs millions d'euros sur la table juste pour simplifier la connexion aux applications pour l'utilisateur final : cela ne se passe pas toujours de façon très simple.

Bruno Brocheton : Je suis d'accord avec ce qui a été dit. Par expérience, je trouve que sur les sujets de cybersécurité, on n'a pas toujours été très bons par rapport aux investissements. Les seules fois où en parle aux comex, il s'agit d'investissement pour du build, pour la mise en œuvre. On a été assez mauvais parce que l'on redemandait toujours du nouveau build et on ne parlait jamais de total cost of ownership, c'est-à-dire du coût des opérations qui viennent derrière. Le pire, c'était d'avoir les outils et de mal les utiliser, c'est-à-dire d'avoir des milliers de numéros de cartes de crédit ou de nombreux e-mails qui partaient à l'étranger. C'était logué mais on ne le regardait pas, ou alors on faisait simplement exploser les coûts mais on n'en parlait pas. Il y a un vrai sujet de maturité de parler en total cost of ownership. En abordant un peu le sujet technique, je vais vous citer deux choses. Nous avons travaillé avec l'ANSSI, Exatrust, le CESIN et le Cigref sur le nouveau plan cybersécurité ou l'action 33 de la Nouvelle France Industrielle. Dans mes antisèches, j'ai pris les deux premiers titres. Action numéro un : renforcer le niveau de compréhension et la prise en compte, au niveau des dirigeants, des cursus de formation de l'État. Action numéro deux sur laquelle nous travaillons avec le CESIN : placer la cybersécurité au cœur de la gouvernance des entreprises. C'est un vrai sujet. Il s'agit de ne pas passer au comité d'audit du conseil d'administration ou du conseil de surveillance mais vraiment passer pro-activement au conseil d'administration lui-même pour former les dirigeants. La culture, la fonction opérationnelle, ça commence par là.

Jacques Marzin : Je suis d'accord, il faut davantage d'éducation sur les aspects de sécurité, y compris pour les équipes de développement ou d'exploitation. Il faudrait aussi former peut-être davantage les spécialistes de sécurité aux systèmes d'information. C'est toujours pareil : dans la découverte d'un équilibre, il faut que chacun fasse la part du chemin qui lui permet de comprendre les contraintes de l'autre. On progresse dans ce cadre mais il s'agit de plus en plus de disciplines extrêmement spécialisées et on

perd assez vite cette teinture. C'est bien en imbriquant les équipes dans une démarche quotidienne autour des mêmes projets que l'on peut arriver à maintenir ce dialogue essentiel.

Michel Picot : Je voudrais que l'on revienne au rôle de la cybersécurité. J'ai entendu le terme de confiance, d'instaurer la confiance qui est la clef de tout business. Faut-il en parler, finalement, à ses clients, aux usagers ? Faut-il qu'une entreprise, ou l'État dise : « je mets tant d'argent pour que vous ayez confiance en mon système » ?

Alain Bouillé : C'est un sujet essentiel, cette notion de confiance, parce que l'on parle beaucoup ici, au FIC, de sécurité des systèmes d'information, de sécurité informatique. Autant la sécurité informatique, la sécurité des systèmes d'information, ce sont des process parfaitement établis, on a des analyses de risque, on est capables de la mesure, de la tester… Cela reste cependant quelque chose de secret, on ne va pas divulguer ici ou là quel est le niveau de sécurité de telle ou telle entreprise. En revanche, la confiance, il faut en parler parce que c'est quelque chose de complètement subjectif. La confiance, pour moi, c'est dans les usages qu'on la voit. Du coup, comme cette confiance est extrêmement fragile et compliquée, il faut la mériter. Vous vous faites percer un site, vous vous faites voler des données et tout ce que vous avez mis en place pour instaurer une certaine confiance avec les clients et partenaires s'écroule instantanément. Je pense que la confiance, contrairement à la sécurité que l'on va garder secrète et stratégique, doit faire l'objet de publicité de l'entreprise : « venez chez moi, car je suis un organisme de confiance ! ».

Michel Van den Berghe : Dans la confiance, il faut considérer l'ensemble. Pour nous, les responsables sécurité, la problématique c'est la personne qui est entre le fauteuil et le clavier. Aujourd'hui, les pirates s'appuient sur la naïveté des gens. Si l'État doit mettre de l'argent, c'est sur ce point. On l'a fait sur la sécurité routière. Avant, les gens disaient « moi, je conduis bien, ce sont les autres qui conduisent mal ». On a informé le public, on lui a expliqué qu'aujourd'hui, pour avoir cette confiance sur la route, il fallait que tout le monde fasse un effort. Pour la cybersécurité, c'est la même chose. On peut mettre tous les moyens de protection. Si une seule personne dans l'entreprise laisse ouverte une petite issue de secours, les pirates vont s'y engouffrer. S'il doit y avoir de l'argent dépensé aujourd'hui au niveau étatique, qu'il serve aux mêmes campagnes que pour la sécurité routière, pour que le public comprenne que la confiance est remise en cause si un seul la trahit. C'est exactement ce qui se passe actuellement. Toutes les grosses attaques informatiques sont toujours arrivées par un utilisateur qui n'a pas fait attention et a ouvert les portes de son système d'information.

Michel Picot : C'est très intéressant, cela revient souvent. Ce matin, on parlait de formation universitaire à la cybersécurité. On pourrait aller plus loin car la génération Y est née dedans, utilise les réseaux sociaux, donne ses coordonnées sans trop comprendre ce qui peut se passer derrière.

Loïc Guezo : La confiance aujourd'hui, si on parle de cybersécurité, c'est essentiellement des labels, des affichages qui permettent de trouver un terrain de discussion. Affichage au sens de logo, certification pour des paiements de carte bancaire, qualification de produit, critères communs, norme PCI DSS, qualification internationale… C'est un premier niveau, mais si on regarde ce qui se passe avec la Lloyd's , qui positionne le risque cyber comme troisième de ses douze risques majeurs, le forum économique mondial qui vient d'introduire le risque cyber à un niveau très élevé, ce qui va se passer, c'est que demain les

grandes entreprises seront interrogées dans un prochaine assemblée générale d'actionnaires sur le niveau de sécurité mis en place, les processus, les investissements, la part d'investissement en cybersécurité par rapport à l'IT… Votre question était de savoir si l'on doit communiquer sur les moyens financiers engagés. J'ai envie de vous provoquer. La réponse est non. On a une obligation de résultat, pas de moyens. Les clients que l'on a avec nous ont une attente basique, c'est une obligation. Cela va peut-être mieux en le disant, mais quand vous montez dans une attraction d'un parc de loisir, vous êtes en sécurité. Quand vous achetez une voiture, vous êtes en sécurité. Vous partez du principe que, bien évidemment, elle respecte les normes, les labels, etc. Nous, on n'affiche pas nos qualifications, le fait que nous sommes PCI DSS, on respecte les normes, c'est une évidence et c'est une attente légitime de nos partenaires, de nos clients finaux, qu'ils soient B to B ou B to C. Il faut bien sûr mettre des choses dans les rapports annuels, il faut expliquer un peu les bilans, les menaces, les réactions, les accès proactifs, etc. On ne parle pas de la même façon en public, comme nous aujourd'hui, et lorsqu'on est dans les locaux de l'ANSSI et que l'on a laissé son portable à l'entrée. Il faut vraiment ajuster le message. Pas de provocation, pas de prise de position trop extrême...

Michel Van den Berghe : Je suis moins d'accord sur ce qu'a dit Loïc. Regardons le Qatargate : ils était PCI DSS, ils avaient tout ce qui fallait… Aujourd'hui, on voit que l'incident et l'attaque avaient été détectés par le SOC de Target. Ils ont remonté l'information à leur direction générale en leur disant qu'il faudrait arrêter l'ensemble des caisses et moyens de paiement dans tous les magasins, alors qu'on était la veille de Noël. On leur a répondu « écoutes, tu nous écris une note de service et on regardera ce qui peut se passer... ». L'ANSSI dit aux OIV qu'ils ont obligation de détecter les incidents de sécurité. Obligation de détecter, c'est tout simplement impossible. Avec le réseau qu'Orange a aujourd'hui, mondial et de très grande taille, comment voulez-vous qu'on puisse nous obliger à détecter toutes les tentatives d'attaques ? Les lois ne feront rien, les régulations ne feront rien. Ce qu'il faut, c'est informer les gens, former les gens, prendre en compte que tout protéger est illusoire. Il faut que les entreprises capitalisent sur leur actifs sensibles, les protègent et sachent gérer les incidents inévitables, car tout le monde continuera à avoir des incidents.

Loïc Marzin : Dans mon propos, je voulais juste citer l'exemple de la certification comme le premier niveau d'échange qui existe aujourd'hui. Je voulais souligner que c'est insuffisant et qu'il fallait passer à des communications plus institutionnelles d'entreprise pour montrer l'engagement pour la transformation numérique avec de la cybersécurité, justement.

Michel Van den Berghe : Le rôle du RSSI au sein de son entreprise va sortir de la DSI. Il doit avoir une place qui lui permette de dire, quand on remonte des alertes, qu'il faut les prendre en compte car c'est un sujet sérieux. Ce n'est pas encore tout à fait le cas aujourd'hui, je crois.

Michel Picot : Pour le mot de conclusion, faisons un dernier tour de table.

Bruno Brocheton : Le Cigref a travaillé avec un cabinet qui s'appelle Futuribles sur un ensemble de scénarios (menaces externes, opportunités, etc.), avec pour chaque scénario les conséquences pour les entreprises. Il en ressort qu'il faut revoir le rôle du RSSI. Si l'information est un actif stratégique, si le RSSI est cloisonné et qu'on parle de compétences transverses, de projets transverses, doit-il aller vers un rôle de cyberstratégie économique ? C'est un peu un teaser pour la prochaine publication.

Alain Bouillé : Ça tombe bien, le CESIN a été créé pour professionnaliser ce métier de RSSI, le sortir de la soute et lui donner la parole. Souvent, et cela fait un peu mal dans la profession, nous sommes en première ligne pour aller réclamer des budgets au DSI, à la direction générale, en première ligne quand ça se passe mal (on a tous vécu des cellules de crise, notamment la semaine dernière) mais, quand il faut parler de sécurité, on n'a pas le droit de le faire car c'est secret. Le bureau communication ne veut pas qu'on en parle. C'est pour ça que le CESIN a été créé, pour redonner la parole aux RSSI. Je suis convaincu que cette profession va devoir évoluer vers un rôle où le RSSI sera complètement connecté à cette digitalisation. De toute façon, il n'y a pas le choix : si l'entreprise ne le fait pas, ça se passera forcément mal et elle sera très vite rattrapée, non pas par la police mais par les méchants.

Michel Van den Berghe : En début d'année on peut faire des vœux. En tant que fournisseur de service, nous avons a constaté qu'en 2014 nous sommes intervenus en mode « médecin légiste », c'est-à-dire pour aider une entreprise après une attaque et voir de quoi la personne est morte. Mon vœux pour 2015, c'est que nous puissions nous transformer en docteur House, afin d'aider à faire le bon diagnostic pour qu'on puisse anticiper l'attaque et faire en sorte que les gens repartent de l'hôpital sur leurs deux pieds.

Loïc Guezo : Le mot important est « anticipation », pour pouvoir accompagner cette transformation numérique et bien séparer les responsabilités et les actions sur ces sujets. En particulier, il faut travailler avec des prestataires spécialisés dans ces traitements d'incident de sécurité, leur détection, etc. L'entreprise se transforme numériquement vers des nouveaux usages. Ce n'est pas pour autant qu'elle doit devenir son propre « producteur d'énergie de sécurité informatique », si je peux employer cette image. Nous sommes en train de vivre cet ajustement en même temps que nous constatons aussi quelques tourbillons non souhaités avec les événements récents. Le Monde, cet après-midi était encore attaqué. La transformation numérique du journal Le Monde n'avait peut-être pas intégré le fait que des inconnus pouvaient quasiment publier sur le site officiel du journal, au nom du Monde.

Jacques Marzin : Il n'y a pas de fin à cette affaire. Je veux juste terminer par une anecdote. On est en train de développer un composant essentiel pour l'État plate-forme. Ce n'est pas grand-chose à faire, c'est déjà fini, ça a pris trois mois de travail. On ne veut pas gâcher la confiance et aujourd'hui je suis obligé de résister fortement à des volontés de déploiement rapide. En effet, alors que ce composant ne transporte rien, qu'il n'expose aucune donnée personnelle, je sais que s'il ne résiste pas correctement à la première agression qui ne manquera pas d'arriver, la confiance sera perdue. C'est d'autant plus dommage que je ne voudrais pas qu'on aboutisse à la conclusion que des usages anodins nécessitent un très haut niveau de sécurité. Chaque fois que la confiance se perd, on relève l'exigence de sa démonstration et ce n'est pas toujours en adéquation avec la volonté des entreprises et des citoyens de payer moins d'impôts.

Michel Picot : Voilà qui est dit. Merci beaucoup messieurs, merci pour vos éclairages.

P3
Comment créer la « confiance numérique »

Intervenants :
- Michel PICOT, journaliste, rédacteur en Chef, Présentateur du Business Club de France - BFM Business Radio
- Muriel BARNEOUD, présidente de DOCAPOST, filiale du Groupe La Poste
- Guillaume BUFFET, président de Renaissance numérique
- Olivier ITEANU, directeur du Cabinet ITEANU Avocats, dédié au droit des TIC (numérique et communications électroniques)
- Claude REVEL, déléguée interministérielle à l'intelligence économique auprès du Premier Ministre
- Pamela WARREN,

Michel PICOT : On s'est beaucoup posé la question du rôle de la cybersécurité dans la transformation numérique. C'était le thème de la plénière d'hier en fin d'après-midi. On a abordé cette question de confiance numérique et Madame la ministre en parlait tout à l'heure. Mais comment la créer finalement, cette confiance des individus et celle des entreprises, comment l'instaurer, comment la susciter peut-être ? Quelles sont les solutions juridiques et techniques permettant d'assurer cette confiance ? Est-ce que l'exploitation massive des données personnelles, les préoccupations sécuritaires des États et des organisations n'altèrent finalement pas cette confiance ? Sécurité, confiance peuvent-elles aller de pair ? Autant de questions que nous allons poser à nos invités.

Je vais demander à Claude REVEL de venir me rejoindre sur scène, à Palema WARREN de monter également, Muriel BARNEOUD, Olivier ITEANU et Guillaume BUFFET. Merci de venir me rejoindre.

Nous allons ensemble ouvrir un vaste débat et j'ai beaucoup de questions à vous poser aujourd'hui sur ce thème.

Pamela WARREN nous a fait l'honneur d'être parmi nous aujourd'hui, elle s'exprimera en anglais. Nous aurons un peu la vision de ce qui se passe aux États-Unis, je vous donnerai la parole un peu plus longuement tout à l'heure.

Quand on a préparé ce rendez-vous, on s'est demandé ce qu'est finalement la sécurité, la confiance numérique, tout ça nous a un peu préoccupé. Nous allons peut-être commencer par une définition, selon vous, de la confiance numérique. Puis nous demanderons à Pamela WARREN comment est perçue aux États-Unis cette ques-

tion de confiance numérique.
Je propose de commencer par un rapide tour de table pour comprendre, pour vous présenter, mais surtout pour avoir votre définition de cette confiance numérique. Claude REVEL, je commence avec vous, vous êtes à côté de moi, vous êtes spécialiste dans l'intelligence économique et stratégique. On va parler de vos différents travaux. La confiance numérique, comment pourriez-vous la définir ?

Claude REVEL : Je crois que c'est un sentiment qui doit être partagé par trois types de public : les citoyens, les entreprises et l'État. C'est, si vous voulez, le lien entre ces trois parties prenantes qui va créer la confiance. Chacun va devoir se retrouver, le citoyen pour ses données personnelles, les entreprises pour la rentabilité de leurs activités (car c'est de la valeur avant tout) et les États pour des questions de sécurité, de souveraineté et de cadre juridique.

Michel PICOT : On va voir dans un instant, parce que c'est ce qui nous intéresse tous, comment créer finalement cette confiance. C'est un vaste débat, on va essayer de trouver des clés. A vos côté Olivier ITEANU qui est avocat et qui a fondé son propre cabinet depuis une vingtaine d'années. Vous êtes spécialisé dans les droits des TIC pour être précis. Vous, vous me dites que la confiance, ça ne se décrète pas...

Olivier ITEANU : Oui, la confiance... Vous savez il y a un mot qui se rapproche de la confiance, qui s'identifie à la confiance, c'est la foi, la croyance, par les temps qui courent c'est pas toujours terrible, les mots confiance et foi, fides en latin. Les américains ont mis sur leurs dollars «In God We Trust » ça veut tout dire. Nous, on l'a mis dans la loi, ce qui est assez révélateur, la loi pour la confiance dans l'économie numérique. C'est un ensemble de choses. Je vais simplement illustrer le propos avec un média en lequel la totalité de la salle a confiance et qui s'appelle la lettre recommandée avec accusé de réception. Il n'y a rien de moins sécurisé qu'une lettre recommandée AR. Elle est dans tous les codes, le code du travail pour licencier, le code des loyers pour mettre fin au bail, le code des sociétés pour convoquer les actionnaires. Pourtant on ne garantit rien, on reçoit une enveloppe.
Donc c'est de la croyance, un ensemble de choses qui ne se décrètent pas. La sécurité est très importante pour la confiance numérique mais c'est un des éléments de la confiance.

Michel PICOT : Muriel BARNEOUD, on ne l'a pas fait exprès, on n'avait pas prévu qu'on allait parler de la lettre recommandée.

Muriel BARNEOUD : C'était très révélateur.

Michel PICOT : Peut-être une réaction. Je veux juste dire que vous êtes la présidente de DOCAPOST, filiale du Groupe La Poste. Pouvez-vous faire une courte présentation de cette filiale ?

Muriel BARNEOUD : En quelques mots, c'est un acteur économique tout à fait normal. On a une seule particularité, c'est d'être détenu à cent pour cent par La Poste et d'intervenir dans l'univers de la transformation numérique des entreprises et des institutions. On va gérer des solutions de back office auxquelles on va appliquer toutes les procédures, toutes les solutions technologiques dont on dispose aujourd'hui pour permettre de les transposer d'un univers qui était un univers physique, comme une lettre recommandée classique, dans un univers totalement digital avec bien évidemment des solutions de signature électronique, d'identité numérique, d'archivage numérique etc... Nous intervenons sur quelques dizaines de milliers de clients, nous pesons 500 millions d'euros de chiffre d'affaire et nous employons 4 500 per-

sonnes en France et dans le monde.
S'agissant de la confiance, ce que vous disiez, Olivier, est très intéressant et est très complémentaire de ce que disait madame REVEL. Effectivement, la lettre recommandée est un objet de peu de solidité ou de peu de technologie, si on va par là, mais opérée par un acteur de confiance. Et on revient sur cette question d'écosystème. La confiance, c'est un sujet qui est un peu au cœur, qui est le fond de commerce de l'univers de la Poste. Nous, nous nous sommes beaucoup penché sur ce qui la composait et on a trouvé trois piliers dans cette confiance. Le premier c'est la compétence, le deuxième c'est la bienveillance et le troisième c'est l'intégrité. Dans toutes les études que l'on a mené, on a retrouvé ces trois piliers comme des éléments majeurs pour poser la confiance d'un écosystème.

Michel PICOT : On va voir, dans un instant, comment on peut aller plus loin et comment on pourrait donner des clés. On va continuer ce tour de table avec Guillaume BUFFET, du think tank Renaissance Numérique. Pouvez-vous nous en dire un mot pour commencer ?

Guillaume BUFFET : Bonjour à tous, je suis président d'un think tank qui s'appelle Renaissance Numérique. Un think tank, c'est un groupe de réflexion, plusieurs centaines de citoyens, d'acteurs économiques ou politiques qui se sont réunis dans l'objectif de réfléchir à la société à l'ère du numérique. Je ne suis pas là pour défendre les acteurs du numérique, je suis là pour participer à la définition d'une nouvelle société de l'ère du numérique plus vertueuse. Évidemment la question de la confiance est essentielle pour nous. Pour la petit histoire d'ailleurs, il y a plus de 10 ans j'avais co-écrit un rapport au Club Sénat qui s'appelait « la sécurité clé de la confiance dans l'économie numérique ». On y revient aujourd'hui.
Confiance, dedans il y a « con ». Et « con », c'est pas ce à quoi on pense le plus souvent, ça veut dire ensemble. Internet ça s'est construit ensemble. Ça s'est construit entre les citoyens, des acteurs, des chercheurs, des militaires. Par essence, Internet a été un espace de confiance extraordinaire, tel que l'être humain n'en avait jamais vu, parce que c'est un espace où tous les hommes étaient, naissaient libres et égaux en droit. Il se trouve que depuis un certain nombre d'années, un certain nombre d'acteurs institutionnels, voyant cet espace se développer, l'utilisant de plus en plus, ont eu envie et besoin de reprendre la main dessus. On va le dire, ils ont fait apparaître un certain nombre de phénomènes de défiance. J'ai presque envie de définir la confiance par sa contraposée, la défiance. On ne va pas se voiler la face, ce n'est pas un problème d'Internet, c'est aujourd'hui un problème de société. On est dans une société de défiance.
Quatre des principaux candidats à la présidence de la République, il y a deux ans et demi, ont construit leurs discours de campagne sur la défiance. J'ai peur des étrangers, j'ai peur des riches, j'ai peur des banquiers, j'ai peur de je ne sais qui. On vit dans une société où on a peur de l'autre et on dit du mal de l'autre.

Michel PICOT : Vous êtes en train de me dire que les réseaux amplifient ce que l'on vit dans la société de tous les jours, dans le monde physique ?

Guillaume BUFFET : Je suis intimement certain, en tout cas, que ce n'est pas la faute des réseaux s'il y a un problème de défiance dans la société d'aujourd'hui. Et j'aimerais bien que dans notre discussion nous réfléchissions pour trouver comment nous, citoyens, pouvons recréer de la confiance entre nous.

Michel PICOT : C'est le but de cette table ronde. Je voulais d'abord vous donner la parole pour qu'on puisse vous présenter. Pamela WARREN pour

commencer est-ce que vous pouvez nous parler de Palo Alto Networks ?

Pamela WARREN : Palo Alto Networks est une société qui a été créée par des technologues de la Silicon Valley qui ont constaté qu'il y avait des manques dans deux domaines principaux par rapport à la sécurité. Tout d'abord le fait que les applications changeaient radicalement, des applications mobiles aux logiciels, en tant que service, au cloud. Puis, les entreprises, quelles que soient les fonctions de sécurité qu'elles ajoutaient dans le réseau, voulaient toujours être plus sûres et protégées. Ces fonctions de sécurité ne se connectaient pas les unes aux autres. Les inventeurs, les fondateurs, ont créé une plate forme qui s'intéresse à tous les aspects de votre réseau, du web aux e-mails, aux centres de données et depuis les machines virtuelles jusqu'au point d'entrée pour les sécuriser contre des menaces connues et inconnues. Et ces capacités peuvent être corrélées pour qu'elles apprennent les unes des autres.

Michel PICOT : Alors je vais quand même vous demander quelle est pour vous, peut-être, la vision américaine de la confiance numérique, quelle est votre définition ?

Pamela WARREN : Je pense que, d'un point de vue de l'utilisateur, que vous soyez un consommateur, une entreprise, une institution gouvernementale qui fait des activités en ligne, l'idée c'est d'avoir un choix qui peut être personnalisé par rapport aux données que vous partagez, avec qui vous les partagez, la manière dont on les partage, et l'utilisation qui en est faite.
Ce sont des piliers qui ne sont pas différents de ceux de l'Union Européenne et de la France. Ce sont des éléments qui sont importants par rapport à la loi sur la protection des données européennes. On pourrait discuter de la manière dont on protège ça, dont on met ça en application, sur la question du fonctionnement des régimes réglementaires. Mais peut-être qu'on en parlera plus tard dans le débat. On a aussi des directives de sécurité différentes de celles des agences gouvernementales, des industries, des distributeurs dans le cadre de leur activité quotidienne .

Michel PICOT : Rentrons dans le vif du sujet, comment créer la confiance numérique ? Puisque c'est ce qui nous intéresse, on va essayer peut être de donner des clés. Je ne sais pas si on aura vraiment bien exposé le mode d'emploi pour créer cette confiance numérique. Mais j'ai besoin d'avoir vos points de vue, votre opinion.
Guillaume BUFFET nous disait tout à l'heure qu'il faut partir de l'utilisateur, des personnes physiques. Qu'est-ce que vous entendiez par là ? Comment partir de ces personnes physiques ? Ceci dit, on a évoqué aussi la question de l'usage et lorsqu'il y a usage, il y a forcément usager. Comment, quel est le point de départ pour vous, Guillaume BUFFET ? Ensuite je vous donnerai la parole, parce que je voudrais qu'on essaye de définir un schéma un peu plus précis.

Guillaume BUFFET : J'ai la sensation que l'on veut enfermer le citoyen, l'utilisateur, dans un rôle totalement passif dans ces questions. Et donc, comme l'utilisateur est un traité comme mineur, il a besoin d'avoir des outils pour penser à sa place, pour réfléchir à sa place.
Je vais faire un parallèle extrêmement osé. Mais j'ai, comme tout le monde certainement ici, été totalement bouleversé par ce qui s'est passé ces deux dernières semaines. Évidemment par ce qui s'est passé mercredi il y a deux semaines. Mais surtout par ce qui s'est passé dimanche 11 janvier. Et ce qui s'est passé dimanche 11 janvier, c'est 4 millions de citoyens qui se sont levés sans que personne ne leur ai rien demandé. Qui se sont levés essentiellement grâce à Internet et aux réseaux sociaux.

Sans Internet et sans les réseaux sociaux, il n'y aurait pas pu avoir ce phénomène citoyen C'est la preuve que 4 millions de citoyens peuvent avoir un sens des responsabilités, peuvent avoir confiance en chacun d'entre eux, confiance dans leur République et se remuer un peu.
J'ai envie de vous lire deux phrases, je vais être un tout petit peu provocant, je suis désolé, mais il y a beaucoup d'émotion sur ce qui est en train de se passer aujourd'hui: « Nous voulons avoir accès aux ordinateurs car les écoutes sont assez stériles ». « Nous voulons avoir accès aux données informatiques de ceux qui fomentent les réseaux sociaux ». J'avais envie de faire un QCM : est-ce que ces phrases proviennent de la N.S.A ? Est-ce que cela provient de la DGSI et du renseignement militaire ? Pas du tout, c'est le président de la commission des lois de l'Assemblée Nationale qui a prononcé ces deux phrases sur Europe 1, il y a exactement une semaine.
Je crois, et c'est ce que j'essaie de faire passer avec Renaissance Numérique depuis un an, que les clés de la confiance dans le numérique reposent dans la séparation des pouvoirs. Mais aujourd'hui il y a une seule et même personne qui émet les rapports, qui écrit les lois et qui est membre de la commission instaurée pour surveiller et vérifier le fait que l'application de ces lois est la bonne.
Je pense, mais monsieur ITEANU vous êtes mieux placé que moi pour y répondre, je pense qu'il y a une vraie question et une vraie interrogation à avoir sur la sécurité du pouvoir. Et je me tourne vers vous car aujourd'hui il est impossible de parler avec monsieur URVOAS. Il refuse de parler avec la société civile. Pas d'autre question.

Michel PICOT : Le ton est donné. On va essayer de décortiquer un petit peu tout cela. Parce que si je vous suis bien, il faut faire absolument confiance aux usagers à 100 %, donc pas de régulation, pas de sécurisation, etc.... Ils sont assez grands, si j'ai bien compris.

Guillaume BUFFET : Non, non, la responsabilité de chacun est extrêmement importante , la responsabilité de chacun est un facteur clé. Nous ne sommes pas dans un monde de Bisounours et Internet n'est pas un monde merveilleux, ce n'est pas ça que je veux dire. Mais enfermer l'utilisateur dans un rôle totalement passif, je ne crois pas que ce soit la solution.

Michel PICOT : D'accord, alors je vais demander à Claude REVEL peut-être de réagir à ce qui a été dit puis de faire avancer le débat. Je poserai la même question à Olivier ITEANU.

Claude REVEL : D'abord, comment dire, Jean-Jacques URVOAS n'est pas du tout quelqu'un de fermé. Ce n'est pas du tout quelqu'un qui veut enfermer le citoyen dans quoi que ce soit, vraiment pas. Je ne l'ai pas entendu sur Europe1, mais je sais ce qu'il a écrit, dont récemment un rapport de la délégation parlementaire au renseignement parce qu'il en est était le président. Le nouveau président est Jean-Pierre Raffarin.
Par ailleurs, contrairement à ce que vous avez dit, il n'y a absolument pas de confusion de pouvoirs. Il y a des parlementaires et il y a un gouvernement. Les lois sont votées entre les deux mais il y a bien une séparation des pouvoirs. Le président de la délégation parlementaire ne concentre pas absolument tous les pouvoirs. Ça c'est une première chose.
Deuxièmement, je crois, comme je l'ai dit au tout début, que la confiance est un lien et pour qu'il y ait un lien il faut que les éléments du lien soient clairs. Et je crois que ce qui peut éventuellement porter préjudice à la confiance, c'est quand les bases du lien ne sont pas claires, c'est à dire le cadre. Il faut que les règles soient claires, il faut que les responsabilités de chacun soient claires. Et ça, le cadre général,

c'est quand même à l'État de le poser et/ou aux États, puisqu'on n'est pas qu'en France, on est dans l'Union Européenne, on est dans le monde et il faut que l'on ait un cadre commun qui soit la base de la confiance, un cadre qui soit posé au niveau international.
Madame Palema WARREN a dit tout à l'heure qu'en fait, ce qui est important, c'est de savoir, que le consommateur sache. La question de savoir, c'est extrêmement important. Pour savoir, il faut que les choses soient claires. Donc je me répète, un cadre clair connu de tous et transparent. Je vous assure, ça, c'est vraiment le fond et, comme je le connais assez bien, c'est vraiment la position de Jean-Jacques URVOAS.

Michel PICOT : Bien entendu vous prenez la parole quand vous voulez, n'hésitez pas. Olivier ITEANU ?

Olivier ITEANU : Il y a différents niveaux dans la discussion, je terminerai par le niveau business quand même.

Michel PICOT : On va y arriver progressivement, j'essaie d'abord de ramener au point de départ.

Olivier ITEANU : Je vais dire un mot. Effectivement, je suis d'accord avec ce que dit Guillaume, j'ai lu les déclarations de Monsieur URVOAS aussi. On ne fera pas la confiance ni la sécurité sur les réseaux contre les citoyens, ça ne marchera pas.
Deuxièmement, je me rappelle qu'il y a 15 ans, j'étais en contact avec une entreprise semi-publique française, même publique je crois. Ils avaient un problème de dématérialisation et le dirigeant me dit « Écoutez, si là il y a un problème, vous savez, j'appelle le ministère, on m'écrit un décret, c'est réglé ». Mais ça, ça ne marche pas non plus, c'est terminé. Donc je dirai qu'on ne fera rien contre le citoyen.
Maintenant, au niveau business, comment va-t-on construire la confiance pour l'utilisateur ? Je reprendrais ce que disait Pamela. Je crois que le mot, c'est simplicité évidemment, comme acteur de confiance, c'est simplicité. Il y a une erreur à ne pas faire, c'est de penser qu'en mettant de la sécurité et de la sécurité et de la procédure, en empilant les mesures de sécurité et de procédure, on crée la confiance. Pas du tout. On a un très bon exemple, en France, c'est la signature électronique, un décret de 2001. Je pense que le rédacteur du décret ne comprenait pas lui même ce qu'il écrivait. On n'a jamais réussi à incrémenter cette signature. Elle va venir. Elle viendra peut-être du terrain et peut être pas du top-down.
Donc, je crois que le mot pour l'utilisateur (on parlera peut-être après de l'entreprise) c'est le mot simplicité. Soyons simple et ça c'est un message à passer au législateur, au pouvoir exécutif et même au niveau business. Si vous voulez réussir vis-à-vis du grand public, des utilisateurs, il faut de la simplicité.

Michel PICOT : Ce qui veut dire qu'aujourd'hui, il y a peut-être trop de couches réglementaires ? Est-ce que vous craignez qu'il y en ai d'autres dessus ?

Olivier ITEANU : Je suis le représentant d'une association qui s'est constituée à la fin décembre et qui regroupe aujourd'hui une vingtaine de sociétés, Orange vient de nous rejoindre, Open Trust aussi. On a aussi des contacts très avancés avec des grands acteurs. DenyAll est un des fondateur. Cette association s'appelle Cloud Confidence.
Il y a beaucoup de choses à dire sur la réglementation. Aujourd'hui il faut savoir que dans le domaine numérique, c'est à 99 % une transposition communautaire, ça se décide au niveau de la Commission européenne. Je vais simplement dire une chose, après je reviendrai là-dessus car c'est fondamental à comprendre. Le président JUNCKER a interdit à ses commissaires, il y a quelques semaines, de dialoguer, d'échanger avec des lobbys qui ne sont pas

enregistrés à Bruxelles. Et bien, c'est une information de ce matin que j'ai vu sur Twitter, il y a près de 200 lobbys qui se sont enregistrés en quelques jours. J'ai ici le programme de la Commission européenne, l'European cloud strategy. Ils ont produit quatre documents, un sur les niveaux de service, un sur la certification en matière de sécurité, regardez les groupes de travail.
Je suis américanophile, je le dis à Pamela, je ne suis pas du tout américanophobe. j'ai été président du Chapitre Français de l'Internet Society pendant trois ans, j'ai été à l'ICANN. Je connais très bien les Américains. Mais pour aller dans ces groupes de travail, pour influencer la Commission européenne pour aller dans notre sens, il faut des ressources qu'aucune entreprise dans cette salle n'est capable d'engager. Il faut regarder les groupes de travail, ce ne sont que des sociétés américaines, des groupes américains, à l'exception de quelques grands groupes français, Orange, peut être La Poste, qui auront d'énormes difficultés à passer des messages. On pourra revenir là-dessus.
Mais la certification que nous avons créée, une certification faite par un tiers, avec des outils de contrôle tous les ans, va clarifier les choses jusqu'à dire très ouvertement « Je ne suis pas soumis au Patriot Act dans l'offre certifiée ». Nous on peut l'écrire en tant qu'association. Les politiques ne peuvent pas. Vous savez qu'à Bruxelles, quand vous parlez du Patriot Act, on vous dit « Chut ! Ce n'est pas politiquement correct. Arrêtez ».
Il y a beaucoup de choses à dire. Le Safe Harbor est un très bon exemple. La commission européenne a négocié le Safe Harbor avec l'administration américaine pour permettre l'export des donnée à caractères personnelles aux États-Unis. Toutes les sociétés qui ont été visées par SNOWDEN étaient signataires du Safe Harbor. Or, la Commission européenne n'a négocié ni contrôle, ni sanction, il fallait le faire quand même ! Je pense, oui, on est tous protégés par la loi. Oui c'est compliqué aujourd'hui parce que ça se passe ailleurs qu'à notre porte. Il faut peut-être prendre les choses en main. Et c'est ce que nous allons essayer de faire avec Cloud Confident.

Claude REVEL : Je pense que c'est une affaire de dosage. Si on regarde un petit peu ce qui a fait le fondement de la révolution industrielle, on pense toujours aux ruptures technologiques, aux grands changements et à l'apprivoisement de nouvelles énergies. Dans les fondements et dans les soubassements de ce qui a fait cette révolution industrielle, on trouve aussi l'installation d'un cadre posé. Notamment la reconnaissance des droits de propriété, des droits de protection d'un certain nombre d'éléments matériels, de l'individu, et dans un dosage qui donnait à la fois un cadre et une certaine durée. Je crois que ce qui est le plus anxiogène et provoque le plus de défiance dans ces univers de réglementation, c'est l'absence de transparence dans la règle, vous avez raison, mais c'est aussi le foisonnement à la fois arbitraire et irrationnel. Je pense qu'un des éléments très importants d'un écosystème de confiance, c'est de donner de la visibilité et de donner de la constance dans le temps. On a terriblement besoin de se projeter dans une durée qui est une durée longue, nécessairement longue.

Michel PICOT : Et de faire ses preuves. J'ai d'ailleurs lu un tweet là-dessus disant que la confiance passe aussi par là, faire ses preuves.

Guillaume BUFFET : La transparence, elle est là. La transparence, c'est avoir accès aux conditions générales d'utilisation de l'ensemble des services sur Internet. L'ensemble des textes de la loi de programmation militaire ou de la loi antiterroriste sont publics. On peut y avoir accès. Je pense que c'est la limpidité qui est encore plus importante. La transparence est là mais ce n'est pas limpide. Et créer la

limpidité est pour moi essentiel.

Michel PICOT : Je rebondis sur vos propos. La confiance est une question de règles claires. Mais qui est l'arbitre' ? Claude REVEL vous voulez peut-être intervenir? Puis je donnerai la parole à Pamela WARREN.

Claude REVEL : Tout le problème, c'est qu'on ne peut pas raisonner en franco-français. C'est probablement une des raisons de l'absence de confiance, toutes les questions dont on parle se passent évidemment au niveau mondial parce qu'Internet est mondial.
On n'a pas, en France, en Europe et dans les autres pays, forcément la même conception de ce qui doit être protégé, de ce qu'est une donnée stratégique, de ce qu'est une donnée personnelle. Et ça, le citoyen français, comme les autres dans les autres pays, ça le perturbe. C'est pourquoi il faut qu'il y ait des règles internationales. Et nous nous y employons.
L'arbitre, le seul arbitre, ce sont les législations internationales, d'abord européennes et ensuite internationales, mais ça ne peut se faire qu'entre les États.
Madame WARREN a parlé tout à l'heure des guidelines. Je crois qu'il peut y avoir un cadre de régulation très général de la part des États et pas d'un État, tandis que les guidelines par secteurs peuvent être décidées par les professionnels. Je voudrais terminer mon propos en disant qu'il faut être extrêmement présent dans les endroits où se font ces guidelines et ces règles. Les Français, la France et les professionnels français devraient en effet, comme le disait mon voisin, être beaucoup plus présents dans les instances publiques. On bat notre coulpe nous aussi, on devrait l'être beaucoup plus, mais également dans les instances privées. Alors, vous allez me dire que c'est cher, que ce n'est pas facile, etc. Si c'était facile, on le saurait et on l'aurait déjà fait.
Il faut mutualiser, je crois qu'un certain nombre de personnes que je connais dans cette salle en sont totalement convaincues. Il faut mutualiser une présence française pour défendre un certain nombre de choses qu'ont dites tous nos voisins dans les instances européennes et dans les instances internationales. L'Etat est là pour le faire de son côté et sans intrusion dans les droits des citoyens, ce n'est pas le but des États.

Michel PICOT : Pamela WARREN, je vous donne la parole, je la donnerai ensuite à Olivier ITEANU.

Pamela WARREN : Oui je pense à cet événement par rapport à notre position en tant que technologue. Un des défis, par rapport aux réglementations, c'est que, souvent, la plupart des gens qui rédigent les réglementations ne sont pas des technologues. Beaucoup de réglementations que l'on a vues demandent des technologies particulières.
Une autre chose à garder à l'esprit, c'est que la technologie doit changer rapidement. On a parlé de récentes menaces. On sait que l'on doit avancer rapidement du point de vue technologique. Si on se base trop sur la réglementation, on est en retard, il y a des failles, il y a des mauvaises interprétations sur la manière dont la technologie peut être mise en œuvre. C'est pour ça que les lignes directrices sont importantes.
Mais je voudrais parler des gens de la partie processus qui mettent en œuvre les technologies. Je veux donner des exemples que l'on a expérimenté depuis que je travaille à Palo Alto Networks, quand je travaillais pour d'autres fournisseurs de technologie et pour le gouvernement avant dans ma carrière.
Les gens continuent à faire des erreurs, y compris ceux qui mettent en œuvre la technologie. On l'a vu ces dernières années, en particulier aux États-Unis, dans la distribution. La conformité ne nous a pas protégés de ces hackers de grands distributeurs. On a mis en œuvre la technologie (et il s'agit de tech-

nologies de pointe) mais ceux qui les mettent en œuvre utilisent l'ancienne manière. Le filtrage par port doit faire face à des applications qui changent rapidement. Les attaques utilisent de nouvelles applications donc le filtrage par port ne sert plus à rien.
Un autre exemple, c'est le proof of concept. Certains technologues ont expérimenté la même chose et même les agences gouvernementales quand elles veulent avoir une autre vision. Quand ils découvrent quelque chose sur leurs réseaux avec nos technologies ils disent : « Éteignez ça, éteignez ça, je ne veux pas savoir ! » Et donc, quelles sont les ramifications par rapport aux administrateurs de technologie ? Quand ils trouvent quelque chose dans leur réseau, ils ferment les yeux et je ne pense pas que l'on ait vraiment répondu à cette question de manière appropriée mais c'est un défi.
La sécurité, soyons clairs, est très complexe. Il n'y a pas une réponse magique, que l'on parle du point de vue de l'utilisateur ou du point de vue du certificateur : est-ce qu'on a des certifications ? Ce ne sont pas des réponses uniques.
Voilà, je voulais juste faire quelques commentaires, apporter quelques réflexions.

Michel PICOT : Je vous pose une question supplémentaire. Avez-vous le sentiment que nous sommes compliqués, nous Européens, dans l'approche de ces questions de cybersécurité par rapport à ce que vous développez aux États-Unis ? On a vu que nous avons des difficulté à communiquer entre nous, à échanger. Comment nous voyez-vous finalement ?

Pamela WARREN : Je pense que l'on a tous les mêmes défis, indépendamment des réglementations des différents pays ou entreprises. Comment communique-t-on par rapport aux utilisateurs, par rapport aux technologies et à ceux qui les mettent en œuvre ? Je pense que l'on doit avoir un équilibre qui inclut un certain niveau de réglementation. Par exemple, la loi européenne de protection des données est transposable dans chaque pays. Aux États-Unis, plutôt que d'avoir une loi sur la protection des données, on a quarante lois différentes. Cela ajoute un niveau à notre complexité. Bien sûr, le président OBAMA essaie de faire des lois nationales de protection des données. On ajoute une réglementation qui peut donner des lignes directrices, éduquer des utilisateurs et éclairer du point de vue technologique aussi.

Olivier ITEANU : La question est de savoir qui est l'arbitre de tout ça. Dans un État de droit, c'est le juge. Il n'y a pas de discussion là-dessus. D'ailleurs c'est le juge qui, seul aujourd'hui, fait reculer les GAFA, fait reculer les Google et Amazon, etc. Ils sont terrifiés, ils ont peur du juge, donc évidemment ce système s'applique.
Je modérerais ensuite le discours sur la complexité, l'international etc. Quand vous êtes un utilisateur et que vous vous inscrivez sur un site de e-commerce pour acheter votre tablette et que vos données se diffusent ou que vous n'êtes pas livré, vous avez besoin d'avoir un recours immédiat.
Le droit international, d'un certaine manière, je vais le dire très rapidement, c'est sur le plan juridique une absurdité, il n'existe pas. Les directives harmonisent des droits locaux. Les conventions, ce sont des accord au niveau des pays. Mais tout ça, ça descend sur le terrain et sur le terrain, il y a des recours.
Parlons un peu de la transparence dont parlait Guillaume BUFFET. C'est vrai que les contrats sont en ligne, tout est en ligne, les conditions générales, etc. Mais 99 % des gens, moi y compris, ne les lisent pas. Souvent, en tant qu'avocat, on nous dis : « s'il vous plaît faites le plus long possible et puis mettez les choses les plus importantes à la fin puisque personne ne les lit ».
J'ai vu une proposition de loi en

Californie qui était extraordinaire. Elle disait : « les conditions générales de service ou de vente au public doivent faire cent mots au maximum. » Voilà c'est très simple, c'est très concret parce que ça, ça peut être lu, ça oblige. Vous savez, en France, avec le code civil, vous avez un principe de responsabilité. Il fait une ligne et demi et existe depuis un siècle et demi, près de deux siècles maintenant. On peut faire de la rédaction concise quand on veut. Encore une fois, je pense c'est le mot simplicité qui est important et comme l'a dit Muriel BARNEOUD, tout à l'heure, les acteurs de confiance s'engagent clairement sur leurs obligations, mais ça c'est vis-à-vis des entreprises.

Muriel BARNEOUD : Mais, Olivier, ne pensez-vous pas que l'arbitre c'est aussi l'utilisateur final ?

Olivier ITEANU : Bien sûr.

Muriel BARNEOUD : Parce qu'on arbitre tous les jours, je pense. On sait tous aujourd'hui qu'aller faire nos recherches sur Google est une façon évidente. On a été dessillé sur ce genre de chose et même nos jeunes le savent très bien, d'ailleurs ils le savent peut être même plus que nous et ils sont bien plus conscients que nous le sommes. Nous utilisons tous les jours des outils qui sont des outils dangereux ou en tout cas dont on sait que le détournement est dangereux, même s'il y a une mention sur la sécurité dans un codicille du paragraphe 25 des conditions générales de vente ou d'achat déposées dans le Delaware ou je ne sais où. Néanmoins nous savons tous quels risques nous prenons.

Je pense aussi que, dans cette histoire d'arbitrage, l'utilisateur final, le client, quelle que soit sa nature, est partie prenante. Je vous rejoins à 200 % sur la manière dont il va être éclairé dans ses choix parce qu'il arbitre tous les jours, il décide tous les jours de le faire. Pourquoi est-ce qu'il le fait ? Parce que la puissance d'usage et la simplicité d'usage de ce qui nous est offert sont un des éléments aussi de la confiance. La simplicité, la facilité à faire doivent être quelque chose de très important dans l'écosystème. Si vous fabriquez quelque chose qui est juste impossible à adapter, du type de la signature électronique façon 2001, ça ne marchera jamais et l'arbitrage au quotidien se fera toujours dans l'autre sens.

Olivier ITEANU : Vous avez raison. Je ne sais pas si vous avez déjà essayé de déposer une plainte ou un grief auprès d'Amazon ou d'eBay à l'occasion d'un litige ou d'un site de e-commerce. Si vous n'avez pas la menace juridique à portée de main, c'est difficile, d'autant plus que bien souvent les conditions générales désignent des lois et des tribunaux exotiques, enfin pas exotiques d'ailleurs car très souvent ils ne sont pas loin de nous.

Donc vous avez raison, l'utilisateur a aujourd'hui un pouvoir et il ne faut pas l'oublier. L'autorégulation, c'est effectivement une chose que l'on n'a peut-être pas intégrée au niveau législation. Mais on a encore besoin quand même au moins de la voie juridique.

Michel PICOT : On en parlera, de ces autorégulations. Guillaume BUFFET et ensuite Claude REVEL voudraient réagir aussi.

Guillaume BUFFET : J'ai l'impression que cette question de l'arbitre, c'est finalement le cœur de notre problématique. Je suis d'accord avec vous, normalement c'est le juge, c'est ce que l'on a tous appris à l'école quand on était petit. Au vrai, aujourd'hui, ce n'est pas le cas.

Pour les questions liées à la relation entre l'État et le citoyen, il n'y a plus de juge. Pour les questions liées à la relation entre un utilisateur et une entreprise on trouve des conditions générales d'utilisation que l'utilisateur n'est pas capable d'évaluer. Ensuite, on n'a pas le choix, c'est-à-dire

qu'aujourd'hui, ce n'est pas possible de proposer à l'ensemble des citoyens de ne plus utiliser les services en ligne parce qu'ils ne sont pas d'accord avec les conditions générales d'utilisation.
Donc le risque, selon moi, c'est que, petit à petit, la défiance existante atteigne un tel niveau que l'on jette le bébé avec l'eau de l'Internet, qu'au lieu d'être sur des critères d'ordre légal on en arrive à des critères d'ordre moral comme on essaye de nous les faire passer aujourd'hui. « C'est bien », « c'est pas bien de faire ça », « tu ne devrais pas », « si tu n'as rien à te reprocher il n'y a pas de problème à ce qu'on te regarde »... On est en train petit à petit de changer de société parce que ce n'est plus le juge qui est là pour évaluer, c'est la morale, ce sont des services secrets ou des conditions générales d'utilisation.

Michel PICOT : Guillaume BUFFET, voici un tweet qui peut vous concerner. Faut-il réguler le web pour gagner la confiance ou faut-il finalement compter sur la transparence et la communauté ?

Guillaume BUFFET : Bonne chance à celui qui réussira à réguler le web ! L'organiser ? Faire en sorte que les gens aient un comportement citoyen me semble absolument essentiel. Le réguler ? Internet s'est construit tout seul et du jour où les États ont voulu le réguler, ils ont démontré qu'ils étaient capables de créer des problèmes.
Pourtant, je suis extrêmement attaché à l'État. Je suis amoureux de notre pays, je suis amoureux de notre histoire autour de l'État de droit. J'adorerais qu'on recrée un monde dans lequel la société, la puissance publique soit là pour aider et pour accompagner. Aujourd'hui ce n'est pas le cas

Michel PICOT : Claude REVEL vous voulez réagir depuis tout à l'heure. Vous me dites il faut que je rebondisse sur certains points. Je vous donne la parole.

Claude REVEL : Le juge, jusqu'à preuve du contraire, applique la loi. Donc il lui faut une loi, après il fait une jurisprudence, il peut faire le maximum pour la faire évoluer. Mais enfin, à la base, l'instrument du juge, c'est la loi. Donc il lui faut une bonne loi. Et donc il faut un cadre clair.
Je reviens à mon idée, à ce que je disais tout à l'heure : un cadre juridique clair et simple en effet. Tout le monde est d'accord et personne ne peut dire le contraire, il y a actuellement une trop grande complexité Une fois qu'on la dit, il faut essayer d'avancer.

Michel PICOT : Une petite parenthèse sur un tweet, en parlant du juge justement. Le juge d'accord mais comment vous assurez-vous de l'indépendance de la République numérique des juges ? Je trouve la réflexion intéressante.

Claude REVEL : Oui mais, enfin, les juges utilisent quand même les instruments qu'on leur donne. En plus, effectivement, on est encore en pays de droit continental où on a des lois qui sont en principe faites de manière assez simple. Il ne faut pas venir les complexifier avec des tas de choses derrière.
Sur le terrain, il y a également les règles, les clauses plus ou moins claires d'application, etc. Là aussi, ça veut dire que derrière, il y a eu un cadre qui a permis cette complexité. On retombe toujours sur la même question, il faut des règles du jeu.
Il faut des règles du jeu, alors la question c'est de savoir qui établit les règles du jeu. On peut les laisser s'établir de manière auto régulée par les entreprises mais il y a quand même peut-être des limites à ça. Par les citoyens, je pense aussi et on peut en parler, il y a peut-être également des limites. Et puis par une coopération internationale digne de ce nom et notamment au sein de l'Union Européenne où, quand même, jusqu'à preuve du contraire, il y a des pays démo-

cratiques. On peut toujours critiquer dans tous les sens, je suis d'accord avec la plupart des critiques. Mais enfin, quand même, les règles du jeu doivent être posées. Donc, a priori, il vaut mieux qu'elles soient déposées par des gens qui défendent l'intérêt général.
Alors, vous allez me demander ce qu'est l'intérêt général. C'est là que nous avons des différences d'appréciation, entre nous, en Europe, et d'autres pays comme les États Unis, il faut le dire clairement, ou d'autres États du monde.
La question est de savoir jusqu'où va l'intérêt général et où il s'arrête. Et ensuite, pour les citoyens et les entreprises, jusqu'où va l'information stratégique qui doit être protégée parce qu'elle est la base de l'innovation et du développement et où s'arrête-t-elle parce que c'est du business pour tout le monde ? C'est là le rôle du législateur aidé par les parties prenantes.

Je vois les choses comme ça. Je ne vois pas non plus d'énormes défiances. Il y a peut-être une défiance mais c'est à nous de faire en sorte de la surpasser, de la dépasser.

Michel PICOT : Si je vous suis bien, la question centrale consiste à trouver le juste dosage de régulation, je ne sais pas si c'est le bon terme, mais sans empiéter sur la liberté ?

Claude REVEL : La régulation c'est une chose, mais il ne faut pas tout ramener à la régulation non plus. Il y a aussi une responsabilisation individuelle. On a parlé tout à l'heure de compétence. Effectivement, plus les gens deviendront compétents en informatique, un minimum en tout cas, plus ils auront confiance. Ils n'ont pas confiance parce-qu'ils ne comprennent pas, parce que, souvent, ils ne savent pas. Et pour les entreprises c'est pareil...

Guillaume BUFFET : Pardon, c'est l'utilisateur ou le législateur qui ne comprend pas ?

Claude REVEL : Mes deux voisines disaient, elles ont raison, que quelquefois, quand on ne comprend pas techniquement les choses, on n'a pas confiance. Donc je dis qu'il y a deux choses. Il y a d'une part des règles du jeu à mettre en place pour que, justement, ce soit plus clair pour le consommateur, l'utilisateur. Et il y a d'autre part une éducation à faire aussi. Dans le système scolaire, les enfants devraient avoir un minimum d'accès à l'éducation numérique. Même constat pour les entreprises. Là on revient à la cybersécurité. Les entreprise doivent peut-être également se responsabiliser de ce point de vue-là, je crois que c'est l'avis de tout le monde ici. Savoir que l'État ne peut pas tout faire et ne doit pas tout faire leur fera prendre d'elles-mêmes des dispositions techniques et de comportement humain, de sensibilisation pour faire face à ces questions.

Guillaume BUFFET : C'est ma dernière intervention sur ce sujet. Vous dites « on ne comprend pas techniquement ».
Les parlementaires ont eu l'excellente idée de constituer une commission pour comprendre les sujets du numérique. Je ne sais pas si vous avez suivi les discussions mais, à l'unanimité de cette commission, ils se sont opposés au texte de loi contre le terrorisme. Et l'ensemble des parlementaires a voté à l'encontre de la recommandation de la commission des experts parlementaires sur ce sujet. Je suis assez d'accord avec vous, je pense qu'il est important de comprendre techniquement de quoi on parle avant de voter des lois.

Michel PICOT : Je voudrais que l'on parle quand même aussi de la confiance dans le business que l'on peut faire à travers les outils numérique. Olivier ITEANU, le droit ne doit-il pas être un peu plus strict, un peu plus encadré pour tout ce qui concerne les transactions numériques et tout ce qui relève du

business autour ou avec le numérique ? Les enjeux sont peut-être plus importants finalement, je vous pose la question.

Olivier ITEANU : Plus strict ? Non, moi je n'ai pas le sentiment aujourd'hui que, de ce point de vue là, on a besoin de de règles plus strictes. Je dirais qu'on a besoin d'avoir des acteurs de confiance, c'est à dire de gens qui s'engagent clairement sur des objectifs.
Je suis désolé, je suis là en tant que vice président de Cloud Confidence. C'est la raison d'être de cette association. Parce que le débat est brouillé, il y a beaucoup d'acteurs sur le marché qui disent qu'ils font des choses et quand on lit attentivement leurs contrats, on a des surprises. C'est pourquoi nous soutenons cette certification dans laquelle il y a un collège professionnel avec une vingtaine de membres, un collège utilisateur (et nous comptons notamment sur l'appui du Cigref, le club informatique dans l'entreprise française) et puis un collège d'écosystème. On est en train de créer l'association en Allemagne.
On a trois règles dans ce référentiel. D'abord, l'information de l'entreprise. Quand je dis information, cela inclut les données à caractère personnel. On en fait, avec raison, tout un fromage, mais il n'y a pas que les données à caractère personnel qui sont intéressantes. Pour Airbus, un plan d'avion ce n'est pas des données à caractère personnel mais c'est important aussi, un business plan également, etc. Donc, les professionnels qui adhèrent à la certification par un tiers s'engagent à donner aux informations de l'entreprise une protection égale à celle des données à caractère personnel. Et ça, c'est fort.
Deuxièmement, ils s'engagent par leur offre à ne pas être soumis à une réglementation extra-européenne qui donne la possibilité à une administration ou à un service de renseignements d'accéder à vos données. Vous voyez ce que je veux dire. Ce sont des engagements fermes qui sont écrits, qui sont dans le référentiel.
Déjà sur ces deux règles-là il y a aussi des questions d'inter-opérabilité entre les services et ça aujourd'hui c'est un sujet de réversibilité, de portabilité des données. Sur ces sujets là, il faut clarifier un peu le marché. Ensuite, eh bien Dieu reconnaîtra les siens puisqu'on est dans la confiance et que l'on a dit que c'était la foi. C'est aux utilisateurs, aux grandes collectivités territoriales, aux entreprises, en fonction de la criticité des données qu'ils ont à confier puisqu'on externalise beaucoup aujourd'hui, de faire le choix de gens qui prennent des engagements précis.

Michel PICOT : Il y a beaucoup de tweets qui circulent, je n'ai pas eu le temps de tous les prendre, mais je trouve qu'il y a beaucoup de méfiance dans ce qui est affiché à l'écran en permanence.

Olivier ITEANU : Nous sommes des mutants, on vit une révolution. Ceux qui viennent derrière nous, les adolescents, sont nés là-dedans, ils ont moins de défiance, ainsi que le disait Guillaume BUFFET, vis à vis de tous ces outils qui sont quand même pour nous, globalement, en fonction de nos âges, relativement ou très nouveaux. Nous sommes des mutants, il faut accepter que le temps fasse son effet aussi.

Muriel BARNEOUD : Nous sommes des mutants ou nous venons de l'ancien monde. C'est vrai, demain ce n'est pas nous en plus vieux, ça aura une autre tête. Nous, nous sommes porteurs d'une transition « Do like it ». On est porteur d'une transition et là-dedans je vous rejoins, la douleur est pour nous parce qu'on a à planter les deux ou trois éléments majeurs qui permettront de faire basculer les choses dans le bon sens.
Et c'est aussi un sujet de confiance. Il y a une question tout à l'heure qui était intéressante, je trouve, entre sécurité et confiance. Pour moi, la nuance

n'est pas anodine. S'agissant de sécurité, on va parler de choses dont on n'aura jamais l'absolue certitude qu'elles ne seront pas bypassées, qu'elle ne seront pas hackées, qu'elles ne seront pas soumises à une réglementation qui évoluera. La confiance, et je ne reviens pas sur la foi car ce n'est pas l'objet, mais c'est quelque chose de plus que ça. C'est la conviction qu'il n'y a pas une malveillance permanente, que, en tout cas, il y a dans un écosystème un partage suffisant de valeurs, de règles, d'éthique, d'envie et de proximité grâce auxquelles on sait affronter et on sait résoudre ce type de problèmes. Des problèmes de sécurité, nous en aurons tout le temps. La façon dont on va les aborder, c'est cela qui, selon moi, constitue la confiance que l'on a dans demain, la confiance que l'on a dans l'inconnu et l'incertain dans lesquels on est en train de rentrer ou dans lesquels on a déjà posé les deux pieds.

Michel PICOT : La technologie va trop vite pour le législateur, la loi doit s'adapter sinon le citoyen sera le grand perdant. Preuve que dans la salle il y a peut-être des gens qui ont besoin d'avoir quelques repères pour être rassurés.
Pamela WARREN, vous vouliez réagir sur ce qui a été dit tout à l'heure par Muriel BARNEOUD ?

Pamela WARREN : Une chose à laquelle je pensais avec cette question sur la confiance entre les entreprises, entre les entreprises et les utilisateurs, entre les gouvernements et les citoyens, c'est que la sécurité fait partie de la fondation de la confiance. Ça revient à ce dont on a parlé tout à l'heure avec la loi européenne sur la protection des données et l'utilisation de ces informations, la qualité de service que vous faites.
Aux États-Unis, il y a un manque de confiance par rapport au citoyen et au gouvernement. Vous dites que sur nos billets il y a marqué « In God We Trust » mais on ne fait plus confiance à une grande partie du gouvernement. Comment avoir un retour sur ce qui est suivi, surveillé par rapport à nos interactions en ligne et nos capacité d'aller en ligne ? Comment ne pas avoir des ramifications de cette surveillance dans le cadre de nos activités professionnelles ou quand on communique de manière privée ? Il y a beaucoup d'éléments qui font partie de cette confiance et je ne sais pas si on peut tout réglementer. Je crois que c'est vraiment une question de voter avec notre porte-monnaie ou avec notre voix : quand vous traitez avec les citoyens, avec les entreprises, vous pouvez choisir de ne pas faire du business avec tel ou tel d'entre eux.
Un des éléments de cette nouvelle évolution des technologies qui me perturbe particulièrement est dans le domaine des mobiles. C'est le tout ou rien d'acceptation d'une application mobile quand on la télécharge, c'est un très bon exemple par rapport aux problèmes de compréhension. Quand je télécharge une application, je pense au bénéfice qu'elle va m'apporter mais est-ce que je pense aux ramifications sécuritaires de cette application ? Elle ne devrait pas avoir accès à mes contacts si il n'y a pas de contexte pour les utiliser. Peut-être que je veux choisir d'autoriser ma localisation. Certaines municipalités dans le monde mettent en œuvre des applications utilitaires intelligentes avec lesquelles je peux appeler ou informer d'une fuite d'eau dans ma ville. Dans ce cas je devrais autoriser ma localisation, dans d'autres cas non. A l'heure actuelle, les développeurs d'application mobile demandent toutes ces autorisations et c'est tout ou rien. C'est un domaine qui m'intéresse particulièrement pour voir comment va évoluer la confiance.

Muriel BARNEOUD : Il y aura un business pour ça. On le voit déjà à l'échelle postale. C'est à dire une gestion éthique de la donnée dès lors que vous rencontrez une attente du marché et elle est très forte, y compris

sur le marché nord-américain. On imagine toujours que c'est un Far-West mais les préoccupation relatives à la vie privée sont aussi fortes et aussi importantes que chez nous. Dès lors qu'il y aura un marché pour ça, comme on aura eu une vague un peu Far-West sur les données, je suis intimement persuadée qu'il va y avoir et qu'il y a même déjà un marché pour une gestion éthique des données. Et c'est quelque chose que nous vivons d'ores et déjà du côté de la poste. Il y a une demande et une appétence pour les offres que nous proposons.

Guillaume BUFFET : Lors d'un forum des villes européennes, il y a quelques jours à Paris, quelqu'un originaire de je ne sais plus de quel pays nordique a fait une comparaison relativement osée mais néanmoins passionnante. Cette personne a invité à considérer la Suisse. La Suisse a réussi à créer la confiance bancaire en ne pensant qu'à l'utilisateur. Et si nous, l'Europe, on était capable de créer la confiance dans la vie privée et dans les données numériques en pensant à l'utilisateur ? La comparaison est osée mais c'est un moyen de développer certainement une économie géniale.
Pour revenir à votre question de départ, quelles sont les clés de la confiance pour développer l'économie numérique ?

Michel PICOT : Je voulais ajouter un tweet : est-ce que sécurité et confiance vont finalement aussi de pair ?

Guillaume BUFFET : Ça rappelle ce que disait notre maman, la confiance ça se mérite ! Non, je parlais de séparation des pouvoirs, dans le domaine économique aussi j'appelle de mes vœux une espèce de séparation des pouvoirs. On en a beaucoup parlé autour des sujets de neutralité. C'est-à-dire que je ne crois pas qu'une entreprise ait à la fois le droit de donner accès à Internet et le droit de choisir à quel morceau de l'Internet elle donne accès.
Aujourd'hui, la question de la loi, c'est de savoir s'il faut qu'il y en ait une ou pas, je ne suis pas assez compétent sur ce sujet. Mais il y a un trou dans la raquette, comme on dit, sur ces histoires de neutralité. Je crois qu'en revanche, légalement c'est très bien défini, l'entreprise n'a pas le droit d'utiliser sa position dominante pour imposer des choix aux utilisateurs. Et aujourd'hui il y a une vraie question autour de ces positions dominantes, donc les entreprises ont des grosses responsabilités.
Je ne voulais pas dire tout à l'heure que l'État est responsable de tous les maux de la planète. Les utilisateurs seraient des Bisounours et les entreprises seraient là pour arbitrer ? Je ne crois pas. Je crois que l'on a chacun nos responsabilités. L'entreprise est responsable, elle a une responsabilité sociale en fait. Et cette fameuse RSE dont on nous bassine les oreilles, je suis moi persuadé qu'elle va prendre naissance avec cette génération numérique, car les entreprises ne pourront pas faire autrement sinon le retour de bâton va être absolument terrible.
Enfin, pour finir, les entreprises doivent avoir une vraie exemplarité. Les entreprises qui font rêver aujourd'hui sont les entreprises du numérique pour la plupart. J'ai appris par un chercheur de Renaissance numérique que Paypal est en train de réfléchir à installer son siège social sur une plate-forme dans les eaux internationales. Comme ça, elle n'aurait plus de responsabilité vis à vis de qui ce soit. Bonjour l'exemplarité ! Je crois que chacun de nous, moi aussi qui suis entrepreneur du numérique, on a un devoir d'exemplarité. Un devoir certainement pas moral mais je dirais éthique.

Michel PICOT : On va faire un rapide tour de table qui sera une forme de conclusion. Claude REVEL ?

Claude REVEL : Oui effectivement un des tweets précédents disait que la loi doit s'adapter

aux technologies. Je pense que la loi doit poser des principes car elle va courir après cette technologie et elle sera toujours en retard. Donc, elle doit poser des principes de conduite, de comportement qui seront ensuite évidemment développés par les parties prenantes. Ensuite, sécurité et confiance vont de pair je pense et c'est là que le curseur doit être bien adapté.

Quand on dit « demain sera merveilleux car on pourra utiliser tout ça de manière spontanée », il ne faut pas oublier que tout ce qui passe à travers Internet est quand même de l'information. La traçabilité, tout ce que vous voulez c'est de l'information. Cette information peut être captée par les uns ou par les autres et pas seulement par les États, figurez-vous, ça peut être aussi justement des grandes entreprises ou des grandes puissances qui ne sont même pas des États et qui ne sont pas soumis à l'intérêt général. Il faut quand même s'en souvenir un tout petit peu, je sais bien que je ne vais pas accroître la confiance en disant cela. Justement, il faut un cadre clair car des choses comme celles décrites par ORWELL dans son « 1984 » ne sont totalement exclues. Il faut vraiment des bases qui soient posées par des arbitres qui soient le plus proches possible de l'intérêt général. Je suis désolée, on en revient toujours là. Alors qu'ensuite il y ait des acteurs, ça c'est une chose. Que les acteurs soient responsables, c'est une obligation.

Par ailleurs, l'éducation est totalement fondamentale comme dans toutes les questions que l'on voit depuis quelques temps. A partir du moment où on aura une éducation un peu plus numérique, on aura peut-être un peu moins ce genre de problème car on aura plus confiance, on saura se comporter de telle ou telle manière.

Je voulais dire aussi deux choses. Vous parliez tout à l'heure d'information des entreprises stratégiques. Il y a une loi qui est actuellement en cours de discussion et également un projet de directive au niveau européen sur le secret des affaires. Le mot secret fait hurler, il ne s'agit pas de garder tout secret, il s'agit au contraire de pouvoir communiquer un maximum de choses, d'être transparent tout en protégeant l'information stratégique de base, tout petit noyau, qui permet l'innovation, l'emploi et la croissance derrière.

La dernière chose, c'est, quand même, un mot sur ce que fait la délégation interministérielle. On a bien conscience qu'il y a une question de formation. On a reçu du Premier ministre le mandat de faire des cahiers des charges, des référentiels de formation très simples, pas chronophages pour les PME qui sont quand même les premières concernées. On l'a fait évidemment conjointement avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI) au niveau technique et je crois que là on participe aussi à établir cette confiance. Quand les entreprises seront mieux formées et donc leurs employés évidemment, les individus, chacun a plusieurs casquette, et bien à ce moment là, ça participera à cette confiance générale.

Michel PICOT : Merci beaucoup. On se dirige vers la fin. Olivier ITEANU ?

Olivier ITEANU : Je dirais que rien n'est inéluctable, tout est entre nos mains, la solution est sur terre et pas dans le ciel. Je crois que les entreprises, si elles respectent les valeurs, si elles respectent les citoyens, peuvent faire de ce respect là un avantage business, un avantage concurrentiel et c'est valable pour des entreprises très locales. Pas besoin d'être globale et les entreprises globales devront être locales.

Deuxièmement, les utilisateurs, les consommateurs doivent donner la prime à ceux qui respectent et pour ça il faut que les entreprises leur fassent savoir de manière simple et claire. C'est la certification Cloud Confidence, je suis désolé, je suis là pour vendre Cloud Confidence. Ils doivent donner la prime, que ce soit

des utilisateurs professionnels, des collectivités territoriales, des petites entreprises, à ceux qui respectent leurs valeurs.
Enfin l'État. On attend de l'État, je crois, un cadre, c'est vrai vous avez raison Madame, un cadre et pas autre chose, il ne faut pas rentrer dans les détails. Il faut un cadre clair et simple et une grande vigilance vis-à-vis de l'Europe pour que les intérêts européens soient clairement défendus auprès de la Commission européenne. Il faut le dire clairement.

Michel PICOT : Muriel BARNEOUD ?

Muriel BARNEOUD : Je commencerais à répondre à la question de savoir s'il n'est pas trop tard et si tout n'est pas déjà entre les mains de Google. Je ne pense pas, non, qu'il soit trop tard, exactement comme vous le disiez, Olivier. Souvenez- vous, il y a dix ans, on parlait des GYM, Google,Yahoo, Microsoft. On parle aujourd'hui des GAFA. Sur les trois il y en a un qui a disparu et il y a un qui a failli disparaître et qui est en train de se réformer à grande vitesse alors qu'on le pensait inatteignable. Les choses vont extrêmement vite, je pense que la puissance des utilisateurs dans la façon dont ils décident à un moment ou à un autre de trouver d'autres solutions et des solutions qui leur conviennent est extrêmement importante. Je serai très prudente sur le fait que le match est joué, je ne le crois vraiment pas.
Je fais souvent le parallèle avec ce que l'on a pu vivre dans l'industrie lourde. On est dans un écosystème où, si on se développe d'une manière effrénée, on pollue, on abîme, on détruit. Je crois que l'on a la même chose ou un parallèle un peu à faire dans l'univers de l'industrie numérique. Si on n'y prend garde et si on ne se comporte pas avec l'éthique voulue, avec le respect des règles et des normes qui nous conviennent bien, on a les mêmes phénomènes de pollution, les mêmes phénomènes d'usurpation, on aura ces mêmes sujets.
Sans faire de parallèle audacieux mais néanmoins en y pensant en matière de RSE, c'est ça qui est devant nous aujourd'hui. Je pense que l'industrie numérique a devant elle aujourd'hui le choix de la manière dont elle se développera, sans créer ces pollutions qui ont put donner lieu à autant d'horreurs dans l'univers manufacturier, et ça c'est une responsabilité d'industriels, d'écosystème dans cet univers numérique. C'est de notre intérêt car sans confiance, encore une fois, il n'y a pas de développement.

Michel PICOT : Merci. Guillaume BUFFET, rapidement, puis nous terminerons avec Palema WARREN.

Guillaume BUFFET : Je reviendrais sur mes trois lettres de départ, sur « ensemble ». On ne peut pas construire cette confiance si on ne le fait pas ensemble parce que le numérique n'est pas pyramidal et on a un esprit qui est trop pyramidal. Non, des parlementaires qui refusent de parler avec le citoyen ne peuvent pas inventer tout seuls la loi du numérique du demain. Non, des entreprises qui ne sont pas capables d'écouter leurs utilisateurs ne peuvent pas construire la confiance de demain. C'est ce lien qui est vital. Ce qui est incroyable, c'est qu'on est là pour le porter, on le propose, on a envie de le faire ensemble. Je vais terminer avec un mot, la laïcité numérique, public/privé ensemble. Il n'y a pas de frontière entre les différents points de vue du numérique, chacun a le droit de croire en ce qu'il veut mais faisons-le ensemble, s'il vous plaît.

Michel PICOT : Pamela WARREN, ce sera le mot de la fin.

Pamela Waren : Merci. Il y a différents problèmes dont on a parlé et je voudrais rappeler une intervention, lors d'une conférence sur la sécurité. « Ma mère, elle s'en fiche de la sécurité sur

son ordinateur. Elle peut avoir sur son ordinateur un virus qui peut avoir un impact sur les autres, elle s'en fiche. »
Je crois que l'on doit se préparer à ce que les utilisateurs du réseau puissent impacter la sécurité d'autres. On doit prévoir que la technologie pallie à cela, automatise beaucoup de protections, pour instaurer la confiance. On peut revenir à des cadres réglementaires et des règles directrices et des contrôles. Il y a des industries qui font ces contrôles. Google le fait avec Microsoft, si il y a une vulnérabilité dans le logiciel qui n'a pas été résolue dans les 90 jours. Ça peut nous aider à restaurer la confiance.

Michel PICOT : Vous pouvez les applaudir. Merci pour la qualité des propos. J'espère que l'on aura fait avancer les différentes réflexions.

P4

Souveraineté numérique : vrai ou faux débat ?

Intervenants :
- Animateur : Michel PICOT – Journaliste BFM Business,
- Bernard OURGHANLIAN – Directeur Technique et Sécurité Microsoft,
- Didier TRUTT – Président directeur-général de l'Imprimerie Nationale,
- Gwendal ROUILLARD – Député du Morbihan, Secrétaire de la commission de la défense nationale et des forces armées.
- Duncan CAMPBELL, Investigative Journalist and Forensic Expert
- Laure de la RAUDIÈRE – Députée d'Eure-et-Loir, Secrétaire de la commission des affaires économiques.

Michel PICOT : Bonsoir, nous voici à la dernière plénière de ce FIC 2015. Je ne vous apprends rien en vous disant que le cyberespace se joue des frontières et accélère la dilution de la souveraineté étatique. Depuis l'affaire SNOWDEN et les attentats de Paris, la notion de la souveraineté numérique est au cœur des débats. Le cyberespace est-il capable de s'auto-réguler ou au contraire faut-il le réguler ? Comment arriver finalement à conjuguer liberté, souveraineté et confiance ? Ce sont des termes que nous avons abordés ce matin. Les technologies ne sont elles pas plus fortes que la réglementation ? Les États n'abusent-ils pas ? Des questions que nous poserons notamment à Duncan CAMPBELL. Ce journaliste d'investigation a révélé au grand jour Echelon[1]. Il nous en parlera ultérieurement tout en dressant la situation actuelle.
Je vais débuter cette plénière en posant la question à Laure De La RAUDIÈRE, députée de la 3eme circonscription d'Eure-et-Loir. Vous êtes spécialiste de toutes ces questions de cybersécurité. Pour planter le décor, je vous le demande : sécurité numérique, vrai ou faux débat ?

Laure DE LA RAUDIÈRE : Vrai débat, essentiel. Tous les enjeux du numérique, qu'ils soient sur les plans économiques, éthiques, ou bien pour la défense de nos valeurs, de notre sécurité, se posent d'emblée au niveau mondial. Comment

1 Echelon est un nom de code utilisé pendant de nombreuses années par les services de renseignements des États-Unis pour désigner une base d'interception des satellites de télécommunication commerciaux. Par extension, le réseau Echelon désigne le système mondial d'interception des communications privées et publiques (SIGINT), élaboré par les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande dans le cadre du traité UKSA.

un pays peut-il défendre ses idées, ses valeurs, ses libertés et bien évidemment son économie, dans un cyberespace mondial ?

Michel PICOT : Il s'agira de déterminer quelle dose de souveraineté est nécessaire et comment y arriver. Gwendal ROUILLARD bonsoir, vous êtes député de la 5ème circonscription du Morbihan, secrétaire de la commission de la Défense nationale et des forces armées à l'Assemblée nationale. Je vous pose la même question : sécurité numérique, vrai ou faux débat ?

Gwendal ROUILLARD : À votre question je réponds « vrai débat ». La France est vulnérable. Nos concitoyens, nos entreprises, l'État mais aussi les acteurs publics sont vulnérables. En rencontrant nos concitoyens au fil des années, je constate que ce constat est partagé. La France s'est mobilisée au travers de sa Loi de Programmation Militaire (LPM). Cela a fait l'actualité d'aujourd'hui au Conseil de Défense pour définir une stratégie, préciser les outils, les moyens humains et matériels, pour répondre aux défis qui sont devant nous. Nous pouvons partager ce message : la sécurité c'est la condition de la liberté. Encore aujourd'hui, j'entends dire que la sécurité est une contrainte qui s'impose à la liberté d'entreprise. Ce qu'il faut bien comprendre, a fortiori après les attentats de Paris, c'est bien que la sécurité est la condition de la liberté, de notre liberté.

Michel PICOT : Vous avez bien fait de le dire, car il ressort dans les tweets reçus des différentes plénières qu'il existe une volonté d'un cadre sécurisé mais avec cette crainte d'une chape de plomb et d'un frein à la liberté.

Gwendal ROUILLARD : Je comprends cette interrogation. Ce sera d'ailleurs au cœur des débats et des discussions du mois de juin 2015 suite à l'annonce par le Président de la République de la révision de la LPM. Chacun doit bien comprendre que l'année 2015 sera une étape pour améliorer nos dispositifs de sécurité . L'essence même du débat sera de savoir où nous mettons le curseur.

Bernard OURGHANLIAN : La question de la souveraineté est un vrai débat, à la fois pour chacun des États qui vit aujourd'hui dans un monde à la fois physique avec des frontières et numérique sans frontière. Les questions de défense du patrimoine des entreprises, de nos valeurs, sont des questions centrales. Il n'est pas à l'ordre du jour d'abandonner ces prérogatives pour un quelconque État. Pour autant, de nombreuses questions se posent. Il est nécessaire d'impliquer l'ensemble de nos concitoyens dans ce débat, de faire en sorte qu'ils soient armés pour répondre à ces questions, et ainsi de savoir pour pouvoir. En matière de sécurité, il existe une tendance à dire que nous avons la possibilité de sécuriser une entreprise, la plus grande soit-elle, sans que les citoyens aient un rôle à jouer. Ce raisonnement est faux. À partir du moment où les machines sont toutes interconnectées, le moindre poste de travail peut par sa faiblesse faire peser potentiellement une menace extrêmement importante. Il suffit de mobiliser des millions de postes de travail, c'est suffisant pour déclencher une simple attaque de déni de service et provoquer l'arrêt du plus grand État. Nombre d'histoires montrent que c'est une réalité.

Michel PICOT : Il en est ainsi pour ceux qui se connectent avec leurs outils sur le réseau de l'entreprise. Ces derniers peuvent provoquer une faille potentielle très importante.

Didier TRUTT : C'est un vrai débat, d'autant que le cyberespace est loin d'être arrivé à maturité. Nous parlons beaucoup d'Internet comme d'un enjeu sociétal et politique mais aussi économique et industriel très important. Nous sommes concernés au niveau national et

européen, cet enjeu, il faut en discuter. Quelle législation faut-il mettre autour de ça ? Les entreprises qui régissent ce domaine légifèrent aujourd'hui sans en dire le nom. Au niveau sécurité, notre société milite pour le travail autour des données personnelles, car c'est là que se trouve le débat.

Michel PICOT : Cette dose de souveraineté, c'est ce cadre sécurisant mais efficace. Mais des abus ont été découverts grâce notamment à Duncan CAMPBELL qui a mis à jour le réseau Echelon

Duncan CAMPBELL : Les organisateurs m'ont demandé de montrer l'importance, dans la souveraineté digitale, du numérique, des débats qu'on a en Europe, même si avec le système de surveillance Echelon, les révélations se sont étendues par la suite à la surveillance d'un État dans des documents fournis par Édouard SNOWDEN.
En 1999/ 2000, les Parlements européens et nationaux ont parlé de la surveillance par satellite du réseau Echelon. Beaucoup de résolutions et d'initiatives ont voulu améliorer la vie privée dans le domaine des communications. Tout s'est arrêté après les attaques de 2001 sur New-York. Le projet Echelon avait pour objet d'intercepter les communications des satellites occidentaux civils, pas militaires. Le projet Echelon a été souvent exagéré sur Internet ou mal compris car c'était quelque chose de spécifique et de puissant. C'était le seul système de surveillance automatisé de masse avant les années 1990, où les agences de renseignement ont mis des dispositifs de piratages sur les autoroutes de l'information et ont capturé les trafics de voies et de données.
Le système actuel de surveillance défini par SNOWDEN s'appelle COMSAT (communications satellite), doté de 40 stations réparties dans 35 pays qui participent à ce système de surveillance, y compris les agences anglophones qui prennent l'appellation de pays-tiers. Beaucoup de pays européens sont membres de ce réseau de surveillance.
Un nouveau document SNOWDEN a été révélé il y a deux jours et publié par le journal Der Spiegel (Allemagne). Ce document montre à l'évidence que le site COMSAT, y compris la station de Menwith Hill (Grande-Bretagne), a pris part à une attaque secrète menée sur Internet et utilisant des réseaux malwares gérés par la National Security Agency (NSA) et le Government Communications Headquaters (GCHQ)[2]. Ceci est appelé des « turbulences », mais il y a beaucoup d'autres informations dans le document. Cette station fait partie d'un système de cyberattaque très vaste, qui est maintenant physiquement intégré, connecté aux câbles d'Internet et à des douzaines voire des centaines de routeurs hackés dans tout le système. Les systèmes d'attaque ont la capacité d'interférer pour modifier le trafic de données en passant au travers des fibres optiques du Royaume-Uni et des États-Unis d'Amérique tout en réalisant une analyse massive et passive. Les documents SNOWDEN montrent que les routeurs modifiés sont utilisés pour façonner le trafic Internet en créant des routes d'exfiltration vers les agences. Ils ont la possibilités de modifier les données en injectant des malwares ou en modifiant les vecteurs de différentes natures. Dans les nouvelles révélations, nous apprenons que les malwares prennent l'appellation de computer network exploitation (CNE). Les délits de destructions délibérées sont désignés sous le vocable de computer network attack (CNA). Cette cyberguerre a déjà commencé et se déroule depuis plusieurs années. Il n'y a pas assez de

2 Le service de renseignements électronique du gouvernement britannique.

temps pendant cette plénière pour décrire comment chaque nœud, chaque borne d'Internet a été infectée, piratée jusqu'aux niveaux des algorithmes sécurisés. Si vous voulez approfondir le sujet, je vous renvoie sur les articles du Spiegel et des sites spécialisés où vous allez trouver des centaines de nouveaux documents. Ces derniers décrivent les méthodes, les outils et la détermination des attaques. Ainsi, des technologies nommées sessionizers prennent toutes les données et les ré-assemblent. Autre exemple, les transactions Internet indexent les contenus à l'échelle des métadonnées. Nous sommes face à une version à grande échelle de la DPI (deep packet inspection)[3]. Il s'agit d'une échelle que l'on ne peut pas comprendre sans connaître le système Tempora[4] qui est un réseau distribué d'accès Britannique. Il existe un système plus global nommé Xkeystore[5]. Selon un document issu d'un logiciel du GCSQ, le nombre de transactions indexées dans Xkeystore pour l'année 2012 seulement était de 2 milliards par jour soit un bilan de 700 milliards par an. Ce chiffre rend Google minuscule et ce système ne cible pas seulement les problèmes de sécurité mais aussi toutes les communications. Dans le cas de la France, il y a des points d'interception pour collecter ce trafic dans les villes de Brighton où j'habite et Douvres sur la Manche.

Quand j'ai révélé l'existence du système Echelon en 1998, personne n'y a prêté attention. C'est seulement en 2000 que l'existence d' Echelon et la surveillance de masse des réseaux de communication ont été discutées à grande échelle. À cette époque-là, personne, évidemment, n'y croyait et c'était compréhensible. La plupart de ces doutes se sont évanouis depuis les révélations SNOWDEN. Je suis très heureux de dire ici que la preuve finale de l'existence et l'étendue du système Echelon sont devenues vérifiables et disponibles grâce à Édouard SNOWDEN. Les documents SNOWDEN qui décrivent comment et quand Echelon a été construit n'ont pas été publiés mais vont bientôt apparaître dans le magazine The Intercept qui est géré par le journal Escape, quotidien d'information qui a d'abord parlé avec M. SNOWDEN.

Les documents confirmeront que le programme Echelon a été créé au milieu des années 60 au pic de la guerre froide. Les américains voulaient surveiller les communications de l'Union Soviétique. Le plus étonnant à cette époque-là était que les États-Unis avaient peur que leurs activités puissent aller à l'encontre des traités internationaux. La première station a été construite en Angleterre où le régime juridique est moins contraignant. Ce système a été aussi utilisé pour la surveillance des communications commerciales. Les communications des citoyens américains ou des dissidents faisant campagne contre la guerre du Vietnam ont été également surveillées. Selon le document SNOWDEN, les américains ont payé pour l'équi-

3 En informatique, le Deep Packet Inspection (DPI), en français Inspection des Paquets en Profondeur, est l'activité pour un équipement d'infrastructure de réseau d'analyser le contenu (au-delà de l'en-tête) d'un paquet réseau (paquet IP le plus souvent) de façon à en tirer des statistiques, à filtrer ceux-ci ou à détecter des intrusions, du spam ou tout autre contenu prédéfini. Le DPI peut servir notamment à la censure sur Internet ou dans le cadre de dispositifs de protection de la propriété intellectuelle. Cf :http://fr.wikipedia.org/wiki/Deep_packet_inspection

4 empora est le nom d'un programme de surveillance électronique du GCHQ, qui permet à l'agence britannique d'intercepter les données transitant par les câbles en fibre optique entre l'Europe et les États-Unis. Cf http://fr.wikipedia.org/wiki/Tempora

5 Xkeystore est un programme de surveillance de masse créé par la NSA et opéré conjointement avec les services de renseignements britanniques, canadiens, australiens et néo-zélandais. Il permettrait une « collecte quasi-systématique des activités de tout utilisateur sur Internet « , grâce à plus de 700 serveurs localisés dans plusieurs dizaines de pays. Cf http://fr.wikipedia.org/wiki/XKeyscore

pement de toutes les stations d'écoute dans le cadre de l'accord Echelon. Là aussi, ces documents seront diffusés prochainement.
L'utilisation des satellites dans le domaine des communications, le fait que les signaux de l'espace envoyés par les différents pays pouvaient être interceptés de manière fiable à partir d'un point unique, ces éléments tendraient à prouver que les notions de frontières et de souveraineté nationale n'existent plus. Comment pourrait-on avoir des discussions sur la souveraineté dès lors que les communications peuvent être interceptées n'importe où ?
À partir de 1968, même si les liens de communication étaient analogiques, les premiers ordinateurs étaient utilisés pour voler les contenus de signaux télégraphiques et analyser les trafics téléphoniques avec des mots-clés ou des numéros cibles. Le grand public n'avait pas entendu parler de ces technologies qui sont maintenant des choses très largement répandues. L'étendue de la surveillance est pratiquement incompréhensible. Il y a des pays entiers où les télécommunications sont enregistrées et gardées pendant plus d'un mois. Si un journaliste avait déclaré cela il y a un ou deux ans, il aurait été perçu comme un paranoïaque ou souffrant d'un problème mental. Ceci n'est pas de la science fiction. Tous les documents sont accessibles sur Google en utilisant le nom de code Mystic. Les réseaux de communication ne sont pas simplement suivis pour détecter des attaques terroristes. Bien sûr, ils sont utilisés à cette fin, mais les communications politiques et commerciales sont aussi ciblées, y compris chez les alliés. Les technologies allemandes ont été ciblées et volées selon les documents SNOWDEN. Les ministères de l'énergie de pays comme le Brésil ou le Mexique ont été pénétrés de force avec des malwares en vue d'obtenir des renseignements. Les négociations sur le changement climatique à Londres et Copenhague ont été ciblées ainsi que les échanges commerciaux. Il y a un exemple marquant des méthodes criminelles, il s'agit d'une attaque sur quatre ans commise par GCHQ aux préjudices des sociétés Belges Belgacom. Des malwares sophistiqués ont été placés pour prendre le contrôle des réseaux mobiles de ces sociétés, surveiller les communications grâce à cette interception (man-in-the-middle attack). Les dommages se sont montés à plusieurs millions d'euros. Le problème n'a pas été résolu de manière claire. Si ces attaquants étaient venus du Moyen-Orient, ils auraient été qualifiés de criminels, car c'est ce qu'ils sont, des démarches auraient été entreprises pour qu'ils soient extradés et emprisonnés. Le silence des gouvernements Britannique et Belge soulève des questions. De tristes événements comme ceux qui se sont déroulés à Paris ont été exploités rapidement par le Premier Ministre du Royaume-Uni pour tenter de distraire l'opinion des activités illégitimes des agences de renseignement. Les dernières attaques, le meurtre du soldat britannique, les attaques à Boston et les attentats de Paris, prouvent que le vœu des agences de renseignement de pénétrer la sécurité de tous les réseaux que vous et les personnes de cette conférence utilisent ne répond pas aux attentes. Il semble qu'il serait plus utile d'utiliser des ressources humaines proches des cibles identifiées plutôt que pénétrer les communications de tout un chacun et de menacer la sécurité de tous. Tout cela crée des défis globaux, auxquels nous serons confrontés et dont nous discuterons, pour ce que dans les années 90 nous appelions les cyberguerres. La cyberguerre est de retour.

Michel PICOT : Je ne pensais pas que nous étions encore écoutés par les grandes oreilles de Boston et Douvres, ou qu'il y avait des grandes oreilles là-bas. Nous voyons que les enjeux sont très importants dans cette cybercriminalité ou cyberguerre économique. Maintenant, nous

allons essayer de savoir quelle dose de souveraineté numérique il est nécessaire d'instaurer. Quel est son juste milieu ? Didier TRUTT, quelle est votre analyse par rapport à tout ce qui a été dit ?

Didier TRUTT : D'abord, ça fait peur, M. CAMPBELL, ce que vous décrivez. Cela met en lumière l'enjeu géostratégique et politique révélé au travers de Wikileaks et des affaires SNOWDEN.

Je vais reprendre le début. Quand nous parlons de souveraineté, sommes-nous dans un cyberespace arrivé à maturité ? Quand je préparais cette intervention, j'étais plutôt enclin à dire pas tout à fait, aujourd'hui je dirai définitivement non. Le cyberspace est un espace jeune : trente ans. Si vous regardez cette durée par rapport à d'autres technologies comme l'aéronautique, les télécoms, l'automobile, qui n'ont eu de cesse d'évoluer, de se transformer depuis plus d'un siècle, trente ans c'est très jeune. J'ai l'espoir que les avancées majeures des technologies seront plutôt devant nous que derrière nous.

Quand nous prenons les entreprises qui régissent ce monde : les GAFA (Google, Apple, Facebook, Amazon), ce sont des entreprises restées très jeunes, agiles, mais qui sont toutes cotées en bourse. Ces dernières pèsent pour la plupart d'entre elles plus d'une dizaine de milliards d'euros. Leur caractéristique est de savoir réinventer leur modèle économique. Citons un exemple : Google, à l'origine un moteur de recherche à base d'algorithmes, cette entreprise investit aujourd'hui dans l'intelligence artificielle et demain sur les objets connectés. Autre exemple, Apple a développé plus de 700 000 applications. Nous sommes encore au début de la dématérialisation. Nous le voyons au travers des contenus tels que la musique, les films... La dématérialisation qui est devant nous concernera des secteurs plus stratégiques : la santé, la banque, où il faudra des infrastructures plus complexes mettant davantage en jeu nos données personnelles. Les données personnelles sont déjà largement utilisées et collectées. Les données personnelles qui seront en jeu demain seront plus massives et stratégiques. Quand nous examinons l'ensemble de ces réflexions sous l'angle de « la souveraineté numérique vrai ou faux débat », je me dis, heureusement, que nous assistons à une prise de conscience des États. Ces derniers se demandent comment légiférer autour de l'utilisation de la donnée personnelle. Nous voyons bien que cette législation ne peut pas se faire uniquement au niveau national mais se situe à l'échelle d'Internet c'est-à-dire à un niveau mondial.

Michel PICOT : Laure de la RAUDIÈRE, vous voulez rebondir ?

Laure de la RAUDIÈRE : Internet est mondial. Une législation mondiale sur les données personnelles me paraît utopique. Nous ne pouvons pas aussi imaginer une régulation franco-française sous peine d'handicaper l'économie numérique en France alors que notre pays a été récemment mis en avant au salon de Las Vegas. La France a prouvé sa capacité à développer toutes ces nouvelles technologies, à innover dans le domaine des objets connectés qui contiennent beaucoup de données personnelles. À ce sujet, Les citoyens demandent plusieurs choses s'agissant des données personnelles :

- D'abord, ils exigent qu'on garantisse la protection de leurs données. Vous avez tous en tête le scandale des « starlettes » américaines dont les photos intimes ont fuité sur le net. Ces victimes ne s'étaient pas fait voler leurs photos dans leur portable, ni voler ce dernier. C'est chez l'hébergeur que leurs photos intimes ont été piratées. Cette situation n'est pas tolérable. Lorsque nos données personnelles sont hébergées dans un cloud américain, français, européen, nous

avons besoin d'avoir une assurance, une garantie qu'elles ne seront pas piratées. Les citoyens attendent de l'hébergeur qu'il mette tout en œuvre pour ne pas se faire attaquer. Ceci constitue la première exigence des citoyens : la protection des données personnelles hébergées.
- Ensuite, deuxième exigence, les citoyens veulent être en mesure de récupérer leurs donnés personnelles. Exemple, j'ai confié à Facebook certaines données, je veux pouvoir les récupérer. Je veux obtenir l'assurance que mes données sont anonymisées, non conservées par cet opérateur, lui interdisant ainsi de me tracer plus tard.
- Enfin, dernière exigence, le citoyen veut savoir ce qu'il advient de ses données : à qui sont-elles revendues ? Il voudrait définir le seuil d'autorisation qu'il accorde à un opérateur en matière d'usage de ses données personnelles. Plus concrètement : est-ce que j'autorise à être pisté partout par Google dès que j'utilise une application de mon portable ? Est-ce que j'autorise l'usage de mes données uniquement en matière de profilage ?
Ces débats doivent avoir lieu avec les citoyens. Les politiques doivent s'emparer de ces sujets-là pour trouver une positon commune. Dans cette matière, je crois que le niveau européen est une bonne taille. En effet, le marché européen, c'est 500 millions de consommateurs dotés d'un fort pouvoir d'achat. Ce marché est suffisamment important pour pouvoir dicter des règles et les imposer sur le plan commercial à des géants d'Internet majoritairement américains aujourd'hui. Les analyses et les études montrent que les marges de ces géants américains sont majoritairement faites en Europe.

Michel PICOT : Comment s'y prend-on ?

Gwendal ROUILLARD : J'aurai trois remarques à faire. Ma première remarque est en rapport à l'affaire Echelon en passant par l'affaire Prism. Cette période couvre finalement 20 à 30 ans de stratégie américaine. Ce que je retiens de ces affaires successives et des pratiques qui en ont découlé, ce sont les liens consubstantiels entre l'État américain et ses entreprises ressortissantes au service d'une stratégie commune entre le Pentagone, Google ,Apple et d'autres sociétés américaines. Ma seconde remarque me ramène à la France. Notre pays met en œuvre dans le cadre de la LPM son pacte de cyberdéfense. Il s'agit de 50 mesures centrées sur trois volets : formation pour répondre aux besoins des entreprises et former des personnels, recherche, et enfin soutien aux grands groupes (PME, fonds propres et bien d'autres dispositifs). Le fil conducteur du pacte cyberdéfense, c'est bien l'éthique. Parmi les discussions que nous allons avoir au Parlement sur la loi de programmation militaire ou la loi sur le renseignement, le mot « éthique » est central. En effet, la France doit garantir son autonomie stratégique par sa loi de programmation militaire, son agence nationale de sécurité des systèmes d'information (ANSSI). Les décisions prises en conseil de Défense ont porté aussi sur le renforcement des capacités du ministère de l'intérieur en matière cyber. Cette forme d'éthique est dans le même temps pratiquée sur les théâtres extérieurs du Mali, de la Centrafrique ou bien en Irak. Tout ceci doit alimenter le débat citoyen.
Dernière remarque enfin, comment faire face à ces défis, qui sont devant nous, pour être prêt à la fois sur le plan stratégique et technique ? Lorsque j'écoute les discussions entre politiques, militaires, industriels mais aussi entreprises et citoyens, nous avons quatre défis devant nous pour permettre à la France et à ses concitoyens de réussir à se réapproprier en partie leurs données personnelles. Les quatre défis qui vont faire débat tant à Paris qu'à Bruxelles dans les semaines à venir s'inscrivent notamment dans la perspective du conseil européen de Défense et du paquet « Juncker », d'un montant

de 300 milliards d'euros. Ces quatre sujets sont : quid d'un système d'exploitation en France et en Europe ? Quid du cloud ? Quid du big data ? Et enfin, quid du/des moteurs de recherche ? Ces quatre chantiers sont clairement posés sur la table aujourd'hui. Le vœu que je formule collectivement pour notre nation, c'est qu'elle puisse investir de manière réactive. La France ne manque pas d'atouts, elle dispose des compétences et des savoir-faire dans ses entreprises. Encore faut-il jouer collectivement ces cartes et c'est maintenant que cela se passe.

Michel PICOT : Il y a actuellement une prise de conscience. Un tweet pose la question suivante : peut-on imaginer de souscrire une assurance contre le vol des données ?

Laure de la RAUDIÈRE : Sur cette question, je réponds « oui, il le faut ». Une société de ma circonscription vend des assurances dans le domaine de la cybersécurité.

Michel PICOT : Vous avez donné le cadre, l'évolution, on saisit bien vers quoi vous tendez...

Laure de la RAUDIÈRE : J'ai entendu deux choses sur le cloud et le big data. Nous pouvons donner un cadre à la protection des données personnelles. Sur l'hypothèse d'un système d'exploitation et d'un moteur de recherche européen, même si des milliards sont posés sur la table, nous ne concurrencerons pas Google. À mon avis, ce n'est pas la meilleure utilisation de l'argent public au niveau européen. L'innovation numérique ne se décrète pas, ne se conçoit pas en haut et de cette façon-là. Il serait plus utile de réfléchir sur l'usage des données personnelles et de ce qui est autorisé. Il serait possible de savoir où se trouvent les données personnelles sur Internet et que l'Europe exige certaines normes de protection. Imaginer, parce qu'on va le décider au niveau du programme JUNCKER, de faire un nouveau moteur de recherche européen pour concurrencer Google, j'ai du mal à souscrire à cette idée-là.

Michel PICOT : un Tweet pose la question suivante: avant de définir quoi que ce soit, que veut faire la France au niveau cyber ?

Bernard OURGHANLIAN : Je voulais juste réagir par rapport aux questions concernant l'usage fait des données. Où sont-elles ? À qui appartiennent-elles ?... Au final, la souveraineté est citoyenne. Même si la souveraineté numérique est conférée à un État, elle appartient de jure à un citoyen. Dans un cadre tel que celui-ci, nous pouvons imaginer tout un tas d'hypothèses telles que faire appel à une corégulation, voire compter sur une autorégulation des sociétés. Si nous sommes réalistes, la régulation sera nécessaire et ne pourra avoir une influence que si elle se manifeste et s'installe au niveau européen. Ainsi, il existe un projet de réglementation européenne relative au respect de la vie privée des données. Ce projet prévoyait dans l'ancienne mandature une sanction pouvant aller jusqu'à 5 % du Chiffre d'affaires (CA) mondial de l'entreprise prise « la main dans le pot de confiture ». La mandature en cours devrait confirmer cette sanction. Cet aspect sanction est un élément de nature suffisamment dissuasif, quel que soit le statut de la société, en particulier pour celles cotées en bourse. À un moment donné, le patron doit rendre des comptes à ses actionnaires. Il devra prendre les mesures qui, en interne, amènent à respecter cette réglementation. Une amende de 5 % sur le CA a un effet suffisamment dissuasif pour que les sociétés, y compris américaines, se conforment à cette réglementation. Le règlement européen s'applique instantanément dans l'ensemble des pays européens contrairement à la directive qui nécessite un processus de transcription dans l'ordre juridique de chaque État. Si l'Europe va dans cette di-

rection, elle se dotera de facto des moyens de redonner à chacun des citoyens sa souveraineté numérique. Ce futur règlement sera de nature à faire évoluer globalement le marché, non seulement au niveau européen, mais à l'échelle mondiale aussi. Sur le plan économique, l'Europe pèse beaucoup dans les comptes d'exploitation des sociétés, y compris s'agissant de sociétés comme Microsoft.

Didier TRUTT : Légiférer au niveau international est certes une utopie mais le faire à l'échelle du marché européen, ce résultat serait déjà appréciable. Vous avez remarqué que chaque fois qu'on se connecte sur un site des GAFA, il est demandé à l'utilisateur d'accepter leurs conditions contenues dans 74 pages que généralement personne ne lit. L'immense majorité clique sur l'onglet agree sans consulter la totalité des clauses. À partir de ce moment, il se réalise une collecte massive de nos données, finalement disséminées partout dans le monde. Nous sommes au début de ce processus de collecte de données. La révolution des objets connectés va amener à la collection de davantage de données. Comment faire pour que ces données continuent à nous appartenir ? Si chacun au final doit tenter de conserver ses données, cela sera compliqué. Il nous faut trouver un cadre permettant de récupérer nos données et de les garder.

Michel PICOT : Cela paraît impossible, extrêmement complexe, les réseaux sociaux ne sont pas que des « grands méchants loups ».

Didier TRUTT : Oui, mais je veux pouvoir, si je le souhaite, contrôler, récupérer mes données, être sûr qu'elles m'appartiennent encore. A partir du clic sur agree, c'est difficile. Nous n'allons pas réinventer un Google européen mais nous avons en revanche énormément d'entreprises, dont certaines sont françaises, qui sont généralement d'excellentes start-up. Nous avons vu ces dernières à Las Vegas, présentant des objets connectés. Ainsi, le président d'Accenture a décidé, suite aux audits réalisés dans tous ses sites de développement, de conserver celui implanté en France en dépit de son coût. En effet, le site français se révèle être le meilleur et le plus productif de tous. Nous avons en France des sociétés capables de se développer.
Toutefois, les start-up se demandent si elles peuvent se développer sur le marché national et atteindre à terme le marché européen. Nous ne développerons pas le Google de demain mais nous pourrons investir le monde des objets tout en protégeant nos données. Nous avons donc devant nous un vecteur de croissance.

Michel PICOT : Je vous livre ce commentaire provenant d'un Tweet : on a bien réussi à réguler l'espace au niveau international sans perte de souveraineté, pourquoi le numérique est-il si compliqué ?

Laure de la RAUDIÈRE : Il y a 60 millions de Français. Au moment où on a régulé l'espace aérien il y avait moins d'utilisateurs de cet espace.

Gwendal ROUILLARD : Je voudrais apporter un commentaire sur les législations internationales, en particulier le volet défense et militaire. Dans ce domaine, nous avons un début de droit international avec la convention dite de Budapest sur la cybercriminalité. Cette convention a été mise sur les rails par les pays membres de l'Organisation du traité de l'atlantique nord (OTAN) et renforcée dans ses dispositions suite à l'épisode de l'Estonie en 2007. Cette convention a été signée par d'autres pays, notamment l'Australie et le Japon. Cet exemple montre que des discussions sont toujours possibles, bien qu'il faille rester conscient des limites de l'exercice. Il n'est pas interdit aux instances civiles de s'inspirer de manière schématique des bonnes pratiques militaires. La

convention de Budapest a été éprouvée positivement par les pays contractants, notamment ceux qui sont membres de l'OTAN.

Michel PICOT :Allons un peu plus loin sur cette part de souveraineté d'État dans le numérique. Pierre BELLANGER nous expliquait que les données, aujourd'hui, ne sont plus isolées et demeurent exploitables assez facilement. Il considère que les réseaux sont devenus un État. Selon lui, pour faire cesser l'anarchie qui règne dans le numérique, il faudrait une dose de souveraineté nationale en s'appuyant sur les lois républicaines en vigueur. Ces dernières pourraient faire l'objet d'une retranscription et d'une adaptation dans le numérique. Selon vous, quelle est la part de souveraineté nationale dans le numérique ?

Duncan CAMPBELL : je pense que le thème qui serait intéressant de traiter est ce qu'on appelle la neutralité du net. Ce concept intègre l'idéalisme d'un média de communication universel que nous pouvons certainement relier au thème échangé aujourd'hui. Les exemples plus sérieux d'interférence par rapport à cette neutralité sont liés au blocage et au contrôle du trafic, à la surveillance mais aussi à l'interférence de ce trafic. Pour ces deux dernières années, l'exemple le plus marquant porte sur le grand pare-feu de Chine. Il existe beaucoup de pressions en Europe pour transférer le contrôle de ce qui est envoyé par le biais d'Internet à la charge des entreprises de communication. Jusqu'à présent, il était établi, dans les litiges, que les transporteurs de données n'avaient pas de responsabilité sur les communications acheminées par les câbles. Maintenant, les limites de l'Internet ont commencé à remettre en cause ce principe. Elles peuvent se montrer subversives, au grand dam de la majorité des utilisateurs et à la satisfaction de certains intérêts, politiques ou autres. L'interférence, si elle devient possible, nous fait quitter le champ des médias de communication courants. Les technologies mises en place à l'heure actuelle permettent des manipulations et des sélections de trafic en fonction des destinations. Pour mémoire, les premiers raccordements techniques ont été faits au milieu des années 90. Nous avons appris que la surveillance de masse, mais aussi les interfaces secrètes, sont désormais possibles. Nous sommes passés d'un média bénéficiant d'une confiance universelle à un média exposé aux interférences et auquel nous ne pouvons plus faire confiance. Pour les élus ici présents, c'est une question. Il existe un fossé que nous ne pourrons pas combler pour avoir une sécurité imbattable. Pouvons-nous l'avoir ? Si la réponse est oui, alors nous défendons notre business, notre sécurité, notre vie privée, et nous barrons la route à des gens comme David CAMERON qui prétendent que nous devons être capable de rentrer dans tous les systèmes. Des personnes vous disent aussi que si vous cassez la sécurité pour un, vous cassez la sécurité pour tous. L'inconvénient pour la société sera plus de cyber-attaques avec en filigrane des informations personnelles et des données perdues. Au final, les économies en souffriront. Les défis sont tout autant difficiles dans la gestion des affaires publiques. Il est impossible d'arrêter tous les crimes, d'empêcher les délinquants de communiquer ou d'utiliser des voitures, des avions ainsi que les systèmes de sécurité sur Internet. Il faut du courage pour protéger la neutralité du net mais c'est le prix à payer.

Michel PICOT : Nous pourrions le résumer par la question suivante : liberté et sécurité sont-elles compatibles ?

Gwendal ROUILLARD : La réponse est oui même si il est difficile de positionner le curseur. Prenons deux exemples : depuis plusieurs années, la France a développé son agence spécialisée, l'ANSSI, forte de 400 personnes mobilisées pour notre

sécurité informatique et numérique. Cet effectif sera porté à 700 en 2017. Pour le ministère de la Défense, chaque jour des équipes se mobilisent pour participer à cette sécurité. Dans nos territoires, le pôle cyber-Bretagne participe aussi à l'exercice de la souveraineté dans les volets formation, entreprise et recherche, ainsi que je l'avais évoqué. Nous voyons bien que nous nous situons entre surveillance, veille, capacité de mobilisation d'un pays et en même temps capacité à discerner. Pour reprendre les discussions d'aujourd'hui, mettons du rationnel dans ce débat. Un incident informatique n'est pas une attaque informatique ; de même une attaque informatique n'est pas une agression informatique. Un groupe, face à nous, n'est pas forcément un État. Il nous faut aussi du discernement par rapport à ce débat sur la souveraineté, sur ce lien sécurité / liberté. Je rajouterai aussi le mot éthique, parce que pour les Français, il ne s'agit pas d'un vain mot mais de pratiques qui en découlent. C'est important de bien situer l'éthique durant ces discussions.

Michel PICOT : J'ai un peu le sentiment, comme le disait Didier TRUTT, que tout cela est très jeune et dans une phase de recherche qui toutefois s'accélère un peu. Ferons-nous le même débat l'année prochaine ou aurons-nous avancé ?

Laure de la RAUDIÈRE : Il y a un sujet que nous avons peu abordé concrètement. Dans nombre de sujets, les États laissent des sociétés privées dire qu'est ce qui est bon dans la protection des données, ou en matière de droit à l'oubli. Je rejoins Gwendal ROUILLARD sur le fait que c'est au politique, au gouvernement de dire ce qu'ils veut. Ce n'est pas à Google ou Facebook de nous expliquer qu'ils protègent nos vies privées, qu'ils ont mis en place le droit à l'oubli…

PICOT Michel : Pour autant, je ne vois pas trop quelle est la position du gouvernement à ce sujet.

Laure de la RAUDIÈRE : Non, mais c'est extrêmement important de le rappeler aussi. Dans les faits, nous demandons à Google, Facebook ou Twitter d'aller effectuer cette police privée pour nous. Je suis vraiment opposée à ces comportements. C'est à nous de définir ce que nous voulons et de le vérifier. Je pense encore une fois que c'est au niveau européen de mettre en œuvre une politique de régulation. Nous n'y arriverons pas seuls mais en travaillant par exemple de manière bilatérale avec les Allemands. Ces derniers sont extrêmement sensibilisés sur le sujet des données personnelles tout comme les Espagnols, les Italiens. C'est au niveau des chefs d'État et des ministres européens que ces discussions doivent se mener. Il ne revient pas à la Commission européenne d'essayer de régler ces enjeux-là en ouvrant des discussions auprès des acteurs américains.

Michel PICOT : Ces discussions ont-elles lieu ? Excusez-moi, mais j'ai l'impression d'entendre cela depuis deux, trois, voire quatre ans… Y-a-t-il des travaux ? Y-a-t-il des avancées ? Après les dramatiques attentats de Paris, nous voyons effectivement une accélération aujourd'hui.

Laure de la RAUDIÈRE : Nous voyons effectivement un tournant en 2014. Vous parlez de trois, quatre ans je ne suis pas d'accord. Fin 2013, il y a eu l'affaire SNOWDEN qui a été un révélateur, en particulier pour les Allemands au plus haut niveau. La sensibilisation d'Angela MERCKEL a fait en quelque sorte « boule de neige » en Europe. Les discussions au plus haut niveau des États sur ces enjeux sont relativement récentes. Je ne parle pas des attaques informatiques des États, identifiées comme un enjeu de Défense depuis longtemps et mentionnées dans le Livre blanc de la

Défense nationale de 2008. Je fais allusion à la protection des données personnelles privées des citoyens, mais aussi des écoutes généralisées. La prise de conscience de ces sujets au niveau européen date de 2014.

Michel PICOT : Un Tweet soulève à la fois une question et un commentaire : la souveraineté numérique passe par une maîtrise des logiciels, du champ des perceptions mais aussi des matériels. Cette maîtrise est-elle possible pour la France ? Je crois que nous pouvons répondre de manière affirmative à cette question.

Nous allons faire un dernier tour de table en guise de conclusion et de perspective. Je voudrais dégager une idée forte à l'issue de ce thème qui nous anime. Nous avons vu que nous n'étions qu'au début de l'âge de la souveraineté numérique. L'année prochaine, j'espère que dans une discussion similaire nous aurons des choses beaucoup plus concrètes à exprimer aux usagers, aux entreprises et de manière plus globale à cette toile du numérique en fixant un cadre. Nous compterons bien entendu sur vos contributions.

Didier TRUTT : À la question posée, à savoir si l'an prochain nous aurons progressé, je dis oui. Je rejoins Laure de la RAUDIÈRE sur une vraie prise de conscience en 2014. Je reste optimiste et réaliste sur la technologie. Elle va continuer à évoluer pour enfin amener quelque chose de plus concret. Pour rappel, il y a un règlement européen voté le 23 juillet 2014 dénommé e-IDAS[6]. La France va devoir appliquer ce règlement européen. La finalité de ce document est de nous permettre, entre tous les États européens, d'échanger et de reconnaître un certains nombre de documents dématérialisés. C'est aussi une question en France de définir quelle solution nous allons mettre en place pour participer de manière effective en œuvrant au niveau européen à travers ce règlement. J'ai lu un Tweet sur l'identité digitale souveraine, thème qu'il faudra mettre aussi sur la table. Personnellement, je crois que les identités sont multiples à travers les réseaux. Au final, cela serait préjudiciable que les GAFA soient les seuls à être en mesure de fournir des identités à nos citoyens.

Michel PICOT : Pour résumer, il s'agit d'instaurer une identité numérique souveraine pour mieux se positionner vis-à-vis des GAFA

Bernard OURGHANLIAN : Je voudrais terminer par deux commentaires. Le premier porte sur l'évolution de la réglementation européenne que nous appelons tous de nos vœux. Celle-ci va au-delà de la question de l'acceptation, sur un simple clic, des conditions d'utilisation des données privées. Nous allons faire reposer la responsabilité et l'éthique de l'utilisation de ces données sur les entreprises collectrices, avec potentiellement des pénalités financières extrêmement lourdes. Nous renversons la responsabilité, qui ne repose pas simplement sur les épaules du citoyen mais aussi sur les épaules de ces sociétés. Le deuxième commentaire concerne un élément que je vais offrir à la réflexion. Nous avons beaucoup parlé d'un équilibre subtil à trouver entre liberté et sécurité. Ce débat ne date pas d'hier, je vous renvoie au poète satirique latin Juvénal mais aussi à la République de Platon. Il y a une phrase extrêmement intéressante de Juvénal : « qui gardera ses gardiens ? » Une des problématiques qui apparaît dans l'af-

6 e-IDAS :http://www.ssi.gouv.fr/administration/reglementation/administration-electronique/le-reglement-n-9102014-du-parlement-europeen-et-du-conseil-sur-lidentification-electronique-et-les-services-de-confiance-pour-les-transactions-electroniques-au-sein-du-marche-interieur/

faire SNOWDEN est, pour être très clair, que la NSA a délibérément violé la loi américaine. Le problème, c'est qu'en l'occurrence il n'y a eu aucun contrôle démocratique de l'usage fait de la loi. En conséquence, le problème qui se pose dans les pays démocratiques et à la France en particulier est le suivant : à partir du moment où nous, citoyens, donnons à nos gouvernants le pouvoir de diminuer notre liberté pour nous donner plus de sécurité, il faut que ce pouvoir s'exerce sous un contrôle démocratique extrêmement strict, qui doit être amélioré.

Gwendal ROUILLARD : Pour faire la transition, j'ajouterai deux points. Premier point, le Parlement mobilise une partie de ses élus au sein de la Commission nationale du renseignement. Depuis plusieurs années, je constate que cela fonctionne bien, même si nous devons améliorer le dispositif et certainement les modalités du contrôle démocratique. Deuxième point, quand la France demande aujourd'hui à Facebook de retirer des vidéos, notamment sur des décapitations, cette société s'y conforme. Je le dis car ces dernières années nous avons progressé, gouvernement après gouvernement. Pour autant, je le reconnais, le chantier est largement devant nous. Deux derniers éléments. Produisons du droit, chacun l'a bien compris en France, en Europe et au niveau international. Enfin, ainsi que je le disais déjà à Nantes au Forum de cybersécurité, chaque citoyen est détenteur d'une part de la souveraineté nationale et c'est plus que jamais d'actualité. Voici quelques années, on voyait des sourires quand nous prononcions ce genre de phrase. Lorsque nous disons que chaque citoyen détient sa part de souveraineté nationale c'est vrai. Le dernier mot, c'est l'esprit du 11 janvier 2015. La République s'est réveillée le 11 janvier 2015, je souhaite que la République reste éveillée durablement et que nous mettions en première ligne la cybersécurité. C'est le vœu que je formule pour les prochaines années.

Michel PICOT : Laure de La RAUDIÈRE un mot de la fin, puis se sera Duncan CAMPBELL pour terminer.

Laure de la RAUDIÈRE : Nous devrons défendre les civilisations, à l'instar du 11 janvier 2015, où les citoyens se sont réveillés pour défendre les valeurs de notre République face aux choix de civilisation profondément différents des terroristes. Nous nous devons aussi de savoir quelle civilisation va se défendre demain dans ce monde du numérique. Nous devons dire quelle sera la valeur de la vie privée demain. Achèterons-nous celle du PDG de Google qui considère la fin de l'existence de la vie privée ? Ou affirmons-nous que cette dernière est le premier espace de liberté ? Est-ce que nous achetons une vision transhumaniste de la société où nous serions capables, par une bonne sélection des génomes, de jouer sur les capacités intellectuelles des enfants à venir ? Est-ce que nous acceptons cela alors que se déroulent, en ce moment, des travaux sur l'intelligence artificielle ? Devons-nous définir une éthique commune et nous y tenir ? Devrons nous aussi accepter de mettre à mal notre principe de solidarité alors que, demain, les assureurs serons en mesure de faire des offres personnalisées en fonction de chaque individu ? Ou continuerons-nous, comme aujourd'hui, à mutualiser le risque sur un plus grand nombre de personnes? Ce sont ces questions-là auxquelles le politique doit réfléchir au niveau franco-français, pour qu'ensuite nous puissions porter ces ambitions avec nos partenaires européens, pour ainsi dicter des règles extrêmement importantes pour défendre notre civilisation et notre façon de la vivre.

Duncan CAMPBELL : Madame Laure De La RAUDIÈRE a mentionné les expériences eu-

ropéennes. Je pense que celles-ci sont une réussite et constituent un point approprié pour réfléchir sur la souveraineté. Il y a cinquante ans, nous avions des frontières qui nous divisaient, des agences nationales confidentielles qui ne partageaient rien et permettaient finalement à des factions de fomenter des actions clandestines. Nous pouvons regarder maintenant l'intégration européenne malgré ses difficultés. Cette intégration a éliminé ces barrières de manière formidable, elle a créé de la transparence et permis, en supprimant les divisions, la création de valeur. Cela devrait s'appliquer également aux communications. Mettez des murs autour d'Internet et vous diminuez la culture et l'économie pour tous. Mais il y a aussi la bataille de ceux qui veulent avoir une politique de la peur. Cette dernière ne disparaîtra jamais. Nous avons eu de bonnes présentations de Bruce SCHNEIER sur les manières difficiles de regarder la peur et la facilité d'exploiter la peur des technologies ou la peur des méchants ou la peur du noir. Les gains que nous retirons de l'Internet, de l'économie et de l'infrastructure numériques, qui fonctionnent, sont largement supérieurs aux dommages qu'ils provoquent. J'espère que, malgré les problèmes que crée mon pays, l'Europe et en particulier la France prendront le leadership dans ce domaine.

ARTICLE A 01

Contenus illicites : de la détection au retrait ?

Intervenants :
- Charles-Edouard PEZE, Juriste, Gandi.Net,
- Alain DOUSTALET, Directeur département Abuse, Orange
- Alexandre HUGLA, responsable département Abuse, Gandi.net
- Eric FREYSSINET, chef de division de la lutte contre la cybercriminalité
- Stéphane BORTZMEYER, AFNIC

Résumé des interventions :
Cet atelier présente des cas concrets de contenus illicites et expose les solutions pratiques existantes pour parvenir à leur retrait. L'objectif est de permettre à chaque usager de l'espace numérique, qu'il soit professionnel ou amateur, d'identifier précisément le rôle, les compétences et les pouvoirs de chaque acteur de la chaîne de publication, afin de savoir à qui s'adresser quand il est confronté à des contenus illégaux. Les trois exemples retenus sont les suivants : le phishing, les malware et les spam. Un petit Livre blanc, distribué à la fin de l'atelier, est consultable sur le site et le complète par d'autres situations pratiques pouvant être rencontrées : fraude 419, défiguration de site, contenus incitant à la haine raciale et diffamatoires (http://pres.gandi.net).

I. Le phishing

Un client reçoit un courriel du conseiller de sa banque lui demandant de se connecter sur le site de la société pour lire un message. La personne clique sur le lien proposé, aboutit sur l'interface d'apparence habituelle et entre plusieurs fois, sans succès, ses identifiant et mot de passe. Puis il constate des virements SEPA vers l'extérieur, dont il n'est pas l'auteur. Vers qui doit-il alors se tourner pour déclarer la fraude ?

Le CERT (Computer Emergency Response Team) de la banque a pour mission de prévenir, de détecter et de traiter les menaces informatiques. Les acteurs techniques recherchent, parmi les noms de domaine qui sont déposés quotidiennement, ceux qui seraient susceptibles d'être utilisés pour une escroquerie, dont le phishing. Dès qu'une opération de phishing est

repérée ou signalée, les clients, victimes réelles ou potentielles, sont contactés et incités à déposer plainte. De plus, le CERT notifie le phishing aux bureaux d'enregistrement, FAI et hébergeurs.

L'AFNIC (Association Française pour le Nommage Internet en Coopération), qui gère en partie les noms de domaine en .fr , n'exerce aucun contrôle a priori sur les noms de domaine, qui peuvent très bien se ressembler de manière légitime, sans qu'il y ait une volonté de tromper l'utilisateur. Par le passé, il est arrivé que certains soient supprimés trop rapidement, alors qu'ils proposaient des ressources utiles et fiables. De plus, dans le cas présent, ce n'est pas un site complet qui est en cause mais seulement le contenu web vers lequel le lien pointe dans le courriel reçu par le client. En l'occurrence, il n'est donc pas possible légalement de bloquer le nom de domaine. L'AFNIC procède néanmoins au signalement du mél litigieux à l'OCLCTIC (Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication).

Si l'AFNIC ne peut pas agir à son niveau, il est nécessaire, en revanche, de signaler immédiatement le mél malveillant à son fournisseur d'accès à Internet (FAI), sur une boîte dédiée à ce type d'alerte. Le mieux est de le transférer, afin qu'il puisse être analysé. Les « listes noires » (ou « blacklists ») des navigateurs Internet sont alors alimentées pour que tout client cherchant à se connecter via ce site de « hameçonnage » reçoive un message d'alerte (du type « Attention, cette page est peut-être une contrefaçon »). Cette procédure peut cependant demander du temps. C'est pourquoi elle doit être doublée d'une autre action, la recherche de l'hébergeur. Dès qu'il est identifié, le FAI contacte les gestionnaires de l'espace de stockage pour leur indiquer qu'ils hébergent un site contrefait visant à arnaquer des clients bancaires et pour leur demander de le bloquer. Dans 70% des cas, il est fermé dans la demi-journée qui suit le signalement.

Si les messages de phishing sont difficiles à filtrer en amont, du fait de leur forte ressemblance avec les messages officiels des entreprises, ces dernières doivent sensibiliser leurs clients et leur rappeler régulièrement (dans les newsletters ou dans les pages assistance) qu'en aucun cas, elles ne demandent par mél un identifiant et un mot de passe.

Les sociétés d'enregistrement de site ou/et les hébergeurs mettent en ligne sur leur portail des formulaires de signalement d'escroqueries. Dès qu'elles sont prévenues, elles vérifient l'identité de l'hébergé et le nom de domaine. Si le contenu signalé est effectivement illicite, elles suspendent le serveur immédiatement. Le nom de domaine apparaît encore pendant quelque temps, en raison d'un temps de propagation inévitable. En revanche, le site Web litigieux disparaît de la Toile dès sa suspension.

Il est à noter que l'obligation de procéder immédiatement à un retrait de contenu ne concerne que les cas de pédophilie et de négationnisme. Toutefois, les prestataires l'incluent généralement dans leurs conditions légales, bien que la loi ne les y contraigne pas.

La gendarmerie procède à une enquête et tente de récupérer les informations techniques permettant de mener les investigations. À cette fin, le bureau d'enregistrement et l'hébergeur doivent avoir conservé les données (traces de connexion ou de l'attaque), si le site a été piraté. Parfois, les informations collectées par le délinquant sur un site Web lui sont envoyées automatiquement par messagerie. L'adresse en question peut se révéler intéressante. Si l'infraction se commet depuis l'étranger, l'enquête sera plus complexe et plus longue.

II. Le malware

Un éditeur de presse en ligne reçoit un mél d'alerte du CERT dont il dépend : sa section « bourse et cotation » est infec-

tée. Il est victime d'un « watering hole » (qui signifie « trou d'eau », en référence au lion qui attend sa proie près d'un point d'eau où cette dernière se rendra inévitablement), méthode consistant à infecter les terminaux de personnes ciblées, en l'occurrence celles qui s'intéressent aux cours de la bourse et aux finances. Le CERT contacte tous les acteurs techniques (hébergeurs, Registrars) et bloque les éventuelles connexions à la section infectée. Afin d'éviter tout problème ultérieur, le CERT cherche à repérer les vulnérabilités du système d'exploitation et du navigateur, afin qu'elles puissent être corrigées.

Dans le cas présent, il s'agit d'un serveur d'hébergement dédié sur lequel se trouve un serveur racine. Seul l'hébergé a les accès. L'hébergeur ne peut pas voir ce qui se passe sur le site, il peut seulement détecter des tentatives de connexion inhabituelles depuis l'extérieur. N'étant pas habilité à pratiquer de l'infogérance, il ne peut analyser les données. De plus, il est impossible de procéder au retrait d'une partie d'un site Web. En liaison avec le support pour l'hébergement, il peut uniquement essayer de trouver une solution technique, en fonction des connaissances du moment, en s'appuyant sur les types de malware connus.

Les entreprises portent rarement plainte pour un événement de sécurité qu'elles ne souhaitent généralement pas divulguer. Quand elles en font la démarche, elles ont parfois déjà nettoyé ou réinstallé le site, dans leur souci de le rendre rapidement fonctionnel, effaçant ainsi le script malveillant, compliquant le travail d'enquête. Si le virus a pu être récupéré, il est analysé, soit par la gendarmerie elle-même, soit, à sa demande, par des éditeurs de sécurité. L'identification des objectifs des délinquants (détournement de données confidentielles, récupération de mots de passe, de numéros de cartes bancaires...) permet de déterminer le niveau de gravité des faits et d'adapter les moyens d'investigation. Enfin, les services d'enquête cherchent à identifier les victimes et les préviennent.

III. Le spam commercial

À la réception de méls commerciaux dont il est impossible de se désinscrire, il faut, en premier lieu, le signaler à son FAI, dans l'espace prévu à cet effet. Ce signalement est envoyé automatiquement et simultanément aux éditeurs anti-spams inclus dans les plate-formes. Les campagnes spam sont analysées au quotidien afin d'identifier celles qui causent le plus de plaintes. Un avertissement est envoyé et une discussion engagée. En cas d'échec, les FAI appliquent des solutions techniques : les messages sont renvoyés directement vers les boîtes spams des clients ou bien sont bloqués en entrée de plate-forme. Dans un deuxième temps, il faut fournir à l'hébergeur l'en-tête complet du mél non sollicité afin qu'il puisse déterminer par où il a transité et quels sont les serveurs impliqués. Il est demandé à l'hébergé d'ôter l'adresse e-mail des plaignants de ses listings ou de vérifier que ses envois contiennent un lien de désinscription fonctionnel. En cas de refus, il est menacé de suspension de son nom de domaine.

La CNIL reçoit chaque année la liste des campagnes spam les plus actives. Elle a le pouvoir de déclencher des enquêtes, de contacter les entreprises concernées pour leur demander de s'expliquer. Quelques sanctions ont été prises par le passé.

La gendarmerie, quant à elle, n'intervient, sur signalement par la CNIL ou par des professionnels, que dans les cas manifestement illégaux, tels que la vente de listes de prospection. Actuellement, plusieurs enquêtes sont en cours sur des gestionnaires de listes. Ces derniers, en infraction avec la Loi informatique et liberté, encourent une peine de 5 ans d'emprisonnement.

ARTICLE A 02

Nouveaux usages, nouvelles technologies : quels défis en matière de sécurité ?

Intervenants :
Madame Sylvaine LUCKX, journaliste chez Mag Securs
Monsieur Serge RICHARD, security Intelligence channel technical leader, IBM Europe
Monsieur Mahmoud DENFER, RSSI chez Valourec
Monsieur Christophe AUBERGER, directeur technique chez Fortinet-France
Monsieur François CHASSERY, directeur commercial et marketing d'une filiale de la poste
Monsieur Olivier DESBIEZ, pôle prospective de la CNIL

Résumé des interventions :
L'explosion du nombre d'objets connectables, et pour la plupart connectés, pose de nouveaux problèmes de sécurité. Tous ces objets connectés alimentent les « Big Data » et la question de la sécurisation de ces objets est passée en revue à travers les prismes des entreprises mais aussi de la CNIL avec une focale sur l'utilisateur final dont les données peuvent être utilisées avec malveillance.

I - Des objets connectés par milliards générant une masse de données considérable.
Aujourd'hui, 12 milliards d'objets sont connectés sur la planète. A l'horizon 2020, des projections raisonnables avancent le nombre de 50 milliards d'objets connectés. A cet égard, il convient de distinguer plusieurs types d'objets connectés : les objets portés sur le corps par leurs utilisateurs (capteurs en tous genres), les objets connectés dans les habitations (domotique) et enfin tous les objets connectés liés au monde du travail (notamment les BYOD). Ils génèrent un volume de données incomparable qui alimente les « Big Data ».
Malgré leur nombre croissant, les objets connectables ne sont pas forcément tous connectés. Néanmoins, la masse de données croît de façon exponentielle et ces données sont parfois très personnelles.

II - Les nouveaux usages induisent de nouvelles menaces…
De facto, la question de l'usage de ces données est posée et est interprétée différemment par les créateurs, les consommateurs et les

instances de régulations comme la CNIL en France.
Tous les acteurs s'accordent à préciser que la menace est constituée principalement par le détournement de finalité. En effet, les données captées, envoyées sur des serveurs, traitées par les créateurs d'objets connectés et remises à disposition du client ne sont pas réellement sécurisées. A titre d'exemple, un sportif appliqué et connecté court un risque. En effet, les objets qui captent ses bio-data durant sa séance et lors de son sommeil afin de lui permettre d'évaluer ses performances et de les améliorer tant dans l'activité que pendant la récupération physiologique demeurent connectés. Ses données peuvent être captées à d'autres fins : quid d'une société d'assurance indélicate qui ferait capter et utiliserait les données du sportif afin d'optimiser les contrats ? Naturellement les sons captés depuis une chambre à coucher peuvent aussi devenir des leviers d'atteinte à la vie privée. A travers cet exemple qui met en scène des données quasi biomédicales, et qui peut se décliner sur toutes les habitudes « connectées », le risque d'interception et d'usage malveillant des données est irrémédiablement en augmentation. Une intrusion massive sur les habitudes de vie et sur la vie privée est théoriquement possible.

Si l'utilisateur contrôle localement les objets connectables, celui ou ceux qui maîtrisent les informations une fois qu'elles sont délocalisées ne sont pas clairement identifiables et encore moins systématiquement bienveillants.

III - … qui nécessitent de sécuriser physiquement les données plus que les « devices » mais aussi de créer de nouvelles certifications et de nouveaux réflexes.

La prise de conscience par les utilisateurs de la circulation de leurs données personnelles doit les inciter à exiger une véritable sécurisation de leurs données.
Ainsi la donnée devient le point clé qu'il convient de sécuriser avant tout. Celle-ci traverse trop d'étapes par essence incontrôlables. Une prise de conscience des utilisateurs est nécessaire. A cet égard, les entreprises qui signent une charte se positionnent d'ores et déjà comme les précurseurs en matière de protection de la vie privée. Néanmoins, il convient d'associer la parole aux actes. En France, la CNIL a d'emblée mis en œuvre un pôle « prospective » qui s'intéresse aux objets connectés. La CNIL propose des analyses de facteurs de risques. Ces outils d'identification de risques sont disponibles pour les particuliers comme les entreprises. L'objectif est de sensibiliser les utilisateurs mais aussi les entreprises aux phénomènes d'usurpation d'identité et de détournement de finalité mais aussi de présenter les conséquences d'une connexion sur internet. Enfin, l'arrivée massive du phénomène de BYOD qui consiste à utiliser à des fins professionnelles ces objets connectés personnels pose un problème de sécurité des données privées comme la géolocalisation de l'employé par l'employeur. La notion de « privacy » doit désormais être incluse dans l'architecture des SIC d'une entreprise pour faire face à l'arrivée massive de ces objets.
Dans ce contexte, il convient de préciser que les objets connectés n'ont pas été conçus pour être « sécurisés » c'est-à-dire qu'ils n'ont pas été pensés pour évoluer en environnement hostile. C'est une des raisons pour laquelle c'est bien la donnée qui transite qui doit être sécurisée.

ARTICLE A 03

Pirater le protocole sans fil de l'internet des objets à l'aide des outils de radio logicielle

Intervenants :
Général d'Armée (2S) Marc WATIN-AUGOUARD, Directeur du centre de recherche de l'École des officiers de la gendarmerie nationale.
Monsieur Sylvain FIEVET, président de Pour action.
Monsieur Jean-Fabrice LEBRATY, professeur des universités, Lyon III.

Résumé des interventions :
L'Agora s'est articulée autour de quatre séquences afin de faire émerger les caractéristiques des métiers du cyber, ceux d'aujourd'hui et ceux de demain. Il s'est agi d'emblée d'aborder la notion d'expertise dans le domaine de la cybersécurité pour révéler que l'ensemble de la société est concerné. Il existe quelques leviers qui peuvent permettre le développement des métiers de la cybersécurité. Celui des ressources humaines est à considérer tout particulièrement. Enfin, les réflexions sur la gouvernance et l'attractivité ont permis de mettre en évidence une approche territoriale et la notion de management du risque, lequel peut être pour partie externalisé.

I – La cybersécurité, une affaire de spécialistes ou une question de société ?

La cybersécurité présente certes des aspects extrêmement techniques mais la part de l'humain est fondamentale. L'individu n'est pas une variable parmi d'autres, c'est en fait LA variable de la cybersécurité. En effet, il existe une foule d'agresseurs et les experts, aussi nombreux soient-ils, ne suffisent pas. La diversité des domaines en cybersécurité est très large et les coûts de formation des experts sont très importants. Aussi, pour faire face à la multiplicité des agresseurs, est-il nécessaire de former un grands nombre de personnes . Cela passe donc par la formation et la sensibilisation dès le plus jeune âge.

Il s'agit également de développer de nouvelles compétences. Elles sont nombreuses et difficiles à dé-

finir, il n'existe pas de liste exhaustive. Ces compétences s'exercent dans trois domaines : économique, sociale et juridique. Les nouveaux métiers sont là, notamment ceux de l'influence et de la contre-propagande. La sécurité est globale, il faut donc des compétences globales.

II – Quels leviers pour le développement de la cybersécurité ?

La réflexion a porté, à la fois, sur les normes et sur la peur.

La question de la nécessité des normes se pose. En effet, elles peuvent contraindre le développeur et l'utilisateur dans son quotidien. Elles peuvent être des freins au développement et à la liberté. Mais la mise en place de normes est aussi une chance pour une entreprise. La norme ou l'exigence de la norme peut être une garantie de qualité. Cette qualité est un ingrédient de la compétitivité. La norme peut donc être un avantage compétitif visible. Face à la norme apparaît en effet la notion de responsabilité, qui si elle est mise en cause, notamment d'un point de vue juridique, peut coûter cher au décideur. C'est donc la peur du poids de la responsabilité qui peut être un levier.

La notion de peur a mis en évidence des divergences. D'un point de vue individuel, il semble manifeste que la peur en matière de cybersécurité peut avoir un rôle bénéfique. Elle va inciter l'utilisateur à plus de prudence dans ses comportements et à faire preuve de vigilance. En revanche, au niveau de l'organisation de l'entreprise, cette peur ne semble pas être un levier performant. C'est peut être plus la contrainte, c'est-à-dire la norme, que la peur qui incitera le décideur à passer à l'action en matière de cybersécurité.

Il existe d'autres leviers qui tiennent au fait que les entreprises sont plurielles et présentent des différences majeures en matière de sécurité. Les cultures d'entreprises sont différentes et les priorités également.

III – Quelle adéquation entre la demande et l'offre ?

Il existe un consensus sur le fait qu'il y a inadéquation entre l'offre et la demande en matière de cybersécurité. Il semble manifeste que les vocations cyber sont peu nombreuses chez les jeunes. Il y a un décalage de langage entre le recruteur et le recruté. Certaines offres d'emploi, manquent de clarté. Cette situation explique que les emplois ne sont pas tous pourvus. La filière de ces métiers de la cybersécurité a un besoin impératif de visibilité et de lisibilité.

Quelles sont les solutions ? Il faut probablement aller vers de nouvelles formes de recrutement. Le diplôme n'est peut être pas l'élément essentiel, il faut avant tout des savoir- faire. Cela peut passer également par une forme plus institutionnelle au travers du registre national des emplois. A un métier correspond aujourd'hui nécessairement un référentiel de compétences.

IV – La gouvernance de la cybersécurité et les territoires.

La gouvernance fait appel à de multiples compétences. Elles sont en pleine évolution. Il suffit de prendre des fonctions techniques qui sont en lien avec les fonctions de direction. La gouvernance s'appuie sur le fait de rendre le risque visible. La gouvernance repose aussi sur un langage commun entre technicien et direction. On assiste donc à la mise en place d'une coordination entre techniciens et direction, sous forme d'équipe. On peut évoquer ici l'externalisation, sous réserve de conserver des fonctions souveraines au sein de l'entreprise. Il faut être conscient que toute externalisation n'exonère par un directeur d'entreprise de considérer l'ensemble des risques. Il n'y a pas d'externalisation de la responsabilité.

La gouvernance, ce sont aussi les territoires. Les acteurs sont multiples et ces acteurs doivent être cohérents entre eux pour aller dans le sens d'une cybersécurité efficace. A côté du monde de l'entreprise, il faut considérer les

collectivités territoriales et les établissements publics. Cela implique un certain décloisonnement entre monde privé et monde public mais également entre monde urbain et monde rural. Les collectivités territoriales pourraient jouer le rôle de catalyseur afin de répondre au défi de la cybersécurité.

Conclusion

La cybersécurité sera assurée si l'action se fait au niveau organisationnel en mettant en place des normes mais également au niveau individuel dès le plus jeune âge. Il s'agira également de mener des actions au niveau des territoires. Enfin actuellement, il faut reconnaître que l'on agit plutôt sur un mode défensif. Il semble indispensable de considérer un mode offensif mais également une démarche proactive pour avoir toujours un temps d'avance sur l'adversaire.


NISTÈRE DE L'INTÉRIEUR
MINALITE
S'ENGAGER A L'INTERNATIONAL

ARTICLE A 04

Simulation stratégique exécutive

Intervenants :
- Cyril AUTANT, Directeur de la sécurité des systèmes spatiaux et systèmes d'information – THALES Communications & Security
- Paul THERON, Expert en Cyber – THALES Communications & Security
- Didier VIRLOGEUX, Responsable Marketing - THALES

Résumé des interventions :
Les cybermenaces évoluent en complexité, pouvant prendre la forme, pour ceux qui en ont les moyens, d'attaques dites « en profondeur ». La particularité de ces attaques réside dans le fait qu'elles font l'objet d'une conception systémique. Tout l'enjeu de l'attaqué sera alors de les détecter au plus tôt pour garder la maîtrise de la situation. Pour en prendre conscience, un serious game est proposé aux participants. Il met en scène une attaque en profondeur sous la forme d'un jeu interactif visant à sensibiliser les joueurs à la gestion de ce nouveau genre de menace numérique.

I – Une complexification de la menace numérique:

La cybermenace a fortement évolué : virus, vers, botnets, sniffers, DDOS ciblés, APT, profilage social sur les réseaux, command & control, agents intelligents autonomes, etc. Aujourd'hui la menace est plus complexe car non seulement la nature des attaques a changé, mais aussi la façon dont les agresseurs s'y prennent. Pour l'attaqué, elles deviennent plus complexes à identifier et à contrer.

Les attaquants et les attaqués peuvent être multiples, avec des objectifs différents pour les attaquants, et des impacts inégaux pour les attaqués. Plusieurs de ces attaquants peuvent s'associer pour mener une attaque globale.

Il existe 3 grandes classes d'attaque :
- Les attaques de cybercriminalité (Sony Pictures en novembre 2014, Adobe, Ebay, Webmails, etc.) sont

des attaques d'ampleur à visée mercantile, qui touchent plusieurs millions d'utilisateurs ou de clients.
- Les attaques visant le renseignement (Lockheed Martin depuis 2009, Services de l'Elysée en 2012, Affaire Snowden en 2013…) sont des attaques furtives ayant des effets à long terme. Pour l'attaqué, l'impact est lourd en termes d'image ou de positionnement concurrentiel.
- Les attaques destructrices (STUXNET en 2010, Oléoduc de Bakou-Tbilisi-Ceyhan en Turquie 2008, menaces sur le contrôle du trafic aérien…) sont encore peu nombreuses. Elles visent notamment les systèmes industriels pouvant déstabiliser une organisation ou un État. La sûreté est un élément fondamental de leur prévention.

Une attaque dite « en profondeur » s'insère dans une réflexion stratégique, pilotée par l'effet final recherché. Cette stratégie va viser des composants différents au sein d'une organisation, ou s'attaquer à plusieurs niveaux, et l'ensemble donnera lieu à une attaque assez complexe, difficile à déchiffrer pour l'attaqué. Ce genre d'attaque nécessite des moyens humains et des ressources techniques importants. L'attaquant peut induire sa cible en erreur, en jouant des coups tactiques qui, en apparence, n'ont aucun lien entre eux et induisent de la confusion quant aux objectifs réels de l'attaque. Il s'agit d'empêcher la cible d'avoir une vision globale de la stratégie et de l'objectif final de l'attaquant. C'est pourquoi il est essentiel de détecter très rapidement une attaque. La vitesse de réaction conditionne la vision globale qu'il sera possible d'avoir et permet d'enclencher sans délai les réactions adéquates. Il faut, dans la mesure du possible, éviter de se retrouver en situation de crise car cela devient vite très compliqué à gérer.

II- Une riposte qui se veut d'inspiration militaire

Pour comprendre cette notion d'attaque en profondeur, THALES a mis au point un jeu interactif qui combine la vision de l'attaqué et celle de l'attaquant. Ce serious game place le joueur dans le peau du directeur général d'une entreprise pétrolière, pilier de l'économie nationale, dans un pays imaginaire considéré comme le 2ème producteur de pétrole du monde. Le contexte est celui d'un appel d'offres lancé par la compagnie nationale d'un pays tiers dans le but de trouver des partenaires industriels capable de les aider à mettre en œuvre les process, l'exploitation et la distribution des ressources nationales de pétrole, un gisement d'hydrocarbures ayant été récemment découvert à la faveur d'une campagne de forages d'exploration. Le délai de réponse à l'appel

Glossaire :

DDOS : distributed denial-of-service, attaque en déni de service menée au moyen de multiples machines robots (botnet) qui saturent un ou plusieurs serveurs en vue de rendre le service visé inaccessible.
APT : Advanced Persistent Threat est un type d'attaques complexes combinant souvent différents vecteurs et stratégies d'attaques, pouvant utiliser des techniques inconnues ou des failles zero day, durant assez longtemps sans être détectées, et la plupart du temps ciblées.

d'offres est fixé à 9 mois, et plusieurs opérateurs vont y répondre. Si l'entreprise du joueur est retenue, elle deviendrait alors la première entreprise pétrolière au monde, mais celle-ci fait alors l'objetd'une attaque dite en profondeur...

Au fil du jeu présenté, le terme de guerre numérique commence à prendre tout son sens. Il en ressort que si l'attaquant a un temps d'avance et la maîtrise de l'initiative, l'attaqué se trouve vite démuni, à tel point que les contre-mesures prises dans l'urgence ne font que permettre à l'attaquant de récupérer davantage d'informations. En effet, alors que l'attaquant enchaîne les coups tactiques - à priori sans lien les uns avec les autres - pour déployer sa stratégie selon l'effet majeur recherché, l'attaqué, lui, joue à l'aveugle sur l'échiquier numérique. D'où l'absolue nécessité de préparer, hors temps de crise, une batterie de réactions de sauvegarde de nature technique et comportementale. L'analyse de risques ne suffit pas. Il faut connaître sa capacité de résistance face au risque cyber et développer des réflexes de défense. L'objectif est de réagir dès que la première attaque est détectée, même si elle apparaît anodine ou isolée.

ARTICLE A 05

Pirater le protocole sans fil de l'internet des objets à l'aide des outils de radio logicielle

Intervenants :
- Yann ALLAIN, Opale Security, OCE
- Julien MOINARD, Opale Security, Ingénieur électronique

Résumé des interventions :
L'explosion du nombre d'objets connectables, et pour la plupart connectés, pose de nouveaux problèmes de sécurité. Tous ces objets connectés alimentent les « Big Data » et la question de la sécurisation de ces objets est passée en revue à travers les prismes des entreprises mais aussi de la CNIL avec une focale sur l'utilisateur final dont les données peuvent être utilisées avec malveillance.

I – Données, mobilité et radiofréquences

Les besoins croissants en communication et en mobilité entraînent logiquement une progression rapide des technologies sans fil et radiofréquence (RF). Que les distances soient limitées (Bluetooth, Zigbee, etc.) ou plus grandes (GSM, Wi-Fi), des protocoles RF existent et sont massivement utilisés. Ils exposent donc les équipements intégrés ou l'internet des objets à des nouvelles attaques provenant de systèmes utilisant les radiofréquences, que les pirates ne se privent pas d'utiliser.

La conséquence logique est l'apparition d'outils dédiés visant à aider les auditeurs de sécurité à évaluer la communication sans fil. Malgré ces outils, ceux-ci et les testeurs d'intrusion doivent pénétrer dans les arcanes du traitement des signaux RF. Ces procédés nécessitent une grande culture électronique (qui est souvent négligée).

Les outils de radio logicielle permettent de découvrir ce domaine d'une manière intéressante et ludique.

La plupart des protocoles sans fil sont mis en œuvre par les équipements qui utilisent des appareils in-

tégrés et par les systèmes numériques de commande, les instruments et les appareils de supervision. En matière d'outils et de méthodologie d'audit des protocoles sans fil, l'approche la plus pédagogique consiste à réaliser un pentest. Les outils de radio logicielle comme HAckRF One ou la carte USRP permettent de continuer à évoluer dans ce domaine d'audit, à moindre coût, en utilisant un récepteur pour la TNT dont le prix est de 10$. Aujourd'hui, les communications radios sont réalisées « sans fils », par le biais des radiofréquences, lesquelles sont des ondes électromagnétiques. Réaliser un audit de sécurité des protocoles implique par conséquent une analyse des ondes magnétiques. Il est avant tout nécessaire de pouvoir les détecter pour pouvoir les analyser afin de retrouver les données transmises. Dans certains cas, il convient de pouvoir les modifier pour être en mesure de les retransmettre.

II – Réalisation du pentest

Pour réaliser ce pentest, il faut adopter une méthodologie décrite durant cette master-class. Avant tout, le signal radio-fréquence doit être capté. Pour cela l'utilisation d'un outil de type Software Defined Radio (SDR) couplé à un hardware permet de trouver et de capturer la transmission par radiofréquence. Cela permet d'abord d'acquérir les données brutes pour ensuite les analyser ultérieurement. Le signal peut être capté avec un receveur TNT, des antennes mais aussi du matériel hardware plus sophistiqué allant de 300 à 3000 $. Les outils comme GNU Radi sont en open source, gratuits, puissants, donc fort utiles.

L'analyse du spectre de fréquence permet ensuite de déterminer la communication radiofréquence, l'utilisation de techniques d'étalement du spectre1 (FHSS, DSSS...) ou la détection des porteuses. Elle se réalise au moyen des « blocks » GNU Radio, outils d'analyse du spectre fréquentiel.

Puis, afin de démoduler le signal, et à l'aide du « block diagram » de GNU Radio, il faut trouver comment les données sont modulées dans le signal radiofréquence (modulation= encodage physique pour le transport de l'information).

L'étape suivante consiste à transformer le « Bitstream » radiofréquence en paquets de données (décodage). Cette étape de l'audit de flux est sans doute la plus difficile puisque les problématiques sont proches du « reverse engineering2 ».

Il est enfin possible d'analyser les données et surtout les faiblesses protocolaires éventuelles. Cette étape plus classique permet de détecter les points faibles de la confidentialité (chiffrement ou non), de mener des attaques par rejeux3, de contourner les dispositifs d'authentification/identification et ainsi d'atteindre la disponibilité (brouillage des ondes).

A l'issue de cette « master-class », les auditeurs pourront commencer à évaluer seuls les lignes directrices, les méthodes et les références d'audits pour évaluer la plupart des protocoles sans fil utilisés par des appareils intégrés.

ARTICLE 06

Les alliances sont-elles possibles dans le cyberespace ?

Intervenants :
- Nicolas ARPAGIAN, rédacteur en chef de la revue « Prospective Stratégique » et directeur scientifique Sécurité numérique à l'INHESJ ;
- Jamie SHEA, Secrétaire général adjoint délégué pour les défis de sécurité émergents au Quartier général de l'OTAN ;
- Noboru NAKATANI, Executive Director, INTERPOL Global Complex for Innovation ;
- Frédérick DOUZET, Professeur des universités, Chaire Castex de cyberstratégie ;
- Julien NOCETTI, Chercheur à l' IFRI (Institut Français des Relations Internationales) ;
- Olivier KEMPF, chercheur associé IRIS.

Résumé des interventions :
Bien que conçu dès l'origine comme un espace transnational, le cyberespace se voit aujourd'hui investi par les Etats et est perçu comme un nouveau champ d'expression de la puissance. Les Etats façonnent donc des stratégies d'action variées (défensives ou offensives, économiques, technologiques, juridiques...) et déploient désormais une diplomatie ad hoc. Mais la nature même du cyberespace, qui favorise les affrontements clandestins et touche à des domaines sensibles, restreint les zones de coopération potentielle. Au delà de la zone de souveraineté, des alliances sont-elles donc possibles dans le cyberespace ? Une sécurité collective est-elle envisageable ? Peut-on imaginer autre chose que des affrontements et des alliances ponctuelles ? Quelles sont les organisations mises en place aux plans stratégique, opératif et tactique ?

I - Particularité du cyberespace : un nouveau défi posé par un rapport de forces non observable

Les activités liées au cyberespace posent un défi nouveau dans le sens où elles ne se heurtent à aucune frontière géographique et dépassent les institutions, les Etats, les organisations telles que l'OTAN, par exemple. Cette dernière organisation se doit d'établir aujourd'hui de nouvelles règles du jeu en matière de coopération avec les Etats non-membres afin de maintenir une cybersécurité réelle et efficace. Le nouveau terrain d'affrontement que représente le cyberespace donne effectivement lieu à une redéfinition de l'ennemi, de l'arme utilisée, de son impact potentiel et des calculs stratégiques pour tenter de lutter contre cette menace. Des actions sont possibles

dans le cyberespace sans que l'on sache réellement qui en sont les auteurs, voire même quelle cibles sont visées. Cette question de la paternité des attaques s'est posée récemment dans l'affaire Sony Pictures Entertainment. Elle a démontré qu'en l'absence de preuve technique et du fait de l'opacité du Web, il est difficile d'identifier, avec certitude, l'origine des cyberattaques.

L'ennemi est devenu physiquement inaccessible mais aussi de plus en plus expert. Sa nocivité est difficilement mesurable. Cette menace globale, dont la diffusion peut être très rapide et l'impact potentiel massif, exige de faire évoluer rapidement les méthodes d'enquête et d'identification des criminels et de se doter de compétences pointues dans ce domaine. Cela nécessite aussi de mettre en place un très haut niveau de coopération entre les agences au sein des gouvernements, entre les Etats, au sein d'organisation internationales et entre secteur public et secteur privé. Afin de mutualiser les savoir-faire et les compétences spécialisées. Interpol a, par exemple, créé à Singapour l'IGCI, centre d'excellence de lutte contre la cybercriminalité, qui sera pleinement opérationnel en avril 2015. Cette organisation associe tout un panel d'experts issus de milieux divers (universités, sécurité publique et privée, sociétés de développement de logiciels de sécurité Internet). L'OCS, quant à elle, regroupe six pays dont la Chine et la Russie et organise depuis juin 2001, date de sa création, des échanges très réguliers sur des problématiques de cybersécurité, d'extrémisme et de terrorisme. Enfin, on peut citer la prompte réaction des Etats-Unis après l'affaire Snowden et le rapport du CFR (Council on Foreign Relations) de juin 2013 dans lequel sont suggérées à la fois une redéfinition des alliances orientées vers les grands pays émergents et une véritable diplomatie numérique.

II - Tensions contradictoires liées à la représentation de la cybermenace

La gouvernance du cyberespace, polarisation universelle et défi commun, fait paradoxalement naître des tensions entre les Etats. En effet, même si la construction d'alliances et le partage d'informations semblent les seuls moyens de lutter efficacement contre cette « pandémie », les capacités cyber représentent indéniablement un outil au service de la puissance des nations, un instrument de regain de souveraineté. Elles font pleinement partie de l'arsenal moderne à développer, mais que l'on est peu enclin à partager, pour la sécurité de la nation. Cette dynamique inverse pousse alors au repli souverain et à la fortification des systèmes à l'échelle nationale. L'échange trop poussé d'informations et de moyens peut effectivement conduire à la perte de la valeur opérationnelle et économique des outils partagés. Par conséquent, cette rivalité de pouvoirs géopolitique peut réduire la coopération multilatérale à un niveau minimal de partage : échange de bonnes pratiques, formation et exercices d'entraînement entre Etats... Cette coopération « en surface » repose, encore actuellement, sur le principe du donnant-donnant, sur une optimisation de l'analyse coût/bénéfices. Il en résulte que les Etats les plus avancés en matière de cybersécurité n'ont pas intérêt à partager leurs outils et leur expertise avec les plus faibles. Ces derniers, faisant confiance aux plus avancés, pourraient juste bénéficier de leur efforts, sans investissement propre. A ce titre, les alliances bilatérales semblent plus aisées que les alliances multilatérales.

III - Vers une coopération efficiente et approfondie : un diagnostic de gouvernance s'impose

Afin de générer un climat de confiance mutuelle et de faciliter les échanges de renseignements, il semble alors impératif de procéder à une « égalisation de ter-

rain » si les données échangées sont des informations sensibles et stratégiques. Ceci suppose d'aligner les efforts de chaque allié, de se mettre d'accord sur les normes de comportement responsable et sur les modalités d'application du droit international concernant les pratiques acceptables dans le cyberespace. Sur le plan international, il s'agit donc de savoir exactement à quoi les Etats sont prêts à renoncer pour développer une coopération efficace en matière de cybersécurité et de montrer que chacun d'eux est prêt à porter assistance à l'autre en situation de crise.

S'agissant de partenariats possibles avec le secteur privé, la manœuvre est d'autant plus délicate qu'elle demande, elle aussi, une certaine prudence dans l'approche. Partager des données sensibles voire embarrassantes avec le gouvernement peut non seulement révéler la vulnérabilité du partenaire privé mais aussi accroître les attentes de celui-ci en matière de protection et d'information.

Par ailleurs, mettre en place une réelle collaboration exige que chaque partie prévoit l'existence d'une structure dédiée à la gestion du cyberespace avec une réelle stratégie de défense. Celle-ci peut être une création ad hoc ou simplement l'adaptation d'une structure préexistante. L'identification précise de l'interlocuteur cyber de chaque partie (ministère, organisme, service...) est notamment essentielle à la bonne coopération Une harmonisation des gestionnaires nationaux du cyberespace semble également un pré-requis d'importance.

Glossaire & Liens :

IGCI : INTERPOL Global Complex for Innovation - (http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation)
OCS : Organisation de Coopération de Shangaï.
CFR : Council on Foreign Relations - http://www.cfr.org/

ARTICLE A 07

L'offre française répond-elle aux besoins actuels des SOC et CERT ?

Résumé des interventions :
Les structures de veille et de réponse opérationnelle relatives à la sécurité des systèmes d'information existent à différents niveaux et aussi bien dans le monde privé que dans le secteur public. Ces centres ont une fonction essentielle et doivent, pour remplir pleinement leur office, développer des partenariats et des réseaux d'échange d'information.

SOC, CERT : la vision de l'État et de l'entreprise

Le SOC du ministère de la Défense est une entité d'une trentaine de personnes travaillant sous le pilotage du CALID (centre d'analyse en lutte informatique défensive). Il a une fonction de supervision et une mission d'appui au commandement. Il travaille au profit de l'ensemble du ministère.

Le SOC, pour une entreprise, a une mission de pilotage et se positionne en appui à la décision. C'est une structure qui va délivrer une prestation de détection d'incident de sécurité. Il s'agit d'un superviseur de sécurité.

Le CERT est quant à lui un appui au SOC. Il remplit également, en quelque sorte, un rôle de pompier. Il procède à la veille interne et externe et noue pour y parvenir les contacts nécessaires avec les structures extérieures susceptibles d'échanger utilement avec lui.

Les conditions d'une bonne coopération

Le ministère de la Défense s'est rapproché d'autres organismes étatiques. Par ailleurs, un groupe comprenant les différents SOC des services de l'Etat se réunit tous les 3 mois. Il existe donc, au niveau gouvernemental, des structures

Intervenants :
Patrick BREHIN, Responsable du CERT, AREVA.
Thomas GIRARD, directeur de la BU défense-sécurité et du département SSI, C-S.
Mathieu HELSIEN, bureau politique inductrielle et assistance, ANSSI.
Raphael MARICHEZ, fonctionnaire de SSI, Ministère de l'intérieur.
Ludovic RAVAUX, officier adjoint au SOC, Ministère de la défense

d'échange qui marchent bien.
Pour les entreprises, l'échange de marqueurs, non connus de l'attaquant, pose le problème d'équilibre de concurrence avec les industriels. Dans un monde des affaires toujours plus compétitif et reposant en grande partie sur la confiance des clients, la confidentialité est un point majeur. Échanger un marqueur signifie évoquer sans détour le fait que l'entreprise a subi une attaque. La confiance est donc absolument nécessaire mais elle reste difficile à mettre en œuvre. Les étapes d'une coopération menée avec intelligence et ayant de bonnes chances d'aboutir seraient les suivantes :
Étape 1 : créer les SOC
Étape 2 : établir des contacts entre eux pour les amener à se connaître et à identifier les modalités d'échanges opérationnels.
Étape 3 : échanger des éléments sensibles.

Qu'est ce qu'un SOC qui fonctionne ?

Les structures de gestion de sécurité des systèmes d'information ont principalement pour mission de présenter au décideur les domaines à améliorer. Elles doivent en quelque sorte dresser un état de la menace et identifier les actions susceptibles d'avoir une efficacité maximale pour y faire face. Il s'agit de montrer au décideur quels leviers ont, pour un coût minimum, le plus d'impact positif sur la résistance et la résilience de l'entreprise.
Le SOC ne doit pas être un organe isolé dans l'entreprise. Il doit être connu des dirigeants, lesquels doivent être pleinement associés à son fonctionnement et aux résultats qu'il obtient en matière de protection des systèmes d'information.
Il doit identifier, à tous les niveaux de l'entreprise, les points de supervision mais aussi les anomalies dans le mode de fonctionnement afin de proposer aux dirigeants les mesures correctives nécessaires.
L'ANSSI a créé, à destination des entreprises, un référentiel pour la construction d'un système de détection rationnel selon les besoins et les budgets. Il s'agit d'un outil à la disposition, notamment, des SOC et des responsables SSI.
Le SOC, en prévision d'une attaque, identifie les responsables des différents services potentiellement concernés. Cette liste est maintenue à jour et portée à la connaissance de la direction pour être validée. Il s'agit pour l'entreprise de bien connaître les domaines d'action des différents responsables de façon à éviter la dispersion de la réponse et des pertes de temps en recherche de la personne à prévenir. Il est très utile de définir à l'avance les procédures de réaction et de s'assurer qu'elles sont bien connues et maîtrisées par celles et ceux chargés de les mettre en œuvre. Là encore, ces procédures ainsi que les personnes responsables de leur gestion font l'objet d'une approbation par la direction de l'entreprise.

Glossaire :

SOC : Security Operating system, centre de gestion de sécurité des systèmes d'information.
CERT : Computer Emergency Response Team, centre d'alerte et de réaction aux attaques informatiques.

ARTICLE A 08

[Réunion des clubs R2GS européens] – Vers une approche européenne en matière de SIEM ?

Résumé des interventions :
Les solutions SIEM ont été élaborées pour faire face à l'augmentation des menaces pesant sur les données des entreprises. Les clubs R2GS cherchent à améliorer leur efficacité afin de sécuriser au mieux les informations. Compte-tenu des bénéfices apportés par les SIEM aux entreprises, l'idée d'élaborer un standard européen semble désormais s'imposer. En effet, les initiatives nationales montrent leurs failles, failles qu'un partage des bonnes pratiques à l'échelle européenne, dans un premier temps, pourrait combler.

La gestion des incidents de sécurité est devenue un enjeu majeur pour de nombreuses entreprises. L'information, publique ou privée, est désormais une ressource essentielle. Afin de lutter contre les menaces pesant sur leurs données, les entreprises se reposent de plus en plus sur les solutions SIEM (Security Information and Event Management), de gestion des informations et événements de sécurité. Ces solutions sont très utiles pour détecter les menaces, élaborer une réponse aux incidents et répondre à la conformité des standards de sécurité.

Le SIEM est donc un système de supervision centralisé de la sécurité se décomposant en deux solutions : le SIM (Security Incident Management), basé sur l'analyse a posteriori, l'archivage, la conformité et le reporting ; et le SEM (Security Event Management), collectant et traitant les données en temps réel.

Le R2GS, en tant qu'association regroupant des experts de l'IT (In-

Intervenants :
- Ulrich SELDESLACHTS, Chairman and coordination of European community, Club R2GS Belgium
- Gérard GAUDIN, Chairman and coordination of European community, Club R2GS France
- Jan DE MEER, Chairman and coordination of European community, Club R2GS Germany
- Alberto MANFREDI, Chairman and coordination of European community, Club R2GS Italy
- Christophe BIANCO, Chairman and coordination of European community, Club R2GS Luxembourg
- Fortune BARNARD, Chairman and coordination of European community, Club R2GS UK.

formation Technology), travaille sur cette solution.

Les activités du R2GS et les SIEM

L'association a constitué en Europe un réseau œuvrant pour la cyberdéfense, la cybersécurité et les SIEM. Apparu en 2009, le R2GS français collabore avec l'Agence Française de Sécurité, travaille pour les ministères de l'Intérieur et de la Défense et entretient des liens forts avec la Commission européenne. En 2012, l'association s'est étendue à l'échelle européenne pour être aujourd'hui présente dans six pays. Son objectif est de mettre en commun les expériences et intelligences en vue de mieux identifier les incidents et d'organiser la réponse la plus efficace possible.

En effet, les attaques informatiques se sont multipliées depuis plusieurs dizaines d'années et se sont complexifiées. Face à cela, les SIEM sont présentés comme la réponse au besoin de sécurisation des informations.

Le modèle SIEM recouvre plusieurs fonctions : la collecte des événements, leur normalisation (de par la conservation des logs), le stockage et l'archivage de ces événements, la mise en corrélation des informations recueillies et le reporting consistant à générer des tableaux de bord permettant un suivi de la sécurité du système d'information. Pour autant, le SIEM demeure un outil de détection de menaces ou d'anomalies mais pas de blocage. Le R2GS s'intéresse au développement des indicateurs opérationnels permettant des analyses comparatives.

Évaluation de la situation de la solution SIEM

Le SIEM apporte un important bénéfice aux entreprises en surveillant les événements de sécurité de l'information pour permettre la mise en œuvre d'un processus de réponse adaptée mais également en mettant en relief les manquements des contrôles de sécurité jusqu'alors instaurés.

La réflexion du R2GS se base sur le modèle « hype cycle » développé par le groupe Gartner. Ce modèle, très pertinent, offre une approche réaliste de la situation des SIEM ainsi que des perspectives d'amélioration de l'efficacité de ces solutions de sécurité.

Contrairement à ce qui se faisait il y a une dizaine d'années, il ne suffit plus d'opter pour une vision uniquement technique. Il convient d'établir une position optimale entre la prévention, la détection et le moment de la réaction en définissant clairement les objectifs de contrôle ainsi que les standards, les modèles de référencement à adopter.

La clef de l'évolution des SIEM tient en la communication qui permet une approche organisée. Les différentes associations R2GS en Europe s'accordent à dire que les efforts doivent être axés sur la phase d'agrégation, consistant à regrouper les événements de sécurité selon certains critères, et la phase de corrélation, visant à établir des relations entre ces événements en vue de créer des alertes. C'est pourquoi un modèle de référencement des différents indicateurs a été établi. Il recense les indicateurs les plus opérationnels. Sur ce point, le R2GS a démontré la pertinence d'une approche statistique. Il est donc essentiel de mobiliser l'ensemble des entreprises.

Ces évolutions, souvent issues d'un concert européen, permettent de simplifier la configuration et d'offrir une vision globale au manager. Elles contribuent également à la cohérence des alertes et des décisions. Mais, afin de rendre cette approche plus visible, il devient indispensable d'adopter une vision européenne, voire internationale. De telles mises en commun contribueraient à adapter au mieux le niveau de détection et permettraient aux entreprises d'effectuer des analyses comparatives des postures de sécurité, le tout en cherchant à améliorer la sécurité des IT.

La volonté d'établissement d'un standard européen

L'important est de développer la

coopération entre États. L'observation du modèle « hype cycle » permet de détecter ce qui ne l'était pas auparavant. C'est pourquoi il convient de maximiser la visibilité des sources de données événementielles. De plus, le stockage des données de logs étant un des éléments critiques de toute solution SIEM, les entreprises doivent veiller à choisir une solution cohérente avec le cycle de vie des données. Enfin, et avant toute chose, il convient de rationaliser, d'évaluer les différents coûts et les répercussions à venir du choix d'une solution. Le partage de la détection des incidents est devenu essentiel. Une visée de la cybersécurité européenne serait alors un des meilleurs outil en la matière. Cet objectif nécessite l'implication de toute la communauté afin d'envisager une standardisation à grande échelle du développement des solutions SIEM. Il s'agit là de l'avenir de la lutte contre la vulnérabilité des informations. Ce sont ces initiatives communes, le partage des bonnes pratiques, qui vont notamment permettre de faire évoluer les comportements, d'où l'idée d'élaborer une plate-forme européenne de détection des incidents. Les États pourraient y référencer, en toute confiance, les pratiques qui fonctionnent et celles pour lesquelles ce n'est pas le cas afin d'évaluer l'efficacité des technologies.

Il faut donc aujourd'hui dépasser la seule dimension nationale de la réflexion.

Conclusion :

L'idée d'instaurer un standard européen se révèle très intéressante. Il conviendrait alors de parvenir à insérer les réflexions entourant les solutions SIEM à la plateforme NIS (Network and Information Security), notamment en vue du projet Horizon 2020. Le club R2GS œuvre à cette fin. La diffusion des bonnes pratiques tend à s'imposer comme le nouveau mot d'ordre.

ARTICLE A 09

La cybersécurité dans le domaine maritime

Intervenants :
- Henri D'AGRAIN, directeur général du Centre des Hautes Etudes du Cyberespace
- Grégoire GERMAIN, directeur du développement de l'offre cyber, Thalès
- Barnabé WATIN-AUGOUARD, chargé de mission au secrétariat général de la mer
- Patrick HEBRARD, coordinateur national cyberdéfense

Résumé des interventions :
L'espace maritime est essentiel dans les échanges économiques mondiaux. Les bateaux qui assurent le transport des matières et des biens comportent de nombreux systèmes automatisés et s'appuient sur des équipements informatiques. Ils constituent par conséquent des cibles potentielles pour les pirates informatiques, avec de graves conséquences potentielles en matière environnementale ou économique. La sécurisation des bateaux repose sur le contrôle des accès à bord et sur la prise de conscience par les armateurs des risques encourus. Les assureurs auront également un rôle important à jouer en termes d'incitation à la mise aux normes des bateaux.

I – Un secteur sensible concerné par la sécurité informatique.

Le secteur du transport maritime est essentiel pour l'économie mondiale : 90 % des marchandises transportées le sont par la voie maritime, 50000 bateaux sillonnant les mers en permanence, certains chargés de 20000 conteneurs, avec une valeur pouvant aller de 2 à 4 milliards de dollars pour les marchandises transportées par un seul bateau. Or, les bateaux prêtent le flanc à des attaques informatiques variées. Ils s'appuient de plus en plus sur des systèmes informatiques pour la navigation, pour des raisons pratiques mais aussi économiques puisque ces systèmes automatisés rendent possible la réduction de la taille de l'équipage. On parle d'ailleurs de « maritique » pour désigner les systèmes embarqués et leurs interconnexions. Ces systèmes peuvent être interceptés ou brouillés, par exemple pour détourner le bateau de sa route. D'autre part, un bateau peut comprendre beaucoup d'automa-

tismes (jusqu'à 400 sur une frégate moderne) qui commandent des éléments nécessaires à la mobilité, à la production d'énergie à bord, à la sécurité ou aux fonctions auxiliaires (réfrigération, pompes…). L'essentiel des systèmes du bord est donc corruptible. Le but des pirates peut être économique (intercepter un bateau pour voler sa cargaison, rançonner l'armateur ou le pays d'origine des marins) ou terroriste (engendrer un naufrage pour provoquer des victimes, détruire une installation ou créer une situation de crise environnementale). Des hackers ont déjà été employés par des pirates somaliens pour localiser puis attaquer et détourner un bateau. Ils pourraient fort bien faire un jour du chantage en menaçant de prendre le contrôle du gouvernail d'un tanker...L'ENISA a publié dès 2011 un rapport sur les risques touchant le secteur maritime.

Pourtant, si le risque est bien réel, les armateurs ont du mal à le prendre en compte, sans doute parce qu'il n'a jusqu'à présent pas été illustré par des incidents graves. Le danger le plus important identifié par les professionnels de la mer est encore l'erreur humaine ou l'inconscience d'un marin.

II – Identifier la menace

Les attaques peuvent venir de l'extérieur du bateau. Très classiquement, les pirates informatiques peuvent exploiter les failles de sécurité du système internet du bord (celui dont se servent les marins pour communiquer avec leurs familles) ou rentrer par le biais des liaisons électroniques qui irriguent le bord. Un autre moyen de s'introduire dans les systèmes informatiques peut consister tout simplement à infecter la clef USB d'un membre d'équipage ou à utiliser un technicien de maintenance qui monte à bord et n'est pas surveillé pendant son intervention. D'autre part, le temps passé à quai se réduit de plus en plus, ce qui conduit à effectuer des mises à jour de systèmes à distance. Là encore, ces opérations peuvent servir à corrompre l'informatique du bord. Si les bateaux les plus modernes ont pu bénéficier d'une architecture informatique conçue dès le départ dans une optique de sécurité, ce n'est pas le cas des navires plus anciens qui nécessitent en permanence des mises à jour et des patchs de sécurité.

En dehors des bateaux proprement dits, les chargements sont également touchés par une utilisation de plus en plus fréquente de moyens informatiques. Ainsi, les scellés informatiques utilisés par les douanes peuvent introduire un faux sentiment de sécurité.

D'une manière générale, le risque augmente du fait de l'interconnexion des systèmes : une vulnérabilité sur un élément menace l'ensemble du dispositif.

III – Une réponse à organiser.

La sécurisation de l'ensemble des systèmes constitue un chantier de longue haleine. Il est cependant indispensable. Il s'agit également de développer une culture de sécurité pour l'ensemble de la filière, depuis la conception sécurisée des systèmes (secure by design) jusqu'à l'hygiène informatique du dernier des membres d'équipage.

Il apparaît indispensable de faire rentrer la sécurité des systèmes d'information et de communication dans les programmes de formation des professionnels maritimes. L'élément humain restera un maillon faible de la sécurité informatique sauf à consacrer du temps et des moyens à la formation des hommes de mer.

Le dispositif répressif doit aussi être complété. Au niveau international, un protocole de 2005 relatif à la convention pour la répression d'actes illicites s'attaquant à la navigation maritime avait fait entrer dans la réglementation la menace NRBC. La prochaine évolution de cette convention sera la prise en compte de la menace cyber. Au plan européen, la normalisation juridique est encore confuse. En France, il a été demandé au secrétariat général à la mer de pré-

parer une stratégie nationale de préservation des espaces maritimes. Celle-ci comprendra également une partie cyber. Le secrétariat s'emploie à convaincre les armateurs un par un et effectue ce travail en lien avec le SGSDSN, l'ANSSI et le ministère chargé des transports.

Les assureurs pourraient, dans le domaine maritime comme dans d'autres secteurs économiques, jouer un rôle primordial dans la prévention. En imposant, par une politique tarifaire orientée, l'application de certaines mesures concrètes de prévention active ou passive, les assureurs sont susceptibles de changer en profondeur les pratiques des armateurs dans le sens d'une sécurité renforcée. Ils permettront aux normes et directives de trouver plus rapidement une application réelle.

S'agissant des opérations de maintenance à distance, il conviendra de plus en plus de s'orienter vers des prestations incluant des plate-forme de test sur lesquelles les mises à jour seront étudiées puis validées avant leur déploiement effectif. Cette mesure, ainsi qu'un contrôle accru des personnes accédant au bord, permettra de limiter les risques d'infection des systèmes embarqués.

Glossaire :

ENISA : European Network and Information Security Agency
SGSDSN : Secrétariat Général de la défense et de la Sécurité Nationale
ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

ARTICLE A 10

Démanteler un réseau de botnets : de la technique au juridique

Résumé des interventions :
Les réseaux d'ordinateurs zombie (botnets) constituent des armes puissantes aux mains des escrocs et cyberdélinquants. Combattre ce type de délinquance en ligne nécessite des moyens et savoir-faire spécifiques. La poursuite des auteurs relève d'un travail complexe et peut butter sur des problématiques d'incrimination ou de détermination de la responsabilité pénale de ces derniers. Les forces de police et de gendarmerie arrivent à des résultats mais doivent souvent passer par une coopération internationale pour agir efficacement.

Fin 2013, Europol, le FBI et Microsoft menaient une action conjointe qui aboutissait au démantèlement du réseau de botnets nommé « ZeroAccess 1». Cette opération, qui visait plus de deux millions d'ordinateurs à travers le monde, a nécessité une intervention à la fois technique et juridique, notamment par le biais de contacts avec les juridictions de chaque pays concerné. Ce cas concret a permis de dresser un état des lieux de la lutte contre les botnets et de la législation en vigueur en France.

I – Lutte contre les botnets

Le démantèlement des botnets requiert une capacité de remonter les adresses IP (Internet Protocol). Ces opérations se révèlent complexes dans la mesure où les hackers utilisent des VPN (Virtual Private Network) anonymes. Malgré tout, cette démarche d'identification des adresses IP lancée tous azimuts sur la toile peut se révéler finalement payante. En effet, les concepteurs de botnets discutent et échangent entre eux sur des forums en ligne underground, restent en lien avec

Intervenants :
A- Colonel Éric FREYSSINET – Gendarmerie Nationale – Chef de la division de lutte contre la cybercriminalité ;
- Johann BARBIER – ARX Défense et Sécurité – Directeur technique ;
- Garrick STEWART – National Crime Agency – Higher Lead Officier (SIO) ;
- Éric VANDERSTELT – FBI ;
- Émily ODOM – FBI ;
- Alice CHERIF – Ministère de la Justice – Substitute du Procureur de la République près le TGI d'Évry ;
- Hervé SCHAUER – HSC by Deloitte – CEO.

certaines personnes, utilisent des pseudos… Ainsi, la police a confondu un jeune adulte par les nombreuses traces qu'il avait laissées dans les machines et sur Internet (infection présente dans dix milles machines).
Les traces repérées sont utilisées dans les enquêtes et échangées entre les services. En fonction du cadre juridique, l'échange des informations à caractère judiciaire se fait soit à la faveur de conventions bilatérales entre États (ex : convention entre les États-Unis et le Royaume-Uni) soit au titre d'une coopération européenne (Europol, Eurojust).

Deux procédés d'enquêtes ne sont pas prévus en l'état actuel du droit positif en France. Le premier consiste à acheter de manière massive des mails en vue de prévenir une infraction, le second repose sur la faculté de mener des enquêtes sous pseudonyme.
L'acquisition d'un nombre conséquent de mails pour démanteler des botnets a montré son efficacité Outre-Manche. Ce mode d'action vise essentiellement à gagner du temps (deux semaines) pour pouvoir mener un certain nombre d'actions sur un botnet. Actuellement, ce type de procédé ne peut pas être financé sur des fonds des ministères de la Justice ou de l'Intérieur car il n'est pas rattachable à des actes d'investigation. Seule une agence de régulation à vocation interministérielle pourrait se voir autorisée à accomplir ce genre d'action.
Les enquêtes judiciaires sous pseudonyme pourraient se révéler fort efficaces pour aller débusquer des délinquants qui évoluent sous VPN en vue de préparer la commission d'une infraction.

II – Le droit positif en France
Le droit positif dans cette matière comprend les volets civils et pénaux. Ainsi, d'un point de vue légal, le cas d'une société infectée par une machine appartenant elle-même au plus vaste ensemble d'un botnet, ne relève pas de la justice pénale en l'absence d'un élément intentionnel prouvé.
Si une société constatait la présence d'un malware provenant du parc informatique d'une autre société, il en serait rapidement déduit qu'il n'y a pas d'élément intentionnel. L'identification d'une adresse IP n'entraîne pas ipso facto l'interpellation par les services d'enquête du titulaire de celle-ci. Seul un travail d'investigation portant sur l'environnement au regard d'un éventuel profil permet de relever des charges sur une personne susceptible d'être l'auteur d'une attaque informatique.
L'entreprise propriétaire de la machine infectée ne saurait quant à elle être mise en cause sur le plan pénal au motif d'une négligence en termes de sécurité. Cette hypothèse est absente du code pénal même si le préjudice causé concernait un traitement de données à caractère personnel. Sur le plan civil, une entreprise qui serait régulièrement mise en cause en termes de failles de sécurité dans son réseau pourrait en revanche faire l'objet par des tiers victimes d'une action civile en dommages et intérêts. Ce cas d'espèce ne s'est cependant pas encore présenté sur le ressort du tribunal de grande instance de Paris.
S'agissant du droit français, l'arsenal législatif en vigueur répond de manière globale aux défis posés par les attaques informatiques de tous types. S'agissant du botnet, ce dernier constitue un moyen pour commettre une atteinte à un système de traitement automatisé de données. La responsabilité pénale du maître du botnet sera recherchée en montrant la finalité illégale de l'infection et de la création du réseau d'ordinateurs zombies. Ainsi, l'affaire Gameover Zeus2 a révélé que l'intention finale de son auteur était la commission d'escroqueries. L'infraction du chef d'escroquerie était dès lors suffisante pour poursuivre l'auteur. Le législateur n'a pas retenu comme circonstance particulière le fait de commettre une escroquerie par l'usage d'Internet.

Une incrimination d'escroquerie par le biais d'Internet, si elle existait, donnerait une meilleure visibilité en termes statistiques pour identifier et quantifier ce type de cyberdélinquance.

Glossaire :

Botnet : Un botnet (de l'anglais, contraction de « robot » et « net » - réseau) est un réseau d'ordinateurs infestés par des logiciels automatiques et connectés à Internet. Ces ordinateurs communiquent, le plus souvent à l'insu de leur propriétaire, avec d'autres ordinateurs infectés pour l'exécution massive de certaines tâches (collecte de données, travail de calcul, envoi de courriels malveillants type spam, attaques par déni service..). Le botnet exploite à la fois la puissance de calcul de l'ordinateur infecté et les réseaux auxquels il est connecté.
Malware : Logiciel malveillant ou maliciel.

ARTICLE A 11

Smart city : quelle sécurité pour la ville de demain ?

Intervenants :
- Gérôme BILLOIS, Senior manager, Solucom
- Chekib GHARBI, Directeur général, CITC
- Sébastien VINANT, Deputy CEO, INEO Digital
- Philippe RONDEL, Checkpoint
- Paul DOMINJON, Directeur des stratégies de sécurité France, Symantec

Résumé des interventions :
Les projets de smart cities sont devenus un enjeu majeur pour bien des villes. Néanmoins, l'interconnexion croissante des systèmes soulève un certain nombre d'interrogations en terme de sécurité. Plus les réseaux intercommuniquent entre eux, plus les menaces sont grandes. Pour autant, il convient d'assurer la sécurité de la globalité des interconnexions et non plus des seuls systèmes pris de manière individuelle. La sécurité des smart cities se doit donc d'être pensée en amont, dès l'élaboration des différents systèmes de la ville afin que leur mutualisation se déroule pour le mieux et que les citoyens soient davantage en confiance.

Définition :
Les smart cities recoupent des définitions et des dimensions multiples. La notion est apparue au début des années 2000. On peut le plus souvent les définir comme des villes regroupant différents systèmes interconnectés. Il peut s'agir de l'eau, de l'énergie, des transports, des systèmes de sécurité mais également des infrastructures et services sous-tendant la smart city ainsi que le territoire, les citoyens et le tissu économique qui y sont liés.

Les projets de smart city se multiplient aujourd'hui à l'international mais la France n'est pour autant pas en reste. Il s'agit là d'un important marché, estimé à 27 milliards d'euros d'ici 2016. Le processus de mise en œuvre est long.

Le passage à la smart city est devenu un enjeu important pour les grandes villes ainsi que les villes de taille moyenne, leur permettant

alors de gagner en efficacité. Mais ces smart cities attirent dans leur périmètre bon nombre d'acteurs menaçants d'où l'intérêt d'envisager les questions de sécurité et de sûreté.

La transformation de la ville en smart city :

Tout l'enjeu de la transformation est d'obtenir, à partir d'une ville où les services fonctionnent, une smart city garantissant un niveau de sécurité suffisant. On note là une évolution importante ces dernières années. Il fut d'abord question d'une ville numérique, puis d'une ville augmentée, avant de concevoir la ville intelligente, la smart city. Le tout est d'envisager la manière dont le citoyen va pouvoir se réapproprier sa ville.

Désormais, les villes dites « contributives » permettent aux citoyens d'interagir beaucoup plus rapidement avec leur environnement par le biais d'un ensemble de capteurs disséminés dans la ville. Ces derniers contribuent à la gestion de la voirie, des parkings, des déchets, des réseaux énergétiques ou bien encore du chauffage. L'ensemble de ces domaines est alors piloté à distance. L'objectif est d'en simplifier l'accès pour les citoyens. La technologie est ici vue comme un accélérateur de connectivités. Son déploiement doit prendre en compte les particularités et les besoins spécifiques des territoires. Le passage vers une smart city doit aujourd'hui intégrer la question de la transition énergétique. Dans certains cas, la mise en place de tableaux de bord se révélera utile afin d'avoir une vision consolidée des indicateurs du territoire et donc un accompagnement des politiques territoriales.

Les enjeux de la transformation :

Les différents domaines de la ville sont largement informatisés. L'idée de la smart city est de faire en sorte que ces systèmes hétérogènes communiquent entre eux pour se fournir mutuellement des informations et ainsi les présenter de manière unique aux citoyens. La volonté d'une interconnexion la plus aboutie possible est au cœur du processus. De celle-ci découlent certaines difficultés comme le fait de faire cohabiter différents systèmes d'information en prenant en compte leurs particularismes sécuritaires. En effet, les risques et menaces sont propres à chacun des systèmes. Le danger majeur est qu'un individu mal intentionné parvienne à accéder à un des systèmes et puisse alors entrer dans les autres dispositifs interconnectés.

Il existe actuellement trois types de smart cities répondant à des niveaux divers de maturité des villes. Le premier type de ville mettra en place des projets dans un domaine en particulier. On parlera de sécurité « by design ». Il sera nécessaire d'envisager l'aspect sécuritaire dès le départ afin de limiter les coûts. Le second type de ville regroupera une interconnexion de systèmes (énergie, transports, télécoms…). Il conviendra alors de sécuriser l'ensemble.

Le troisième type de ville est celui d'une ville quelque peu réticente à la technologie du fait de craintes en terme de sécurité ou de financement. Le « e-citoyen » transformera sa ville et sera plus avancé que les initiatives de sa propre commune. Le challenge sécuritaire sera différent en fonction de ces trois types de ville. Mais à chaque fois, l'idée sous-jacente sera de faire adhérer le citoyen à la smart city en le rassurant face aux questions relatives à la sécurité et à la sûreté.

La multiplication des systèmes et des connexions contribue à faire croître les menaces. Actuellement, les risques d'attaques sont élevés sur les smart cities. De même, certains individus chercheront à frauder tandis que d'autres s'attaqueront directement aux systèmes industriels.

Malgré le fait que les systèmes soient en place depuis de nombreuses années, ce n'est que depuis peu que les problèmes de sécurité sont envisagés. Le retard pris doit donc être rattrapé d'autant plus que les menaces ont

évolué ces dernières années. On est passé d'attaques de masse à des attaques ciblées. Les administrations publiques sont les plus visées. De même, trois quarts des attaques touchent les PME.
En terme de secteurs, l'énergie et les transports sont considérés comme des infrastructures critiques. En outre, le vieillissement de certaines de ces infrastructures contribue à leur vulnérabilité.
L'hyperconnexion contribue donc à une hypervulnérabilité. Là repose tout le challenge. L'hypervulnérabilité est créée par la répartition de capteurs sur l'ensemble du territoire.
En terme de gouvernance, il est essentiel pour les politiques d'intégrer toutes ces dimensions sécuritaires.

La sécurité et la sûreté dans la smart city :
Les vulnérabilités arrivent bien souvent par le biais des petites communes. Sur un territoire plus important, comme celui d'une métropole ou d'une communauté d'agglomérations, il est indispensable qu'un département soit dédié aux questions de sécurité et de sûreté globale et non plus seulement à celle de la cybersécurité. L'enjeu est de créer une entité ayant la capacité d'assurer une gouvernance globale et transversale pour ce qui attrait à la sécurité de l'ensemble des projets. Tout cela se développe progressivement autour des smart cities. Il convient plus que jamais de mutualiser les moyens tout en prenant en compte les contraintes financières s'imposant aux collectivités. La sécurité des systèmes de la ville doit être envisagée sur le long terme. Les différents acteurs doivent également être formés à ces problématiques.
L'essentiel est de trouver la bonne maille de mutualisation selon l'échelle des collectivités. Les systèmes doivent être sécurisés dès leur élaboration, au stade même de projet, afin de faciliter la sécurité liée à l'interconnexion qui s'en suit. En effet, cette dernière présente de nombreux intérêts en permettant par exemple aux citoyens de disposer d'un maximum de services sur un support unique (exemple des cartes à puce ou d'un capteur unique pour les énergies). Une réflexion commune de mutualisation des systèmes comme l'eau, l'électricité ou les autres énergies est actuellement en cours. Elle soulève les problématiques de la propriété des données, de l'éthique et de la « traçabilité » des individus. La CNIL aura ici un rôle essentiel à jouer.
Afin de sécuriser au mieux les systèmes, il sera nécessaire de cloisonner les identifiants, de proposer des services sur un support unique avec des identifiants différents. Il existe un réel enjeu quant à l'anonymisation des données.
Pour beaucoup, la question n'est désormais plus de savoir si les grandes villes verront leur système smart attaqué, mais quand cela se produira.

Conclusion :
En somme, la cyber-résilience apparaît comme la solution la plus adaptée aux problématiques sécuritaires des smart cities. La réalisation de tests en amont présente aussi un intérêt afin d'adapter au mieux les efforts. La sécurité doit être prise en compte du départ. Elle doit devenir une priorité afin de pouvoir combattre les failles et de faire fonctionner l'ensemble des systèmes interconnectés. On doit passer d'une sécurité individuelle à une sécurité globale en cloisonnant ce qui doit l'être tout en tenant compte des niveaux de risque.
La sécurité des smart cities reposerait donc sur l'éducation de l'ensemble des acteurs (élus, citoyens…), en vue de créer un système de confiance.

ARTICLE A 12

Lutter contre la cybercriminalité en se mettant dans la peau d'un cybercriminel.

Intervenants :
- Marc OLANIÉ, journaliste à CNIS Mag
- Olivier BURGERDIJK, head of strategy, Europol EC3
- Peter FIFKA, senior program manager-investigations, Microsoft Digital Crime Unit
- Erik BARNETT, Attaché auprès de l'UE, US Immigration and Customs Enforcement – Homeland security investigations
- Eric FILIOL, directeur du laboratoire de recherche, Ecole Supérieure d'Informatique Electronique Automatique (ESIEA)
- David SANCHO, Trend Micro

Résumé des interventions :
Pour faire face efficacement à la cybercriminalité, il peut être intéressant d'adopter la mentalité de l'agresseur. Se mettre dans la peau du cybercriminel nécessite une gymnastique intellectuelle particulière. Il est éventuellement possible pour les entreprises de faire appel à des délinquants repentis. Quoi qu'il en soit, cette démarche intellectuelle doit être particulièrement bien bordée sur le plan éthique afin d'éviter tout dérapage.

I – S'adapter face à la délinquance informatique.

Les modes d'action des cyberdélinquants ont évolué très rapidement. Les acteurs sont désormais nombreux dans ce domaine. Il est possible aujourd'hui d'attaquer une entreprise en faisant transiter l'agression par un tiers (ordinateur robot infecté par un virus par exemple) ou encore de changer de cible très rapidement. Par ailleurs, la cible des délinquants reste toujours l'argent : les données sont négociables, le temps passé à rétablir un système coûte cher, la réputation a un prix qui se paie immédiatement… Face à cette multiplicité d'acteurs et de technologies employées, une agence seule ne peut pas agir efficacement et il est désormais indispensable de conjuguer les compétences pour répondre utilement à la menace.

Ainsi, les entreprises spécialisées du secteur privé ont tout intérêt à collaborer avec les forces de sécurité et les magistrats. Il s'agit de partager des savoir-faire et des outils pour les unes, de sensibiliser et de faire prendre conscience des enjeux pour les autres. Les juridictions ont en effet besoin d'avoir une information complète et opérationnelle sur les atteintes liées à la cybercriminalité

pour pouvoir en prendre la juste mesure et en tirer des conclusions adaptées et proportionnelles.
La nécessité d'une coopération entre privé et public a d'abord émergé aux Etats-Unis, elle devrait aujourd'hui être universellement comprise. Le partage des informations entre partenaires privés, entre acteurs privés et publics, nécessite de la confiance. Il est par conséquent essentiel de définir strictement les conditions d'intervention des forces de l'ordre. Paradoxalement, il est difficile de différencier les intérêts publics et privés sur internet.

II – Chacun doit rester dans son rôle.

Pour établir des contre-mesures efficaces, il est toujours utile de se mettre dans la tête d'un agresseur potentiel et d'imaginer ses objectifs et les moyens qu'il est susceptible d'employer pour les satisfaire. Il s'agit bien, ici, de réfléchir comme un hacker mais non d'agir comme un hacker. Les questions d'éthique et de déontologie sont à considérer avec attention, de même que les restrictions légales qui pèsent sur un citoyen respectueux des lois. Entre les Etats, la compétition est rude et chacun considère les choses selon son intérêt et sous l'angle de ses propres règles légales. Dès lors que l'on touche aux questions de sécurité nationale, la solidarité entre Etats s'estompe très rapidement… Le rôle des entreprises privées ne doit pas être confondu avec celui des agences nationales : on ne mène pas des actions de la même manière si l'on est militaire, policier ou entrepreneur privé. Ce dernier est en mesure de participer à la recherche des cyberdélinquants mais ne souhaite pas être entraîné au-delà de ce rôle déjà important. C'est bien à la gendarmerie et à le police de protéger contre le crime.

III – L'emploi de hackers, un choix délicat.

Pour lutter efficacement contre les attaques, il devient de plus en plus nécessaire de faire appel à des dataminers, c'est-à-dire des spécialistes dans l'exploitation des bases de données et la recherche d'information au sein des masses de données. Il s'agit en effet de déterminer les éléments modifiés ou ajoutés pour trouver d'où est venue l'attaque. Le datamining devient une compétence importante pour les entreprises. Il est également possible pour une société d'engager un hacker pour le charger de la défense de ses systèmes d'information. L'avantage de la méthode est que la personne missionnée pour protéger les systèmes va réfléchir avec la tournure d'esprit du hacker : elle va chercher les failles potentielles comme le ferait un hacker et pourra appliquer sur celles qui seront découvertes les corrections nécessaires. Pour attirant qu'il soit, ce recrutement de hackers « retournés » dans le droit chemin ne séduit pas forcément les grands groupes. Ces derniers sont arrêtés à la fois par des questions d'éthique et de prudence. Les dirigeants et responsables de la SSI considèrent souvent qu'il est dangereux d'introduire dans une société un individu qui a trempé en eaux troubles. La crainte est que le raisonnement reste corrompu et que les comportements puissent dévier de nouveau de la norme. Les écoles qui forment aux techniques de contre-hacking mettent l'accent sur l'éthique : il s'agit de réfléchir comme les délinquants informatiques, et non d'agir comme eux. Comme il n'y a pas de système standard d'attaque, il convient avant tout d'être créatif et innovant. Pour anticiper les tendances, il peut être utile de faire de la recherche sous identité masquée. Pour autant, seules les forces de police possèdent la faculté d'agir sous couverture pour déceler des comportements délinquants sur Internet.
La prévention passe certes par des mesures techniques et l'acquisition par l'entreprise de compétences en matière de SSI. La formation des personnels aux mesures basiques de protection apparaît néanmoins indispensable pour réduire d'emblée les risques. Un individu un peu futé et doué d'un minimum de connaissances est bien souvent en mesure de

trouver, par un social engineering bien mené, les informations dont il a besoin pour mener une attaque. Il s'agit d'éviter la dispersion de bribes d'informations qui, rassemblées, offrent un panorama de ce que l'entreprise souhaite justement tenir discret. C'est la sensibilisation des employés et des clients/fournisseurs qui permet seule d'obtenir ce résultat.

ARTICLE A 13

Accompagner et financer l'innovation :

Résumé des interventions :
Afin d'optimiser le potentiel créatif dans le domaine du cyberespace, la France met en place des solutions d'accompagnement et de financement de l'innovation. La détection, la fourniture d'infrastructures et de services doivent permettre d'exprimer pleinement les capacités de création des entreprises françaises. Ce principe est également décliné au niveau européen. Ainsi l'ensemble de ces mesures donne des moyens et offre des solutions aux start-up et aux innovateurs. Elles sont donc particulièrement adaptées aux PME et ET

La France met en place des solutions d'accompagnement et de financement de l'innovation en particulier dans le domaine cyber. Elles sont multiples et mises à disposition selon les objectifs ainsi que la portée et la durée attendues. L'Europe est également active dans la protection de ces projets. Le secteur privé, très actif, s'inscrit lui aussi dans cette dynamique de fourniture de services.

I. Des solutions françaises :
Le nombre de ces dispositifs d'accompagnement et de financement est très important. Cependant plusieurs initiatives sont d'ores et déjà activées dans ce secteur.

Le PEA, le plan d'épargne en actions, s'est renouvelé au 1er janvier 2014. La DGA peut fournir par ce biais des moyens et une sécurité afin de susciter l'innovation. Le PEA se décline en deux produits : le PEA rapide et le PEA à long terme. Le PEA rapide permet à une PME de bénéficier de fonds dans un délais court. C'est ainsi que

Intervenants :
- Thierry FLAJOLIET, manager international des métiers de l'IT, du Cloud et de la Sécurité.
- Pierre-Yves AUBERT, Business Acceleration Officer, EURATECHNOLOGIES.
- Frédéric VALETTE, responsable du pôle SSI, DGA.
- Raouti CHEHIH, CEO, EURATECHNOLOGIES.
- Philippe DEWOST, directeur adjoint en charge de l'économie numérique, mission programme d'investissements d'avenir à la caisse des dépôts.
- Thierry ROUQUET, commission sécurité numérique, AFDE

3 millions d'euros sont injectés par an au service de ces entreprises dans le domaine cyber. Le PEA à long terme est quant à lui plutôt destiné aux PME ayant besoin de financer des projets de recherche et développement, notamment dans le cas d'appels d'offres. Ces fonds sont disponibles rapidement mais la PME doit faire preuve d'une robustesse avérée. Le PEA à long terme mobilise ainsi 35 millions d'euros par an dans le domaine cyber. Les projets ainsi soutenus s'orientent dans des domaines aussi variés que la cryptographie, le développement d'équipement ou la recherche.

Le deuxième dispositif majeur est le PIA, Plan d'Investissement d'Avenir. Les premiers retours sur ce dispositif se feront en 2020 pour le PIA 1. Cet investissement se fait sur la promesse ou l'espoir d'un retour. C'est ainsi que la caisse des dépôts ainsi que neuf autres opérateurs ont reçu pour mission de gérer ce fonds afin de soutenir la stratégie de sortie de crise. Une des conventions de ce plan concerne l'aide au démarrage d'entreprise. Ce fonds national d'amorçage possède un budget de 600 millions d'euros en provenance du fonds pour la société numérique. Il permet de financer jusqu"à 50 % de l'investissement numérique des entreprises du secteur technologique en lien avec la stratégie nationale pour la recherche et l'innovation . Mais il existe aussi plusieurs autres solutions comme le fonds d'investissement direct qui peut fournir jusqu'à 30 % de l'investissement de l'entreprise ou le crédit d'impôt recherche.

II. Des solutions européennes:
La cybersécurité est un enjeu pour un acteur à la hauteur du continent. C'est donc naturellement que l'on doit raisonner « Europe » comme volume de marché dans le domaine de la cybersécurité. L'union européenne s'est ainsi également dotée d'un programme d'accompagnement et de financement de l'innovation. Horizon 2020 est un programme pour le développement de la recherche et de l'innovation avec rendez-vous sur objectif en 2020. Son budget est à la hauteur de son ambition : 80 milliards d'euros. La procédure et la rapidité de libération des fonds sont accrues. L'accompagnement est également total de la conception à la commercialisation.

Ces solutions sont mises en place suite à la déception de nombreuses entreprises qui n'ont pas réussi leur entrée en bourse. Mais l'incubation et l'accélération de ces sociétés sont possibles par le biais d'accélérateurs, à l'instar de l'EIIT. Souvent les entreprises n'utilisent pas assez les capacités entrepreunariales de l'Europe.

« Le marché, c'est l'Europe ! ». Les entreprises doivent prendre en compte ce facteur structurant. La naissance de standards, de critères, et de certifications communes sera un des enjeux de la souveraineté européenne. La sélection de matériel, en particulier de cybersécurité, doit être liée à la certification d'un niveau européen. Ne pas l'intégrer, c'est déjà partir avec un désavantage. Le financement en devient une obligation car le ticket d'entrée est élevé, c'est un secteur hyper spécialisé et hyper compétitif.

III. La FRENCHTECH :
Après l'approche étatique, il y a également des initiatives hybrides comme la French Tech. Le gouvernement français a ainsi créé l'initiative French Tech. Celle-ci s'appuie sur les acteurs qui travaillent au sein des start-up et autres entreprises françaises, qu'elles soient en France ou à l'étranger. Le but est de faire rayonner ces initiatives et de favoriser l'émergence d'innovations. Cette communauté forme un réseau d'accompagnement et de financement. Le rayonnement favorise l'investissement dans le secteur du cyberespace. Ces investissements peuvent être français ou étrangers. L'initiative French Tech n'est pas encadrée

par l'Etat, elle est soutenue par l'Etat. La French Tech favorise ainsi l'accès des entreprises aux aides de l'Etat.

Neuf métropoles French Tech existent déjà, entre autres Lille, Lyon, Toulouse, et ce réseau de développement s'agrandit chaque année. Rien que sur la capitale des Flandres, cette initiative a permis de créer plus de 3000 emplois. L'accélération des entreprises représente un budget de 200 millions d'euros par an et le soutien à la promotion de la French Tech est de 15 millions d'euros par an.

La French Tech regroupe plusieurs SATT qui permettent une montée en puissance des entreprises. Le leitmotiv de la French Tech est de prouver que « La France est le meilleur endroit au monde pour créer une start-up ». Reprendre l'initiative numérique est un objectif économique, mais également de défense. La souveraineté technologique se retrouvera au prix de l'acquisition des dernières techniques de maîtrise du silicium.

Glossaire :

EIIT : European Institue of Innovation and Technology.
ETI : Entreprise de Taille Intermédiaire.
SATT : Société Accélérateur de Transfert Technologique

ARTICLE A 14

Quelle sécurité pour le e-commerce ?

Intervenants :
- Thomas CARLAT, journaliste
- Alexandre ARCOUTEIL, responsable d'activité CERTISSIM / FIA Net
- Pierre BLANCHIER, responsable de la sécurité des systèmes d'information / BOURSORAMA
- Thibault KOECHLIN, consultant en sécurité / NBS System
- Claude MEGGLE, consultant indépendant sur la sécurité / EESTEL
- Laurent PERRIAULT, directeur des opérations / CLARANET

Résumé des interventions :
La performance d'un site doit considérer l'insécurité du e-commerce dès sa création. La sécurité résulte d'un arbitrage aléatoire entre les bénéfices escomptés et les pertes dues à la fraude.
Pour contrer le vol de données, essentiellement les codes bancaires, la parade se situe à tous les niveaux. L'e-consommateur est responsable du choix des mots de passe, de l'utilisation de son mobile et de la préférence donnée à des sites sécurisés. L'e-marchand décide de l'architecture de son site et des niveaux de sécurité qu'il met en place pour les flux financiers.
La qualification de sécurité, la maîtrise ou la délégation de la gestion monétique, l'ergonomie de circulation et d'achat pour les e-consommateurs sont autant d'éléments stratégiques pour les sites du e-commerce pour prendre des parts du marché.

1 – Que représente la fraude sur l'e-commerce ?
L'e-commerce représente 8% du commerce en détail hors alimentaire, en augmentation de 17.5% entre 2012 et 2013. D'après le rapport annuel de l'Observatoire de la sécurité des cartes de paiement, sur l'exercice 20131, le taux de fraude sur les paiements par carte sur Internet baisse significativement : 0,229 % pour 2013 contre 0,290 % en 2012 et 0,341 % en 2011. Toutefois, le taux de fraude à la carte sur Internet demeure vingt fois supérieur au taux de fraude constaté sur les paiements de proximité.
Près de 3% des tentatives de transaction seraient de nature frauduleuse d'après FIA-NET-Certissim, qui représente environ 10 % des transactions sécurisées du e com-

merce. Ramené au e-commerce français dans sa globalité (soit environ 45 milliards d'euros de chiffre d'affaires en 2012 selon la FEVAD - Fédération du E-commerce et de la Vente A Distance), le volume d'affaires concerné par ce risque atteindrait quelque 1,7 milliard d'euros. Il y a une modification du profil des fraudes, la société constate une légère baisse du montant moyen des paniers qui s'établirait à 297 euros pour 2012, soit 8% de moins qu'en 2011. Des paniers élevés génèrent des contrôles systématiques. Sur un panier moyen d'un e-marchand, le taux de fraude est entre 2 et 1,5 %. Si les fraudeurs atteignent leur objectif, l'intensité de leur attaque est multipliée par 5. Enfin, moins d'une tentative de fraude sur trente aboutit réellement à un impayé frauduleux pour le site marchand. Deux types de fraudeurs peuvent intervenir. L'opportuniste ne donne pas de suite à sa tentative d'effraction tandis que le professionnel réitérera autant que possible une fraude aboutie. La réactivité des e-commerçants à la professionnalisation des fraudes entre 2009 et 2011 n'a pas été immédiate. Le taux d'impayé en moyenne nationale en termes de chiffre d'affaire est de 0.2 % des transactions. Ainsi, un e-commerçant peut se considérer peu exposé à la fraude si son chiffre d'affaire n'est pas impacté au-delà de ce poucentage.

2 – Les fraudes

Près des deux tiers de la fraude sur cartes bancaires proviennent de l'usurpation des numéros bancaires. Les méthodes employées sont les spywares (ou logiciels espions) pour permettre l'accès aux mots de passe, le phishing (hameçonnage) pour récupérer des données personnelles au niveau du e-consommateur ou encore le piratage des sites des commerçants où sont stockées les données des cartes bancaires. Le niveau de sécurisation relève d'un arbitrage entre les frais de sécurisation, les pertes enregistrée pour l'e-commerçant et l'assurance pour l'e-consommateur que la transaction est totalement maîtrisée.

Le mot de passe « faible » reste la partie la moins sécurisée de la e-chaine. En effet, lorsque le client crée son profil sur un site, il serait nécessaire qu'il n'utilise pas systématiquement les mêmes identifiants et mots de passe. En effet un e-commerçant compromis peut avoir un effet domino sur d'autres sites. Il est conseillé aussi que le mot de passe comporte au moins un chiffre, une majuscule et un caractère spécial. Il apparaît que la modification systématique du mot de passe ou/et la création de mots de passe « complexes » soit fastidieux pour l'utilisateur qui attend de la e-vente la souplesse, la rapidité et la simplicité. Un e-commerçant ne peut contraindre le client à modifier systématiquement son mot de passe ou ses mots clés. Il lui incombe en revanche de le lui rappeler avec cependant le risque de perdre son client pour un site plus souple. Il est possible de contrer cette faille en faisant appel à des services de coffre-fort de mots de passe.

3 – Les solutions

L'organisation d'une architecture sécurisée en amont augmente le coût d'installation de 10 %. Si la sécurisation est faite en aval, le coût d'une attaque peut en revanche être de 100 %...

Beaucoup de solutions et de normes sont mises en place dont les règles PCI DSS et CISP . L'authentification forte est considérée comme la réponse la plus appropriée. Elle consiste à renforcer la sécurité d'une transaction en ligne et repose sur un identifiant couplé à un mot de passe, auquel s'ajoute la possession d'un objet matériel propre à l'utilisateur, remis par sa banque. La tokenisation vise à remplacer les numéros des cartes bancaires par un token, celui-ci ayant une valeur arbitraire qui n'a aucun lien avec le numéro de carte initial. L'authentification forte peut être contournée si elle est considérée comme l'unique point de résistance. Un virus dormant activé après l'authentification est tout à fait envisageable. La reconnaissance d'un mobile délégué à l'e-consommateur est aussi aléatoire si

celui-ci n'applique pas des règles de base de sécurisation de son matériel. Une nouvelle génération de cartes bancaires a été proposé dont le code de sécurité (cryptogramme visuel) se renouvelle automatiquement toutes les heures.
Le site d'Amazon a développé le système one-clic où l'e-consommateur a au préalable fourni toutes les informations bancaires nécessaires pour effectuer ces achats en ligne. Mais si une seule donnée à la source est modifiée, par exemple la nouvelle adresse IP d'un ordinateur neuf, le système est bloqué.

Conclusion.
La variable humaine dans la sécurisation du e-commerce reste importante. L'e-consommateur peut, par la gestion des différents sites qu'il consulte, réduire les risques de pénétration et de correspondance. Des procédures de certification permettraient aussi aux clients de se détourner des sites qui ne présenteraient pas les sécurités nécessaires.
L'e-commerçant doit accepter la prise en compte du facteur sécurité dès l'initialisation de son site, il reste l'interlocuteur principal pour inciter ses clients à une consultation raisonnable.
Mais pour de grosse plate-forme, la maîtrise du flux financier est une question stratégique. En maîtrisant la circulation et le profil de l'acquéreur, ces e-commerçants acquièrent une connaissance parfaite de leur clientèle.
Les techniques qui se développent sont autant de niveau de sécurisation qui rendent plus complexes l'activité des fraudeurs. La fiabilité résulte d'un juste équilibre à trouver entre la technologie et la pédagogie.

Glossaire :

PCI DSS : Payment Card Industry Data Security Standard
CISP : Cardholder Information Security Program

ARTICLE A 15

La coopération internationale contre la cybercrimilité, des attentes du terrain aux programme internationaux

Résumé des interventions :
Le cyberespace ne connaît pas de frontière et les cyberdélinquants en profitent, obligeant les États à mieux se connaître pour coopérer et coordonner leurs actions. L'atelier repose sur quatre approches distinctes mais complémentaires. Le monde académique et la sphère policière opérationnelle soulignent les enjeux de la coopération policière. L'intervention d'un magistrat et celle d'un acteur du conseil de l'Europe dessinent les modalités des coopérations internationales.

Recherche et applications opérationnelles

L'apport de la recherche est essentiel aux forces de sécurité pour lutter contre la cybercriminalité. La recherche permet de mettre en lumière les éléments structurants d'un problème. Elle peut révéler également le besoin de certaines compétences. Le monde universitaire a un impact sur les organisations à caractère opérationnel dans le domaine de la cybersécurité. L'aide peut être substantielle, comme l'a démontré la recherche sur des contentieux du cyber. Ainsi, les travaux sur le harcèlement cyber (cyberstalking) au Royaume-Uni ont permis en 2012 d'incriminer ces comportements. Il est également possible d'évoquer les travaux entre différents pays européens sur la cyberpornographie. Les coopérations et partenariats sont multidisciplinaires. L'aide apportée est réelle. Le monde universitaire doit se persuader de cette efficacité, c'est même un critère d'évaluation de son travail. Certes, entre le début des travaux de recherche et leur mise en œuvre opérationnelle, des mois, voire des années, peuvent

Intervenants :
- Alexandre SEGER, secrétaire de la convention sur la cybercriminalité, Conseil de l'Europe
- Papa Assan TOURÉ, magistrat, directeur du centre national d'état civil au Sénégal
- Laurent BAILLE, coordinateur des projets de cybercriminalité, gendarmerie nationale.
- Carsten MAPLE, director for cybersecurity research, université de Warwick.
- Jean-Christophe LE TOQUIN, consultant en stratégie en cybersécurité, cybercriminalité et données personnelles, Socogi.

s'écouler. L'aide proposée se matérialise tout d'abord par la publication d'études et de travaux. Dans le domaine de la cybersécurité et plus globalement de la sécurité, les productions gagneraient à être bien plus nombreuses à l'instar des publications médicales. Il y a donc un potentiel de développement très important.

Une coopération indispensable

La coopération internationale s'appuie sur un volet technique et sur une action opérationnelle. Cette dernière est incarnée à l'échelle de l'Europe par la convention de Budapest et les directives européennes. Ces textes visent à harmoniser les législations nationales. Ces coopérations sont portées par des acteurs et organisations telles que le G7, Interpol, Europol ou encore Eurojust. On peut relever des pistes d'amélioration en s'assurant par exemple d'une application effective des directives, en réduisant les délais dans les processus et en recherchant leur standardisation. Dans l'absolu, la création d'un Schengen numérique, c'est à dire un espace supranational de coopération policière et judiciaire, serait idéale. Dans le cadre de la coopération technique au niveau européen, de nombreux projets ont abouti. Ainsi en est-il du collège européen de police (CEPOL). Les possibilités d'évolution sont nombreuses. Une meilleure coordination s'impose face à la multiplicité des projets et des acteurs. L'un des leviers dans l'amélioration des coopérations est un langage commun. Les partenaires doivent se comprendre pour communiquer. A cet égard, Europol ou Eurojust ont un rôle crucial à jouer en permettant la création de réseaux. Les partenariats sont à nouer avec le monde académique qui peut apporter une plus-value certaine aux forces de sécurité intérieure. Pour illustrer ce type de partenariat on peut citer le CECyF en France.

Le cas du Sénégal et de la convention de Budapest

L'étude de la coopération internationale éclaire sur l'état et les formes de coopérations possibles. L'exemple sénégalais est à ce titre intéressant. La problématique en matière de cybercriminalité est un contentieux de contenu. Pour y faire face, deux obstacles doivent être franchis. Le premier est celui de la norme juridique qui doit s'imposer avec cohérence. Le second obstacle relève de la coopération internationale qui doit faciliter la mise en œuvre de cette cohérence. Ces deux problèmes pris en compte permettent alors d'envisager, une stratégie qui s'appuie sur trois niveaux. Le premier est celui d'un niveau sous-régional, celui de la Communauté économique des États de l'Afrique de l'Ouest. Cette coopération vise à harmoniser différentes législations. Pour autant, les mécanismes n'existent pas. Le second niveau est celui du continent africain. La Convention de l'Union africaine sur la Cybersécurité et la protection des données à caractère personnel vise « à la fois à définir les objectifs et les grandes orientations de la société de l'information en Afrique et à renforcer les législations actuelles des États membres ». Cette convention, dite de Malabo, présente deux inconvénients. Elle est d'une part fermée aux pays non membres de l'Union africaine et d'autre part les mécanismes de coopération ne sont pas identifiés. Le troisième niveau dépasse le cadre continental. Ainsi, le Sénégal considère que la convention de Budapest est suffisante et très intéressante. Il juge donc qu'il est utile d'y adhérer. C'est une convention ouverte qui permet de s'insérer dans la lutte contre la cybercriminalité avec des mécanismes identifiés.

S'agissant de l'implémentation de la convention de Budapest, il convient de préciser le contexte. Chaque année des centaines de millions de données sont dérobées, le cybercrime est une attaque contre le droit à la vie privée. Il touche également à la liberté d'expression et met en

danger les démocraties. Ensuite, en lien avec ces attaques, c'est aussi la preuve numérique qui est importante. On constate que les victimes attendent peu des capacités de la justice. Dans la plupart des cas, les preuves se trouvent dans d'autres pays, soumises à d'autres juridictions. Cette situation est un frein majeur aux poursuites. C'est donc un véritable défi qui invite au développement des coopérations. Il faut considérer trois angles d'attaque. Le premier est celui que propose la convention de Budapest avec la mise en place de standards pour 63 pays. Le second est celui du suivi et de l'évaluation de la mise en place de la convention. C'est le comité de suivi de la convention qui propose des recommandations, des exercices et des notes d'orientation pour faciliter la mise en œuvre de la convention de Budapest. Enfin, le troisième angle d'attaque repose sur la mise en œuvre de techniques de coopération qui permettent d'agir immédiatement sur le terrain.

Glossaire :

ENISA : European Network and Information Security Agency
SGSDSN : Secrétariat Général de la défense et de la Sécurité Nationale
ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

ARTICLE A 16

Comment se préparer à l'arrivée du règlement européen EIDAS ?

Intervenants :
Reinhard POSCH, CTO de la République Fédérale d'Autriche ;
Frédéric DUFLOT, chargé de mission – affaires réglementaires et juridiques, ANSSI ;
Arnaud DUBOIS,PDG de Dhimyotis ;
Andrea SERVIDA, Task force "Legislation Team (eIDAS)" de la Commission européenne - DG connect
Bruno CHAPPERT, Imprimerie nationale

Résumé des interventions :
Le règlement n°910/2014 du Parlement européen et du Conseil du 23 juillet 2014 pose les bases réglementaires pour une uniformisation, au niveau européen, des services d'identification et d'authentification permettant, à travers les frontières des Etats-membres, de signer des documents ou de s'identifier avec un haut niveau de confiance. Ce règlement s'impose aux Etats-membres sans qu'il soit besoin de le transposer en droit national.

I - Une réglementation transnationale européenne pour peser dans le monde

Le 1er juillet 2016 entrera en application, pour la plupart de ses dispositions, le règlement européen eIDAS, sans qu'il soit besoin de le transcrire dans le droit national. Ce règlement vise à « instaurer un climat de confiance dans l'environnement en ligne » afin de faciliter le développement économique et social. L'UE prend en compte le fait que les populations utilisent de plus en plus les services en ligne et que cet usage doit pouvoir se faire dans des conditions acceptables de sécurité. Porté par les efforts des Etats-membres, eIDAS permet de donner aux citoyens de l'Union une identité numérique forte et utilisable partout en Europe. Les schémas d'identification électroniques bénéficient de trois niveaux de garantie (faible - substantiel – élevé) selon des spécifications techniques qui seront fixées au plus tard le 15 septembre 2015 par la Commission.

Cette réglementation européenne a également pour objet de peser face aux GAFA en imposant l'identité numérique européenne. Il s'agit de forcer les grandes compagnies, notamment américaines, à prendre en compte cette identité dans les échanges commerciaux. C'est une

question liée à la souveraineté numérique européenne qui trouve toute sa pertinence dans les négociations du TAFTA.

II - Prendre en compte les nouveaux usages

Le règlement eIDAS permettra de sécuriser les services en ligne, nouveaux ou déjà en place, au sein de l'UE. Les services d'identification, de certification de site web, le cachet électronique, la signature à valeur probante sur téléphone et tablette constituent autant de progrès proposés au public pour l'accomplissement de formalités administratives ou d'achats sécurisés en ligne. A chaque usage pourra correspondre un niveau de sécurité adapté : le niveau demandé pour des opérations bancaires n'est pas forcément le même que celui exigé pour une affaire d'état-civil ou pour un achat en ligne sur un site d'enchères.

La norme eIDAS concerne le secteur public, auquel elle s'impose de fait, et le secteur privé, qu'elle finira par toucher par nécessité. Selon les secteurs, elle s'appliquera au plus tard en 2018. Ainsi, le secteur bancaire, qui est resté en retrait de ces questions pour le moment, sera bien obligé d'adopter ces normes pour les usages liés au téléphone portable ou à la tablette, par exemple. L'industrie, de son coté, a une immense tâche devant elle pour s'adapter.

III - Donner une vraie valeur à la signature électroniques

La norme eIDAS va accélérer le développement de la signature électronique. Actuellement, les chronotachygraphes installés dans les poids lourds et les autocars utilisent l'identification du chauffeur grâce à sa carte, de même que les professionnels de santé s'identifient avec leur carte personnelle pour accéder aux services de l'assurance maladie. Plus de deux millions de professionnels sont concernés. La nouvelle norme européenne permettra de s'identifier par le biais d'intermédiaires de confiance. Il s'agira d'une signature certifiée, reconnue par les tribunaux et opposable au niveau européen. L'utilisation de cette signature devra concilier facilité d'usage (indispensable pour que son utilisation entre durablement dans les mœurs), niveau élevé de sécurité et confiance du public. En France, la notion de signature électronique est déjà connue et utilisée, l'introduction de la norme eIDAS ne constituera donc pas une révolution mais plutôt une évolution. Le RGS devra en revanche s'adapter et les administrations se mettre à niveau (à tous les niveaux, depuis les collectivités territoriales jusqu'aux services de l'État).

En fonction des usages, les niveaux d'authentification seront variables. Ce sera le cas également en fonction des pays : il faut accepter le fait que chaque Etat est différent et qu'il utilise des moyens d'authentification qui lui suffisent. Un niveau minimal sera cependant imposé de manière à ne pas créer de maillon faible. Enfin, la question de la conservation et de l'archivage n'est pas totalement réglée. La signature doit-elle être valable pendant 10, 20, 100 ans ? Il s'agit d'établir une durée compatible avec les impératifs de la vie économique et qui ne fragilise pas les accords commerciaux.

Glossaire :

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

eIDAS : electronic IDentification And Signature – Identification et signature électronique. Pour le texte intégral , en français, du règlement, voir le site institutionnel http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=OJ:JOL_2014_257_R_0002&from=EN

GAFA : Google, Amazon, Facebook, Apple – acronyme utilisé pour désigner les groupes actuellement dominants dans le domaine du commerce électronique.

TAFTA : Trans-Atlantice Free Trade Agreement – accord transatlantique de libre échange.

RGS : Référentiel Général de Sécurité – voir http://references.modernisation.gouv.fr/rgs-securite

ARTICLE A 17

Gestion des risques et assurances

Intervenants :

- François Beaume, Président de la commission SI, AMRAE
- Jean-Philippe Bichard, Fondateur rédacteur en chef site et mensuel de Cyber Risques News
- Jérôme Gossé, Responsable souscription RC Professionnelle et Management, Liabilities Zurich France
- Lazaro Pejsachowizc, RSSI, CNAMTS
- Bruno Ollivier, Deputy CSO, Atos Big Data & Security

Résumé des interventions :

Plusieurs incidents récents ont joué un rôle moteur dans la prise de conscience à la fois de l'impact financier d'un incident de sécurité mais également de la responsabilité qui pesait sur le « top management » de l'entreprise. La protection des données d'une entreprise est un enjeu stratégique. Il relève de la responsabilité de l'entreprise d'établir une cartographie des risques qui permettra de garantir la chaîne des processus et des engagements contractuels. L'assureur peut accompagner et sensibiliser les entreprises sur les données que celles-ci acceptent de partager. La mise en sécurité des réseaux ne relève pas de l'expertise des compagnies d'assurances. Par leur visibilité sur les risques potentiels et l'évaluation des frais possibles au règlement d'un accident ou d'une attaque cyber elles participent cependant aux processus décisionnaires des responsables sécurité informatique.

Evaluer la valeur de l'immatériel, déterminer qui est responsable et qui est victime d'une cyber attaque, évaluer le préjudice immatériel constituent autant de difficultés. Les entreprises et les assurances doivent trouver une plate forme minimum de confiance et de partage des données afin d'estimer au mieux la valeur de biens immatériels à assurer. Certains craignent pourtant une intrusion des assurances dans le bien informationel des entreprises.

I – Le périmètre

En amont de toutes décisions, le risk-manager doit bâtir une gouvernance de sécurité globale cohérente, à partir de laquelle il sera possible d'identifier les risques. L'analyse portera sur les systèmes d'information interne, les collaborateurs, les contrats avec les sous-traitants, la chaîne d'approvisionnement, les technologies de rupture, les infrastructures et les chocs externes. Les réseaux ouverts, l'externalisation, l'infogérance, le Big Data sont autant d'éléments à prendre en compte dans la sécurité interne de l'entreprise. Une cartographie des risques lui permettra de hiérarchiser les éléments à sécuriser et de s'assurer du degré de maturité sécuritaire du système d'information. L'émergence du cloud a complexifié la chaîne de responsabilité et de décision notamment par le transfert de la sécurité et la multiplication des interlocuteurs.

Cette analyse du système permettra de développer et de valider les procédures de sécurisation par la sensibilisation du personnel, la définition des contrôles à mettre en place et l'inventaire des éléments de règlement de la crise sur les bases de la méthode MEHARI1.

2 – Mise en place de la prévention

La mise en lumière des risques et des fragilités du système de l'entreprise permettra l'élaboration d'un plan d'action qui garantira la chaîne des processus et des engagements contractuels alignés sur les enjeux des entreprises. Enfin cette analyse permettra d'identifier les actifs stratégiques en classifiant le patrimoine immatériel, en répertoriant les conséquences d'un incident cyber pour l'entreprise et pour les utilisateurs.

La prévention et l'estimation de la prévention à l'aune du risque encouru se heurtent à deux difficultés. En interne il y a un manque de culture cyber qui rend la compréhension difficile à tous les niveaux RH, dont les décideurs. Par ailleurs les cyber-risques gardent cette particularité qui semble les rendre non assurables par les méthodes classiques d'assurance alors même que les polices d'assurances couvrent des incidents générés par des failles cyber comme la responsabilité civile en cas de fraude. C'est à ce stade que l'expertise de l'assureur est nécessaire. D'une part, il est en mesure de présenter un catalogue des bonnes pratiques qui permettra de caler la cartographie des risques. D'autre part, c'est à lui de définir ce qui rentre dans l'assurable. En effet l'objet de l'assurance n'est pas de couvrir ce qui arrive régulièrement mais ce qui statistiquement a une probabilité faible de se produire. L'objectif est alors de déterminer la probabilité d'apparition des cyber-sinistres et de s'assurer que les responsabilité de chacun sont clairement identifiées afin d'établir l'imputabilité de la faute.

3 – Le transfert de risque

L'investissement dans une assurance cyber n'est pas encore systématique. Le transfert de risque sur une police d'assurance en cyber-sécurité est difficile à estimer et la contractualisation d'assurance sur le cyber-risque reste encore aléatoire. Les niveaux de franchises sont modulables mais restent élevés et il n'est pas possible pour les décideurs de mettre en balance la valeur d'une police classique et celle inhérente à la cyber-sécurité. En effet il y a une différence d'estimation de 1 à 100 entre les deux. La valeur des polices de cyber assurances est telle que des entreprises les jugent trop onéreuses au regard du risque encouru. Afin de pouvoir assurer ces données vulnérables et stratégiques, il faudrait envisager l'intervention des pouvoirs publics.

Lors d'un incident cyber, la solution ne s'énonce pas seulement en termes de cyber assurance. L'impact sur l'environnement de l'entreprise fait apparaître des risques émergents aux conséquences multiples tels que la défiance des consommateurs. Alors qu'une partie des incidents est déjà couverte par les assurances

traditionnelles, comment estimer la valeur du préjudice en cas de perte de données, qu'elle soit frauduleuse ou accidentelle ? La gestion de la crise implique plusieurs niveaux d'intervention, l'identification du problème et des données touchées, le recours à des avocats, l'organisation d'un plan de communication.
La bonne qualification des responsabilités permettant de fixer un juste prix pour la valeur de la police d'assurance rend nécessaire une coopération plus importante entre les compagnies d'assurances et les entreprises. Par ailleurs, la qualification et la responsabilité de chacun peut être compliquée dès lors que les entreprises externalisent une partie de la gestion de leurs données auprès d'entreprises de service du numérique. Se pose la question du niveau au-delà duquel la juste information devient une capacité d'intrusion des assurances sur des données confidentielles de l'entreprise.

Conclusion.
Un bon niveau de sécurité sur la protection des données peut toujours être contourné par de mauvais collaborateurs. Mais une authentification objective du niveau de sécurité définit le niveau de remboursement possible en cas de cyber-attaques. La difficulté reste d'anticiper les besoins en cyber-sécurité des entreprises.
Il demeure que la protection du patrimoine informationnel de l'entreprise revêt une dimension capitale bien que le préjudice réel d'une attaque cyber reste au-delà des préjudices matériels prévus. La définition des responsabilités et l'identification des victimes est démultipliée. L'émergence du cloud a changé la donne dans la définition des responsabilités, notamment avec l'interface des entreprises de services du numériques.

Glossaire :

1 MEHARI(MEthode Harmonisée d'Analyse de Risques), mise au point par le Club de la Sécurité des Systèmes d'Information Français (CLUSIF), pour réaliser une appréciation optimale du risque et gérer le risque dans le temps par la connaissance de son cycle de vie.

ARTICLE A 18

Prévenir et détecter les fuites d'information, une illusion ?

Résumé des interventions :
Toute entité peut, dans le contexte actuel du développement de la dématérialisation des données et de leur partage, être victime de leur fuite, à un moment à un autre, que ce soit en raison d'un acte involontaire ou malveillant. Un certain nombre de démarches et d'outils existent pour optimiser la protection des données en amont et, le cas échéant, pour détecter les fuites au plus vite afin d'en limiter l'ampleur.

I – La valeur des données

La massification des données est un fait. Tout organisme ou entreprise se trouve dans l'obligation de partager des informations par le canal numérique, en interne et vers l'extérieur. Les échanges se multiplient également en raison du développement du travail collaboratif. Les données peuvent fuiter involontairement, par mégarde ou négligence, mais également par malveillance. Ces dernières peuvent en effet intéresser la concurrence (espionnage industriel notamment), la presse, des hacktivistes de haut niveau… Elles peuvent aussi tout simplement être révélées sur des réseaux sociaux comme Facebook par d'anciens salariés cherchant un nouvel emploi. Le but poursuivi est d'en tirer parti, de les vendre ou de les publier afin de créer un préjudice. Pour pouvoir élaborer et mettre en place une stratégie de sécurisation et savoir réagir, le cas échéant, à une fuite de données qu'il est impossible d'empêcher totalement, il est indispensable de procéder à un inventaire du patrimoine informationnel, d'en prendre la mesure et de hiérarchiser chaque élément. Cette procédure permet à l'organisme de prendre

Intervenants :
- Florence PUYBAREAU, journaliste indépendante,
- Joseph HAMZE, Expert SI et moyens de paiement, Société générale,
- Philippe LE BOUIL, chef du bureau Protection Environnement, DPSD,
- Erwan KERAUDY, CEO et cofondateur de CybelAngel,
- Eric DUPUIS, Directeur de l'activité « Consulting Services », Orange cyberdéfense
- Vincent LAURENS, Sogeti, Head of Security Business Development.

conscience de sa richesse et d'entamer alors une démarche de sécurité proportionnée à ce qui mérite d'être protégé. Dans un premier temps, il s'agit d'établir clairement la distinction entre les informations qui peuvent être jugées ouvertes et celles qui relèvent de la confidentialité. Dans un deuxième temps, ces dernières devront être classifiées. Les individus en charge du traitement des données devront, dans un troisième temps, en connaître la valeur, afin, pour les RSSI, d'adapter le niveau de sécurisation requis et, pour l'ensemble des utilisateurs, leur comportement, en limitant au maximum la prise de risque pour les données les plus sensibles. Cela exige de leur part une bonne connaissance des caractéristiques et des vulnérabilités des outils et logiciels informatiques. Ainsi, la problématique des équipements mis à disposition par l'employeur à domicile doit être prise en compte : c'est souvent par une simple clé USB branchée sur un ordinateur personnel, insuffisamment protégé, que des informations pourront être perdues ou captées dans le cyberespace. Cette valeur doit être déterminée à la fois en interne et sur le « marché noir » de l'information, où elle sera inévitablement monnayée.

Pour ce faire, les acteurs de la sécurité doivent être capables de porter un regard extérieur sur les informations détenues dans l'entreprise, afin de déterminer lesquelles seraient les plus prisées et les plus intéressantes pour un tiers. C'est en fonction de cette « demande » extérieure que le degré de protection devra être pensé et appliqué. Une veille effectuée sur les données circulant dans le cyberespace peut être très instructive. Les entreprises peuvent confier ce travail de recherche à des sociétés spécialisées dans ce type de tâche, telle que CybelAngel. La défense doit s'organiser contre le vol émanant de l'extérieur ou susceptible d'être effectué par un personnel de l'entreprise.

Ce travail de référencement en amont est d'autant plus nécessaire qu'il est impossible de contrôler l'ensemble des flux et que la sécurité des données a un coût, assuré par des budgets toujours limités. Il assure à l'entreprise un degré de préparation et une maturité optimaux face à une éventuelle fuite d'informations. Elle pourra alors mesurer l'impact de leur perte et ainsi mieux se prémunir contre la fuite d'informations sensibles.

Enfin, la valeur des données n'est pas intangible : elle varie dans le temps, selon le contexte économique, commercial ou géopolitique. Il est par conséquent primordial d'exercer une vigilance permanente et de procéder à une actualisation régulière du patrimoine informationnel.

II – Les solutions de protection des données numériques

Il n'existe pas de solution clé en main. La réponse ne peut pas être que technique, elle est également organisationnelle. Le facteur humain est aussi primordial. Le responsable de la sécurité informatique doit être en mesure de détecter les connexions sortantes du système d'information dont il a la charge, de repérer tout phénomène anormal. Cette capacité dépend de l'efficacité des outils employés et de son intuition, de sa propre réactivité. La responsabilisation de tout manipulateur de l'information, à n'importe quel niveau, est nécessaire. Des réponses juridiques existent, avec des sanctions pouvant conduire jusqu'au licenciement. À ce titre, l'exemple du groupe américain de la grande distribution Target est édifiant : suite à la révélation d'une fuite de données massive en 2014 (70 millions de données personnelles piratées, adresses mél, postales, numéros de téléphone), le PDG lui-même a dû quitter la société.

Si une fuite d'informations initiée par un utilisateur peut assez facilement être décelée et stoppée, il est indispensable de s'armer contre les attaques massives, opérées par exemple à partir de botnets, et, pour ce faire, de réfléchir à de véritables stratégies de défense.

Les informations circulent, elles sont transmises aux employés, aux fournisseurs, aux sous-traitants, aux régulateurs, aux avocats (par exemple, dans le cas des opérations de fusion-acquisition), aux consultants en recherche et développement. La mise en œuvre d'une défense périmétrique sur chaque point sortant n'est pas réalisable. En revanche, les usages gagneraient à être davantage contractualisés. Ainsi, chaque acteur de la chaîne d'information, chaque personne, physique ou morale, prenant connaissance d'informations sensibles, s'engagerait à assurer une traçabilité des données et consentirait à ce qu'une échéance soit imposée à la détention de l'information. Une homologation de sécurité des différents prestataires et contacts pourrait également être exigée. Ainsi, un cabinet d'avocats aurait l'obligation d'apporter la preuve que son système d'information est suffisamment et durablement protégé. Sinon, il n'est pas exclu de demander au partenaire avec lequel on travaille, de venir consulter sur place les documents les plus confidentiels. Il est de toute façon recommandé d'identifier les individus ou les entités auxquels on ne peut suffisamment accorder sa confiance.

Il serait souhaitable de développer les audits sur les systèmes de sécurité protégeant les données, de mettre en place des outils de métrologie.

Les outils de chiffrement, comme le DRM (digital rights management ou gestion numérique des droits qui autorise un accès conditionnel à une oeuvre, la lecture nécessitant un dispositif spécifique) et la cryptographie, technique pour laquelle la France est par ailleurs en pointe, constituent également des solutions envisageables. Cependant, elles se heurtent à des difficultés d'interopérabilité entre les équipements et les systèmes d'information d'organismes différents.

Dans bien des cas, une réflexion sur le ratio entre le budget dédié à la sécurité et le préjudice financier de données perdues devrait être conduite. De même se pose la question du recours de plus en plus en fréquent aux services de cloud, qui permettent certes de réaliser des économies mais qui augmentent les risques de perte ou de captation de données car ils se synchronisent et répliquent les informations dans le cyberespace.

ARTICLE A 19

[Master class] Quelles solutions innovantes en matière de chiffrement ?

Intervenants :
- Eric FILIOL, responsable de l'axe Confiance Numérique et Sécurité, ESIEA
Synthèse effectuée par la GAV Salignat Séverine, CREOGN

Résumé des interventions :
La France fait état d'un retard significatif en matière de technologies de chiffrement. La libéralisation tardive de la cryptologie et la prise de conscience de son importance, notamment avec les révélations d'Edward Snowden, ont ouvert la voie a un nombre conséquent d'innovations cherchant à répondre aux nouveaux enjeux.
Certains progrès, longtemps espérés, ont été rendus possible ces dernières années. Les technologies de chiffrement ont ainsi gagné en rapidité. Il convient alors de les développer tout en veillant à répondre aux problématiques sécuritaires et juridiques qu'elles peuvent engendrer.
Malgré certaines voix s'élevant en faveur de son interdiction, le chiffrement semble avoir un avenir prometteur devant lui.

Le chiffrement est devenu une matière encore plus critique que par le passé. Les révélations faites par l'ancien employé de la NSA Edward Snowden ont montré que, derrière le chiffrement, se cachent un grand nombre d'enjeux pour la sécurité des États, de leurs communications, des entreprises mais aussi pour la protection des libertés individuelles et de la vie privée.

La volonté de faire évoluer la cryptologie montre que celle que l'on connaît à l'heure actuelle ne répond plus à l'ensemble des besoins et préoccupations.
Dès lors, il est possible d'envisager l'évolution des techniques de chiffrement mais également la vision que les États ont du contrôle de ces technologies. Le chiffrement est aujourd'hui devenu indispensable.

Son utilisation intéresse jusqu'au domaine d'activité des juges antiterroristes.

Rappel des différents types de cryptologie : concepts et limites

Il existe différents types de cryptologies faisant tous du chiffrement mais de manière différente et avec des motivations différentes.

La première est la cryptologie symétrique reposant sur une théorie de la fin des années 50, la théorie dite de Shannon ou de l'information. Elle permet le chiffrement très rapide de données de gros volume et de grande taille mais présente malgré tout certains défauts.

De son côté, la cryptologie dite asymétrique est aujourd'hui couplée à la théorie de la complexité supposant qu'il existe des problèmes calculatoirement difficiles à résoudre à l'instar de la factorisation. Il s'agit de systèmes nettement plus lents que les systèmes de cryptologie symétrique et donc réservés au chiffrement de petites quantités. Ils permettent d'assurer les fonctions d'authentification, d'intégrité et de signature numérique.

Les deux méthodes ont leurs forces et avantages mais présentent des différences notables en terme de sécurité. De fait un troisième type de cryptologie, la cryptologie hybride, tente de marier au mieux les deux procédés.

Malgré tout, le principal problème du chiffrement repose sur sa portée limitée. Jusque récemment, on ne savait pas faire de calculs sur des données chiffrées. A cette difficulté s'ajoute le manque de confiance dans les algorithmes dont la plupart ne sont pas nationaux.

Pour tenter de combler ces lacunes, des solutions voient progressivement le jour.

Les évolutions scientifiques et techniques

Le chiffrement homomorphe est vu comme celui le plus à même de susciter des applications industrielles et des innovations.

En 1978, Rivest, Adleman et Dertouzos s'étaient interrogés sur la possibilité de faire des calculs sur des données chiffrées, ce qui était alors considéré comme « le Graal de la cryptologie ». Depuis, les travaux de Craig Gentry ont permis l'établissement du chiffrement homomorphique venant consacrer cette quête. Il permet d'effectuer des opérations de base sur des données inconnues, chiffrées. Deux systèmes ont alors vu le jour : le chiffrement partiellement homomorphique (exemple du vote électronique) et le chiffrement totalement homomorphique symbolisant l'objectif recherché (l'ensemble des opérations de recherche s'effectuent sur des valeurs chiffrées).

Le principe étant désormais acquis, il convient maintenant de l'améliorer. Cependant, la perspective d'effectuer des calculs sur des données chiffrées est à même de poser des difficultés en justice quant à la notion de preuve numérique.

Une autre évolution est celle des schémas de chiffrement authentifiés combinant un mode de chiffrement et un mode d'authentification. La volonté est de parvenir à échanger de manière sécurisée tout en dissimulant la communication en cours. Cela est assimilable au procédé dit de stéganographie consistant à cacher une information secrète dans une information anodine.

Mais il est possible d'aller plus loin grâce à la technologie Perseus, elle-même inspirée de la théorie des codes. L'idée est que malgré le bruit produit par la transmission, le récepteur puisse récupérer la donnée. Il convient alors de chiffrer le message avec un code convolutif reposant sur une clef, le codeur étant secret et changeant en permanence. Un tel procédé est beaucoup plus sécuritaire car très compliqué à déchiffrer.

De nombreuses autres idées sont en cours de développement. La technique consistant à chiffrer sans que cela se voit, sans passer nécessairement par la stéganographie, est quelques chose de prometteur et fait partie des évolutions à considérer concernant le chiffrement.

De plus, les algorithmes poly-

morphes et métamorphes se sont développés en s'inspirant des travaux effectués sur les virus. Il s'agit de faire fluctuer l'algorithme avec la clef de chiffrement, à l'instar de ce que font les virus pour survivre. On parle de polymorphisme et de métamorphisme.

Sur ces points, un projet a récemment été lancé : le projet Metacrypt faisant varier en permanence l'algorithme et réalisé en partie avec le projet Gostcrypt dans lequel il est prévu que l'algorithme soit différent du départ.

A côté de cela, l'évolution symbolisée par les trappes mathématiques pose la question de savoir s'il est possible d'établir une backdoor indétectable. Tout l'enjeu n'est pas de concevoir un tel système mais de prouver qu'il est possible de le faire.

Les travaux sur les designs combinatoires, initialement financés par la NSA, offrent quant à eux des perspectives d'évolution intéressantes. Il s'agit d'objets ayant de fortes probabilités d'invariance, permettant donc de dissimuler une grande quantité d'informations.

Enfin, la dernière évolution notable est celle de l'aire quantique consistant à utiliser une incertitude au niveau physique. Depuis mars 2014, une équipe des universités de Singapour et de Toronto est parvenue à faire ce qui est assimilable à un chiffrement quantique. Les performances en terme de rapidité sont encore quelque peu décevantes mais une fois de plus, le principe est acquis. Il conviendra ici de parler de technique des transferts équivoques.

Les évolutions légales et sociétales

En France, la cryptologie a été libéralisée avec la loi pour la confiance dans l'économie numérique en 2004, après le Patriot Act. En effet, une étude de 1998 avait montré que le retard de la France en la matière avait entraîné des pertes économiques pour les entreprises nationales, d'où sa libéralisation.

Or depuis quelques temps, des signaux alarmants laissant supposer une volonté d'interdire certaines applications ont été observés, ce qui pourrait à terme se révéler dangereux. En effet, les expertises judiciaires montrent que rares sont les délinquants utilisant les techniques de chiffrement. Dès lors, leur interdiction serait pour beaucoup un non sens.

Conclusion :

Les évolutions en terme de cryptologie et de chiffrement sont très nombreuses. Les opportunités sont grandes, notamment dans le domaine industriel avec la création de nouveaux produits, car si des systèmes sophistiqués ont vu jour, il est indispensable de parvenir à les sécuriser dans leur intégralité. La France et même l'Europe doivent donc rattraper leur retard en terme de technologie de cryptage et de chiffrement, notamment pour assurer la bonne santé de leurs entreprises.

ARTICLE A 20

La cybersécurité « française » à l'export : état des lieux et perspectives

Résumé des interventions :
La réflexion se base ici sur les chiffres fournis par le Livre Blanc de l'association française des éditeurs de logiciels et solutions Internet (AFDEL). Le constat d'une France à la marge des exportations de produits de cybersécurité apparaît rapidement. Il devient plus que nécessaire de remédier à la situation, notamment en cherchant à rendre le pays plus attractif aux investisseurs privés.
Un important travail de fond doit être entrepris par les entreprises concernées. Elles doivent réenvisager leur approche des marchés afin d'obtenir les moyens de se projeter à l'international. Mais pour en arrivant là, la conquête de l'Europe s'impose comme un prélude nécessaire.

Intervenants :
- Yann SERRA, informaticien, grand reporter
- Thierry FOUQUET, Commission sécurité numérique, AFDEL
- Pierre CALAIS, Directeur Général Adjoint, Stormshield
- Clives JONES, Deputy Director, Ukti

La cybersécurité recouvre de larges domaines qu'il convient de distinguer clairement. Elle comprend à la fois les logiciels antivirus, les technologies de communication comme les cartes à puces et les outils de communication, ainsi que l'ensemble des services s'y afférant.
Le secteur des logiciels de cybersécurité est mondial et dominé par les États-Unis et Israël. La France a quant à elle une position de leader dans le secteur de la biométrie et des cartes à puce. Les services demeurent la matière la moins exportable.
Il est intéressant d'envisager les possibilités d'exportation des produits de cybersécurité commerciaux où la France occupe une position très faible. L'exportation de ces produits de cybersécurité civile français, qu'il s'agisse de logiciels d'authentification ou d'antivirus, représente

entre 50 et 100 millions d'euros. Sont ici exclus les produits destinés au secteur de la défense.
Ce chiffre, correspondant au chiffre global des exportations, représente moins le chiffre d'affaire de n'importe quelle société américaine ou israélienne de taille moyenne. En comparaison, au Royaume-Uni, le chiffre d'affaire à l'export avoisine les 1,4 milliard d'euros. Les exportations françaises sont en majorité relatives à la sécurité des systèmes d'information.

Les causes du retard français :
Les difficultés de la France ne sont pas seulement dues à une problématique d'exportation mais davantage à un manque de dynamisme de la filière pour partie lié à son financement. A la différence des pays leaders, la France ne possède pas d'entreprise suffisamment importante pour peser sur le marché. Les sociétés sont très lentes à produire un chiffre d'affaire conséquent et perdent rapidement leur compétitivité d'origine.
La France ne parvient donc pas à suivre un marché beaucoup trop rapide pour elle. Cela est notamment dû au fait que le secteur de la cybersécurité française n'est pas assez attractif pour les investisseurs privés, à la différence des États-Unis qui parviennent à en tirer aisément profit. A cette difficulté s'ajoute l'absence de marché boursier européen des valeurs de technologie, ce qui ne permet alors pas de valoriser les sociétés. Le manque de culture entrepreneuriale est également en cause.

Malgré les volontés, la situation française n'évolue pas. Les montants investis par le secteur privé dans la cybersécurité sont constants depuis 10 ans. A l'inverse, les investissements et aides du gouvernement sont conséquents. En outre, le rôle de la Banque Publique d'Investissement est à saluer.

Les difficultés et les enjeux :
L'important est de parvenir à attirer les investisseurs privés. A cette fin, il convient de prendre conscience de la dimension européenne du marché de la cybersécurité. L'établissement de standards communs à différents pays pourrait permettre d'instaurer une notion de confiance indispensable à un marché aussi conséquent. Les investissements dans les sociétés européennes ouvriraient ainsi la voie à des exportations aux États-Unis et en Asie.
La priorité est donc de solutionner les problèmes de financement.

Pour parvenir à exporter au sein des différents pays européens, ciblés au préalable, il est nécessaire d'adopter une stratégie propre à chaque pays. Or cela nécessite un investissement plus conséquent que la position adoptée actuellement.
La France doit également modifier son approche opérationnelle, sa vision du business. Les politiques de marketing doivent être revues pour prendre en compte les caractéristiques propres des marchés visés. Mais la France n'est pas la seule à devoir adapter ses techniques d'approche des marchés. L'Allemagne a la même difficulté, ce qui explique la faiblesse de ses exportations de technologies de cybersécurité.
De plus, la tendance française à privilégier les entreprises locales la dessert au niveau européen et donc international.

Les solutions :
Afin de développer les exportations françaises, il est nécessaire d'associer les entreprises à l'échelle européenne. Pour y parvenir, les entreprises françaises à l'origine de produits de cybersécurité doivent croître grâce à des efforts continus en terme de R&D et d'investissements. La France doit voir plus loin en permettant à ses entreprises de se développer pour vendre. Elle paie aujourd'hui le tribut de son manque d'investissement dans le numérique et peut s'en sortir en optant pour une vision européenne.
Il convient alors de financer un maintien suffisant des technolo-

gies en différenciant clairement le domaine des technologies de souveraineté de celui des technologies commerciales.

S'agissant d'un marché de globalisation ou de projection à l'international, celui des technologies de cybersécurité a certes besoin d'investissements, mais également de technologies dites de rupture se distinguant des autres pour susciter l'engouement. Dès lors, une part de prise de risque devra être acceptée.

Le fait pour la France de posséder des technologies souveraines ne suffit donc pas. La confiance qu'elles inspirent convient au marché local mais se révèle être un argument insuffisant à l'international. Il est possible d'utiliser l'exemple du groupe Airbus qui tire les bases de sa puissance de son association à l'Europe.

En outre, le développement des associations entre la France et l'Allemagne pourrait se révéler profitable. De même, le produit que l'on cherche à exporter doit être le plus compétitif possible et, de fait, proposer une solution se différenciant des autres pour s'imposer.

Il faut aussi avoir à l'esprit le fait que la tentative de conquête d'un marché ne se produit qu'une fois. Si la chance n'est pas saisie immédiatement, il sera extrêmement compliqué de renouveler l'approche.

En modifiant ses positions et en ciblant ses objectifs, la France serait par exemple à même de s'imposer sur le marché polonais où peu d'acteurs locaux sont présents en matière de produits de cybersécurité.

Au Royaume-Uni, la bonne santé du taux d'exportation repose sur les travaux des universités, des clusters et le soutien du gouvernement. A l'image des États-Unis, d'Israël et du Royaume-Uni, la France doit donc parvenir à établir un écosystème. Cela passe par des efforts dirigés vers les sociétés concernées et un accent porté sur le développement des partenariats, lesquels permettront d'accroître les capacités des entreprises à se projeter à l'international.

ARTICLE A 21

Quelles places pour les menaces cyber dans les plans d'urgence gouvernementaux ?

Intervenants :
Raphaël PROUST, journaliste, L'Opinion ;
Evence RICHARD, préfet, Secrétariat général de la défense et de la sécurité nationale (SGDSN) ;
Lieutenant-Colonel Christophe DESHAYES, bureau défense et sécurité nationale DGGN ;
Daniel BOGDANOV, chercheur senior, Cybernetica ;

Résumé des interventions :
En cas d'attaque d'envergure, qui menacerait les intérêts vitaux de la nation ou les besoins essentiels du pays et de sa population ? Quelle est l'action du Gouvernement ? Quels sont les acteurs concernés ? Quels outils à disposition des gouvernements permettent de réagir de manière appropriée aux événements, tout en protégeant les citoyens, ainsi que les intérêts vitaux et économiques nationaux ? La cybersécurité fait-elle l'objet d'un plan d'urgence gouvernemental distinct ou est-elle intégrée dans chaque type de plans gouvernementaux ? La gestion d'une crise ayant un volet cybernétique, requiert-elle des dispositions spécifiques ? La présente conférence propose des éléments de réponse à ces questions.

I. La planification du SGDSN

La planification, dont le secrétariat général de la défense nationale (SGDN) a la charge, s'inscrit dans une volonté nationale de sécurité. Elle vise à protéger les populations qui résident sur le territoire national, mais également à assurer le fonctionnement des secteurs vitaux de la Nation. Certains secteurs sont d'ailleurs du ressort de l'Etat, tandis que d'autres dépendent du secteur privé. Les menaces sont très diverses : menace terroriste, bombes, prise d'otages, meurtre de masse etc. Mais il convient de ne pas omettre les attaques contre les systèmes d'information. De fait, depuis le début du mois de janvier 2015, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a relevé un nombre croissant d'attaques contre la France
Parmi les plans gouvernementaux,

le plus connu demeure incontestablement le plan Vigipirate. Il existe également un plan cyber au sein du plan Vigipirate, qui est mis en place pour assurer la mise en œuvre de la stratégie générale de sécurité. Mais Vigipirate est et doit rester avant tout un plan de veille et de prévention. Si ce plan n'atteint pas l'objectif fixé, d'autres sont alors mis en place. Ces plans sont dits de la famille "pirate" : PIRATAIR pour tout le domaine aérien, PIRATMER pour le domaine maritime, et enfin PIRANET.

Un exercice PIRANET est prévu en France dans les mois à venir, afin de tester (au plus près de la réalité) la refonte dont il a récemment fait l'objet. Il part de 3 scénarios types afin de caler des modes d'intervention de référence :

Situation d'incertitude, avec dysfonctionnements importants sans que pour autant on puisse en définir la nature,

Situation d'attaque contre des intérêts vitaux de la nation,

Situation de blocage par déni de service.

Le but est de pouvoir assurer la continuité de la vie de l'Etat, de la vie économique, et bien entendu de pouvoir mener les investigations judiciaires nécessaires pour aboutir à la découverte puis à la condamnation des auteurs des attaques. PIRANET est ainsi un plan classique sous la direction du premier ministre et d'un ministre désigné suivant la gestion opérationnelle de la crise, ainsi qu'avec tous les acteurs concernés dans un cadre interministériel. Pour rappel, l'ANSSI est l'opérateur de l'Etat pour toutes les questions Cyber. Il convient de garder à l'esprit que le scénario cyber est également intégré aux autres plans que sont le PIRATAIR et le PIRATMER.

Enfin, l'Etat impose aux grands opérateurs d'importance vitale (énergie, eau potable, alimentation) un effort en termes de planification. Celle-ci sera rendue obligatoire lorsque les décrets d'application de l'article 22 de la Loi de programmation militaire entreront en vigueur.

II. La gendarmerie nationale, acteur de la planification

La gendarmerie nationale est un acteur très présent dans le domaine de la planification, qu'elle soit opérationnelle ou qu'elle soit de crise, agissant alors naturellement sous l'égide du SGDSN. De la planification jusqu'à l'opérationnel et à la gestion de crise, il n'y a qu'un pas. Il existe en effet une grande porosité entre les mondes réel et virtuel et c'est bien aussi le quotidien de la gendarmerie nationale que d'agir dans le cadre du cyberespace.

La vraie problématique est que l'on considère souvent le monde du cyberespace d'un côté, et le monde de la gestion de crises de l'autre côté. Or, il s'agit pour la gendarmerie de créer ou trouver les interfaces entre ces deux mondes tout en poursuivant l'ensemble des missions qui lui sont confiées quotidiennement. Dans le cadre d'une crise, la gendarmerie mène son action au plus près du terrain. Elle teste régulièrement sa résilience au cas où elle devrait agir en mode dégradé.

L'une des réflexions engagées aujourd'hui au sein du Ministère de l'intérieur, en lien avec le SGDSN, est justement la mise en œuvre du "gendarme connecté". Le but est de "libérer" le gendarme du cloisonnement de sa brigade afin d'être encore plus disponible sur le terrain et au plus près de la population. En cas d'attaque contre les moyens connectés de la gendarmerie, cette dernière est préparée à opérer en mode dégradé, tout en s'appuyant sur ses services spécialisés au premier rang desquels se trouve le Service des technologies et des systèmes d'information de la sécurité intérieure (STSI2) et l'ensemble de la chaîne fonctionnelle SSIC (Sécurité des Systèmes d'Information et de Communication).

III. Point de vue extérieur et dimension internationale – le cas lituanien.

En matière de planification, la notion de proactivité est parti-

culièrement importante. Un gouvernement doit être proactif, dans tous les domaines économiques et industriel, mais plus encore au plan informatique ; il en est de même dans le domaine des dépendances économiques, notamment lorsqu'il s'agit des divers approvisionnements extérieurs. Une telle proactivité est ainsi mise en œuvre dans la collaboration entre l'ANSSI et l'agence lituanienne de SSI, qui se montre très performante. Il est également indispensable de détecter les cyberattaques, et donc de bénéficier de très hautes technologies afin d'assurer un service de "monitoring" dans les domaines-clés (transport, énergie etc.). Enfin, il faut identifier et qualifier la réalité de l'attaque en cours. Les témoins d'alerte doivent ainsi être bien rodés, afin que le gouvernement concerné puisse préparer une réponse appropriée.

Des technologies-clés peuvent par ailleurs améliorer significativement la protection d'un Etat et de ses points vitaux. Ce dernier doit les intégrer dans sa stratégie et sa planification en vue de cyberattaques.

Il existe des clauses de sauvegarde et de solidarité au niveau européen et international, malgré une approche très régalienne de ces questions. L'Agence Européenne de la Sécurité de l'Information participe de cette dynamique. On notera que le secteur de l'aviation civile se prépare déjà à cette alternative, notamment depuis l'éruption du volcan finlandais en 2010. Il en est d'ailleurs de même pour le secteur de la santé, ce qui traduit une réelle volonté des États de coopérer en dépit de nombreux obstacles.

La concurrence entre organismes constitue un problème majeur pour la gouvernance européenne et nuit ainsi à la qualité de la réponse en termes de réactivité et d'efficacité. Pour répondre au défi de la cybercriminalité, une agence comme Europol constitue un bel outil de coopération européenne. Au niveau européen, et contrairement à ce qui existe dans chaque pays, aucun plan spécifique ne permet de faire face collectivement à une menace ou à une attaque qui se produirait dans un Etat-membre.

ARTICLE A 22

Quelle politique industrielle française ?

Résumé des interventions :
La structuration de la filière cybersécurité en France tend à évoluer vers le développement d'une véritable politique industrielle. L'écosystème français de la cybersécurité a été marqué par des opérations de consolidation menées par de grands groupes comme Airbus, Thalès, Safran et Orange. Cet effort de constitution de champions s'effectue au milieu d'un important vivier de petites et moyennes entreprises (PME), organisées autour de l'association Hexatrust. Cette dynamique répond à une problématique de confiance et de souveraineté, renforcée depuis la mise à jour des activités de la national security agency (NSA).

I – Une structuration de la filière cybersécurité en France pour quelle politique industrielle ?

Avoir une politique industrielle dans cette filière nécessite l'implication de l'État à travers l'agence nationale des systèmes d'information (ANSSI). Chargée de la défense des systèmes d'information de l'État, l'agence a aussi un rôle de régulation et de contrôle dans le domaine de la politique industrielle de cybersécurité en France. En effet, l'ANSSI apporte sa contribution dans les politiques de labelisation des produits et des prestataires des systèmes de sécurité d'information. Il s'agit ainsi d'agir à divers niveaux : entreprises, opérateurs d'importance vitale (OIV) et administrations. La réussite de cette structuration exige de dépasser l'approche de la vision d'intégration verticale. L'ère de la dématérialisation et du collaboratif oblige à inventer d'autres formes de travail en réseau. Ceci passe d'abord par un changement de l'exercice de l'au-

Intervenants :
- Valéry MARCHIVE, Journaliste, LeMag IT/Tech Target
- Pierre CHASTANET, Deputy Head of Unit, Trust and Security, Directorate General of Communications Networks, Commission Européenne
- Yves VERET – CALAO, Senior Advisor Sécurité Numérique,
- Thierry DELVILLE, Inspecteur Général de la Police Nationale, Délégué ministériel aux industries de sécurité
- Jean-Noël DE GALZAIN, fondateur de l'association Hexatrust
- Thomas FILLAUD, Chef du Bureau politique industrielle, ANSSI

torité, qui ne se construit pas sur un rapport imposé mais sur un respect entre les partenaires. Ces nouvelles organisations souples, en réseau, n'excluent pas pour autant quelques intégrations de nature technologique, en particulier avec du service, pour réussir quelques consolidations horizontales sur un sujet de masse critique.
Le rôle majeur de l'État est d'agir comme modérateur et régulateur. Il revient à la puissance publique de fixer la stratégie nationale de sa politique industrielle. Cette stratégie nationale passe par un besoin accru de réglementation et de certification des systèmes d'information. Les entreprises nationales doivent évoluer dans un monde numérique de confiance.

II – Le positionnement des PME françaises

Les PME sont très biens positionnées pour proposer des offres innovantes au bénéfice de grands industriels dans les thématiques liées à la cybersécurité (attaques ciblées, chiffrement de la voix et des données …). Ces solutions innovantes prennent la forme de produits mais aussi de plus en plus de services. Cependant, les PME souffrent encore d'un manque de visibilité sur le marché pour proposer leurs solutions à de grandes entreprises. Celles-ci préfèrent s'adresser, pour des raisons de confiance, à de grands intégrateurs qui utilisent des solutions américaines, israéliennes voire asiatiques.
Pour remédier à ce manque de visibilité, les PME Françaises de la cybersécurité se sont regroupées en vue de créer un label d'excellence destiné à valoriser les ventes réalisées à l'étranger. Il existe aussi un catalogue qui récapitule l'offre française de cybersécurité. Les PME françaises apportent une plus-value indispensable à l'industrie française. Elles sont les seules dans le tissu industriel français à être en capacité « d'agilité industrielle ». Les PME disposent d'équipes innovantes par rapport aux grandes entreprises qui cumulent un problème de compétences réelles, d'accès aux technologies et de compétitivité.

III – L'accès au financement et à la commande publique

Les sociétés de financement ont un rôle majeur à jouer, notamment par le biais du corporated venture1, éventuellement mutualisé. Le corporated venture est un des instruments pour faire vivre un tissu de PME dans la proximité d'un certain nombre de grands groupes. Cependant, l'accès au financement par le biais de subventions est largement favorisé par l'existence de nombreux dispositifs nationaux et européens : programmes d'investissement d'avenir, crédits impôt-recherche, programme Horizon 2020, business angels...Pour compléter ces offres, les entrepreneurs doivent aussi être en mesure d'attirer les investisseurs. Ces derniers ne s'engageront que si le bilan de l'entreprise démontre des capacités de croissance et un carnet de commande bien pourvu. L'accès rapide au marché pour développer le chiffre d'affaires est donc fondamental à la réussite de toute levée de fonds auprès des investisseurs. Le levier de la commande publique constitue sans nul doute un des moyens les plus efficaces pour accéder rapidement au marché. Pour aider les entreprises, l'ANSSI élabore un guide d'achat à l'attention des acheteurs publics. Ce guide donne une marche à suivre sur l'achat de produits de confiance et inscrire ces derniers dans les marchés publics. À titre de bonne pratique, l'ANSSI a noué un partenariat avec l'Union Générale des Achats Publics (UGAP) pour faire en sorte que les produits de confiance élaborés par les PME françaises soient intégrés directement dans les catalogues de ce groupement.

IV – Le rayonnement européen et mondial de la politique industrielle française

Les entreprises françaises doivent s'adapter au changement pour assurer leur rayonnement. Ce changement se traduit par un

passage, dans tous les domaines, des produits aux services, mais aussi de la propriété des produits à l'usage de ces produits. À ce titre, la cybersécurité devient trop complexe pour que les acteurs du marché achètent les produits sans bénéficier d'une assistance technique d'un prestataire. Ce nouveau marché de service a besoin en retour des personnes qui maîtrisent bien le milieu où ils évoluent, pré-requis indispensable pour installer des technologies de confiance répondant aux besoins des clients. Enfin, pour assurer le rayonnement de la filière française de la cybersécurité, le gouvernement a validé la feuille de route du plan cybersécurité, dit Plan 33. Celui-ci fait partie d'une série de 34 plans établis dans le cadre du programme de la Nouvelle France Industrielle2.

Glossaire :

1 Le corporate venture consiste à structurer les relations entre un grand groupe et une jeune entreprise innovante soit en acquérant tout ou partie du capital de jeunes entreprises, soit en externalisant certaines entités du groupe pour en faire des entités indépendantes.
http://leg.u-bourgogne.fr/rev/084061.pdf

2 Nouvelle France industrielle est le nom donné aux plans de ré-industrialisation de la France qui s'articule autour de 34 plans de reconquête industrielle.
http://fr.wikipedia.org/wiki/Nouvelle_France_industrielle

ARTICLE A 23

LA SECURITE DES GRANDS EVENEMENTS

Intervenants :
Daniel GUINER, expert près la Cour pénale internationale de La Haye
Lieutenant-colonel Jean-Guillaume REMY, CPGC, gendarmerie nationale
Général Thierry OROSCO (2S), ancien commandant du GIGN
Zeina ZAKHOUR, responsable de l'offre de sécurité, Athos

Résumé des interventions :
Tout grand événement se caractérise par une forte présence de personnalités, de spectateurs et de médias. Nécessitant une planification intégrée, il est impératif d'en maîtriser les risques cyber sur le C2. La gendarmerie nationale voit dans l'isolement des moyens de C2 le point clé de la protection. Pour le volet privé, les maître-mots sont la disponibilité, l'intégrité et la confidentialité.

I Grands événements et risque « cyber »

Le représentant du centre de planification et de gestion de crise (CPGC) de la gendarmerie nationale revient sur les caractéristiques d'un grand événement. Il s'agit le plus souvent d'une concentration d'autorités et de population constituant une caisse de résonance médiatique. En marge de l'événement lui-même, les autorités doivent maintenir l'activité économique. Les menaces « cyber » qui concernent le plus souvent les grands événements sont les arnaques, les vols d'information aux VIP, les attaques portant des revendications sociales, le cyberterrorisme et les attaques contre le C2. Les forces de l'ordre peuvent y faire face de diverses manières, par exemple en augmentant la fréquence et le nombre des cyberpatrouilles, par l'application stricte des mesures d'hygiène informatique et l'isolement des moyens C2. Le rôle des cyberpatrouilles consiste à identifier la menace, détecter les signaux faibles et agir en cas d'infractions.

Un grand événement est avant tout une concentration dans l'espace et dans le temps. Les vulnérabilités proviennent surtout de l'augmen-

tation du nombre de partenaires et de la mixité des réseaux. Pour les autorités administratives chargées de sécuriser ces rassemblements, le risque est de raisonner vrai avec des éléments faux. Plus la boucle de décision est grande, plus les vulnérabilités sont importantes. Pour faire face à ces risques, il faut mettre en place des bulles tactiques avec un réseau « mèche ». Ce réseau doit être un réseau privé, crypté (128 bits) et temporaire.

Trois points doivent focaliser l'attention des responsables de la sécurité informatique. Ce sont la disponibilité, l'intégrité et la confidentialité. C'est particulièrement vrai lorsqu'il s'agit de grands événements sportifs qui se caractérisent par un périmètre étendu (exemple : JO LONDRES : 200 pays, 10000 équipements informatiques, 90 sites et 3000 experts informatiques). Il faut donc une approche intégrée de la sécurité. Le prestataire de sécurité doit travailler avec toutes les équipes chargées des questions de sécurité. Il a notamment pour mission de centraliser et d'analyser toutes les informations relatives aux menaces cyber portant sur l'événement en cours ou en préparation.

II Les mesures de sécurité

S'agissant des moyens à déployer pour se protéger, le CPGC considère qu'il est nécessaire de faire une cartographie globale des adversaires. Les entreprises concourant à un grand événement doivent aussi se protéger. La gendarmerie nationale peut, à ce titre, s'appuyer sur son réseau de spécialistes N'Tech (nouvelles technologies). L'ANSSI intervient aussi sur les PIV.

La question de la gestion de la presse est primordiale. L'information est aujourd'hui diffusée en temps réel. Il faut donc partir du postulat que toute information peut être révélée sans délai. Tout le travail des équipes chargées des rapports avec la presse consiste par conséquent à maîtriser autant que possible les informations qui émanent de l'organisation. La gendarmerie peut compter, en la matière, sur les officiers communication (qui existent à l'échelon régional et dans certaines unités spécialisées).

Les infrastructures bâties pour les grands événements doivent intégrer dès leur conception la conciliation entre monde physique et monde digital, en particulier du point de vue de la sécurité. Il convient de tester les réseaux très en amont du début de l'événement pour détecter les failles et y apporter les corrections nécessaires. La sécurité revêt aussi une dimension humaine à ne pas négliger. Les personnels intérimaires, en particulier, doivent être recrutés avec soin. La loi offre la possibilité de faire des vérifications par le biais d'interrogations par les services habilités des fichiers spécialisés. Lorsque l'événement dépasse une certaine ampleur, il s'avère nécessaire de mettre en place des « security operation centers », éventuellement avec des solutions de gestion à distance.

B
ARTICLE 01

Cyberextorsion : du cryptolocker à la rançon en bitcoins

Animateur :
Michel Picot, journaliste, BFM Business
Intervenants :
Alain Bouillé, président du CESIN
Bruno Brocheton, vice-président du CIGREF
Jacques Marzin, directeur de la DISIC
Michel Van Den Berghe, directeur général de Orange Cyberdefense,
Loïc Guezo, directeur du développement chez Trend Micro

Résumé des interventions :
L'extorsion, le chantage et les demandes de rançon ont toujours fait partie intégrante des activités criminelles. Internet a simplement permis de moderniser ces procédés. Lorsqu'une entreprise ou une personne se retrouve confrontée à une demande de rançon suite au cryptage de ses données, quelles solutions s'offrent à elle ? Quels sont les solutions existantes pour déchiffrer ces données ? Quels sont les recours judiciaires qui permettent d'identifier les criminels ? Quels sont les acteurs à contacter ?

Les problématiques issues de l'intrusion au sein des systèmes automatisés mettent en jeu la compétitivité des entreprises. Les fraudes qui en découlent touchent aussi bien les particuliers que les entreprises. S'agissant de cyberextorsion, force est de constater que le point commun réside dans l'absence quasi-systématique de dépôts de plainte malgré les dispositions qu'offrent la loi Godfrain, dont la plus récente reconnaît l'infraction de vol de données. Pourtant, face aux modes d'action élaborés par les délinquants, il existe des bonnes pratiques à mettre en œuvre, qui permettront aux services spécialisés de faire fonctionner pleinement les dispositions de coopération internationale existantes.

I – Quelques modes d'action.
Parmi les modes d'action utilisés par cette nouvelle forme de criminalité, les rançongiciels1 constituent une famille à part entière. Ce genre de phénomène malveillant a été observé dès 2011. La victime peut afficher l'ensemble de ses fichiers mais ceux-ci ont été cryptés à son insu, ce qui la prive d'accès à

son contenu. Elle ne peut en récupérer l'intégralité sans les clés de cryptage, cédées contre rançon au bénéfice de l'auteur du chantage ou de l'extorsion. Toutes les sociétés n'acceptent pas pour autant de payer une rançon. Ainsi, la société Domino's Pizza 2a refusé de s'acquitter d'une rançon auprès d'un maître-chanteur qui détenait son fichier de clients (pas moins de 600 000 noms). Un autre mode d'action consiste en l'émission par les délinquants de faux ordres de virement tendant à obtenir un gel des fonds. Il convient de rappeler que les banques ont à ce titre des obligations de vigilance et que leur responsabilité peut être engagée dans l'exécution d'un faux ordre de virement.

II – Les bonnes pratiques

Il existe des bonnes pratiques dans la lutte contre la cyberextorsion. Sur le plan de la prévention, il est préconisé d'installer un pare-feu et de mettre les données en lecture seule. Il est nécessaire aussi de ne pas détruire les fichiers. En effet, ils pourront être exploitables en matière de preuve pénale et utilisables pour circonscrire la menace. Sur ce registre, les copies d'écran se révèlent être un indice prometteur dans la résolution d'une enquête. Dans le cadre des investigations, le juge des libertés et de la détention (JLD) peut autoriser la réalisation de perquisitions et de saisies informatiques. En appui de ce type d'opération, Europol sera en mesure de neutraliser le virus extrait.

III – La coopération internationale, clé de voûte du succès des enquêtes.

La dimension internationale est primordiale. Elle se manifeste entre-autre par le Centre européen de lutte contre la cybercriminalité (EC3) et Eurojust. La convention de Budapest autorise la constitution d'équipes communes d'enquête et le gel de données. En France, l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) est un point de contact privilégié pour le gel de données numériques.

Les conventions internationales ont prouvé leur efficacité grâce aux actions concertées des attachés de sécurité intérieure (ASI) et des magistrats de liaison. Toutefois, il faut souligner la position des autorités américaines. Ces dernières ne souhaitent pas communiquer d'adresses IP sans au préalable qu'un État ait procédé de manière officielle à une demande d'entraide internationale. Légale sur le fond, il n'en demeure pas moins que ce type de procédure est long en termes de délais de réponse.

Conclusion

L'augmentation du niveau de sécurité de base s'impose. Elle passe entre-autre par l'organisation d'ateliers de prévention, permettant en retour de bénéficier d'une traçabilité des établissements qui ont été sensibilisés. La solution judiciaire offre un arsenal assez complet. Cependant, pour mieux connaître les modes opératoires des cybercriminels, il faudrait renforcer les efforts de formation en faisant appel à un partenariat public/privé ainsi que à un renforcement des moyens humains et matériels.

Glossaire :

1 Un rançongiciel est un programme malveillant reçu par courriel ou mis à disposition sur un site Internet, qui provoque le chiffrement de tous les fichiers d'un ordinateur (et des fichiers accessibles en écriture sur les dossiers partagés si votre ordinateur est connecté à un réseau informatique). Il existe des moyens de prévenir et de remédier à ce rançongiciel. Source : http://www.ssi.gouv.fr/actualite/alerte-campagne-de-rancongiciel/

2 http://www.lemonde.fr/pixels/article/2014/11/21/apres-son-piratage-la-base-de-donnee-de-domino-s-pizza-publiee-sur-internet_4525393_4408996.html, Le Monde, article du 21 novembre 2014.

B
ARTICLE 02

Dématérialisation et sécurité

Intervenants :
- Michel Cazenave, RSSI, Ministère des Affaires Étrangères et du développement international
- Guillaume Despagne, Spécialiste de l'organisation et de la distribution de la téléphonie mobile
- Benoît Louvet, FSSI, Ministère des Affaires Sociales et de la Santé
- Emmanuel Michaud, Imprimerie nationale, directeur de la branche service de confiance
- Jean-Marc Rietsch, CEO - FEDISA

Résumé des interventions :
La dématérialisation n'est pas un simple basculement d'un support papier vers un format numérique ou d'une saisie manuelle des informations vers un traitement automatisé de celle-ci. Elle est à l'origine d'une révolution sémantique avec l'émergence du mot dématique mais aussi des processus métier. Réduction des coûts administratifs, des délais de traitement et plus largement amélioration de la compétitivité, de plus en plus d'entreprises et d'administrations utilisent désormais des procédures totalement dématérialisées.
Pour autant, le passage à l'identité numérique fait naître de nouveaux problèmes en termes de sécurité. Comment identifier la personne ? Comment vérifier son identité numérique ? Comment archiver et protéger l'intégrité numérique des documents ? Comment tendre au risque zéro alors que celui-ci n'existe pas ?

I – Les enjeux

La dématérialisation dans les secteurs de l'économie et des administrations ne se réduit pas à une problématique de mutation technologique mais à un véritable basculement des process. En effet, les enjeux ne sont pas « comment faire à la place de » mais comment transposer dans un monde numérique l'activité humaine de la circulation d'informations et des pratiques formelles ou informelles. Certains proposent dès lors le terme dématique, contraction de dématérialisation et d'informatique, l'estimant

plus approprié pour appréhender les trois éléments qui participent à cette révolution.
Dans un premier temps, la dématérialisation correspond à la transformation de documents papier en format numérique. Mais la saisie numérique rend également possible la collecte systématique de données individuelles permettant la validation d'informations nécessaires à l'accélération et la fluidification des traitements administratifs. Or, cette collecte engendre, en aval, des problématiques de traitement et de conservation des données. Cette révolution technologique induit une conduite du changement maîtrisé. Cette révolution sociétale est plus ou moins prégnante en Europe. On constate que les pays du nord de l'Europe détiennent un niveau d'application numérique fort.
La numérisation n'est opérationnelle que si l'objet et le but de la saisie sont bien déterminés. En effet, la valeur de l'information numérisée implique des niveaux de sécurisation différents et un glissement des métiers et de nouvelles hiérarchies dans les processus décisionnaires. La responsabilité et la place de chacun dans la chaîne économique sont modifiées par ce nouveau traitement des informations. Il est, dès lors, nécessaire de considérer la notion de sécurité et la valeur juridique de ces nouveaux documents.

II - Une nouvelle sécurité pour une nouvelle information

La création de fichiers numériques n'est possible que grâce à une collecte de nombreuses données personnelles à sécuriser. Afin de définir le bon niveau de protection, il est important d'intégrer le plus en amont possible les risques envisageables et la valeur de l'information stockée. L'analyse de ces éléments structure les solutions et classifie les niveaux de sécurité nécessaire. La prise en considération de la vulnérabilité de ces informations se fait à chaque étape de la conception, la prise de conscience du risque d'une attaque potentielle faisant partie du process. Le choix des données collectées, leur type et leur utilisation formatent l'organisation du travail et le niveau des responsabilités.
La validation des données est tout à fait exemplaire de la mise en place de nouveaux réflexes professionnels. La signature physique comme primat de l'identification individuelle est-elle transposable ou est- elle remplaçable ? A l'origine de la question il est nécessaire de s'interroger sur la valeur de la signature et sur son objet. La signature numérique apporte un autre niveau d'authentification. Elle est dans les faits aujourd'hui, un mécanisme numérique utilisant un certificat électronique et créant autour du document une « enveloppe cryptographique » garantissant que le document ou l'e-mail n'a pas été modifié depuis la signature, qu'il provient bien de la personne qui a signé, et auquel peut être associé un horodatage à partir d'un serveur d'horodatage accrédité. Le process de dématérialisation favorise la production de vérifications internes plus opérationnelles et valide la cohérence des informations. Il permet une plus grande fluidité des opérations en amont avec un risque de contournement plus faible.

III - La valeur juridique

Au moment de la numérisation, il est essentiel d'accorder toute son importance à la place du juriste lors de la création du document. Par son expertise il pourra estimer la valeur juridique du document donc le niveau de sécurité et permettre la confiance dans la protection des données. Il peut apporter une évaluation objective des risques au regard des droits et des contentieux. Toutefois, il doit aussi adopter un nouveau regard sur la notion de risques numériques.
Les pratiques induites de la production de preuves sont encore à la source de la « double peine ». Quel est le sens de la preuve par la présentation du document original ? Est-ce la preuve papier ou la valeur authentique de l'information saisie avec les procé-

dures nécessaires pour identifier sa date d'enregistrement et sa non-modification ultérieure ? L'information numérique n'est pas la transposition du document physique. Il est donc nécessaire d'estimer la valeur d'usage de la pièce à produire. Le traitement sera alors différent entre les pièces d'archives à conserver sous format papier et les documents à caractère probatoire. Avec la signature numérique ceux-ci sont recevables sans support papier. Par exemple, la généralisation de la facture électronique est sécurisée grâce au système de sceau électronique 2Bdock.

Par ailleurs, la détermination de la valeur juridique ou non d'un document permet d'éviter la surenchère sécuritaire. En effet 80 % des données récoltées ne nécessitent pas un niveau de sécurité élevé. C'est le sens qu'il faut donner à la dernière convention de l'Union européenne qui indique trois niveaux : faible, substantiel et élevé. Au delà d'un aspect sécuritaire les députés européens en appellent à des dispositifs qui ne soient pas disproportionnés par rapport aux besoins. Cette réglementation européenne doit favoriser un climat de confiance et de sécurité dans l'environnement numérique. Elle sera applicable à partir du 1er juillet 2016.

Conclusion

La sécurité numérique implique l'acceptation d'une remise en cause de ce qui existait auparavant. La surprotection peut être contre-productive et ralentir le process de dématérialisation. A contrario, il est primordial de protéger les données personnelles d'où la problématique inhérente suivante : où placer le curseur de la sécurité et de la validité juridique ?

Glossaire :

ENISA : European Network and Information Security Agency
SGSDSN : Secrétariat Général de la défense et de la Sécurité Nationale
ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

ARTICLE 03

Identité numérique : quels schémas à court et moyen terme :

Résumé des interventions :
L'identité numérique est essentielle au développement de la confiance. Mais elle n'est pas uniquement une affaire de technologie. C'est d'abord un écosystème à mettre en place. Entre e-administration et usages privés et/ou commerciaux, quels schémas mettre en place ? Quels liens entre identité régalienne et identité privée ? quelle répartition des rôles et des responsabilités dans le développement de nos identités numériques ?

Autrefois, l'identité de l'individu ne se définissait que par la fonction régalienne de l'État. Désormais, chaque acteur du cyberespace possède une capacité d'identification et d'authentification des utilisateurs de ses services. La multiplicité de ces identités pour un même individu devrait tendre vers un processus d'unification. Cette démarche permettrait ainsi une gestion centralisée en vue d'une utilisation distribuée.

1. Une définition complexe:
Selon Aristote, l'identité est ce qui est de même nature ou de même espèce alors que pour Leibniz, l'identité est l'égalité. Avant l'avènement du numérique, la définition de l'identité était problématique et complexe. De nos jours, elle a pour principale fonction d'arriver à différencier un élément d'un ensemble. En définitive, l'identité se rapproche d'un ensemble de composantes ou d'attributs que l'on pourrait à la fois attribuer et utiliser pour distinguer un individu.
De cette réflexion, nous en déduisons quatre schémas majeurs : la relation d'une personne avec un usage, l'identité régalienne, l'identité et enfin l'identité personnelle.

Intervenants :
- Animateur : Claire LEVALLOIS-BARTH
- Guy FELCOURT, conseiller stratégique pour les banques.
- Claire LEVALLOIS-BARTH, enseignant chercheur.
- Laurent COUSSONNET, directeur de l'innovation du groupe SOPRA.
- Mamadou BA, directeur du marketing, Morpho.

Ces identités peuvent être authentifiées selon différents vecteurs : mot de passe, empreintes digitales, prélèvements ADN, iris, réseau veineux et autres. Actuellement, les observateurs constatent l'arrivée progressive des données à caractère biométriques dans les procédures d'authentification de l'identité d'un individu.
Une clarification des termes est également indispensable au niveau de la sémantique de l'identité. La différence entre l'identification et l'authentification en est l'exemple parfait. L'identification permet la détermination de l'identité d'une personne, alors que l'authentification consiste à reconnaître celle-ci. Cette détermination induit une incertitude a contrario de l'authentification. La problématique sous-jacente est celle de la protection de la vie privée. L'ensemble de ces données et la diffusion de celles-ci présentent en l'absence de règles juridiques un risque majeur pour les droits et les libertés de chacun.

2. Une identité ou des identités :
La première identité d'une personne dans le monde réel est attribuée par l'État. Disposition relevant d'une mission régalienne, chaque individu de nationalité française dispose dès sa naissance d'un NIR délivré par l'Institut national de la statistique et des études économiques (INSEE).
L'entrée du cyberespace dans nos vies respectives entraîne de facto une multiplication des acteurs avec pour corollaire l'utilisation d'identités différentes. Chacun de nous est détenteur de plusieurs identités numériques : identité bancaire, passnavigo, carte d'étudiant ...
À ces identités-clients s'ajoutent aussi les identités des objets de type smartphone. Dans cette configuration, l'identité de l'individu peut être divulguée par l'intermédiaire de l'identité des capteurs auxquels il est associé, volontairement ou non. Par exemple, le téléphone portable permet l'identification de son utilisateur. Il en est de même pour des objets comme les montres cardiofréquencemètres ou les oreillettes bluetooth. Ainsi, l'être humain peut se définir à travers les identités de ses capteurs.

3. Vers l'identité unique:
La première conséquence de ces identités plurielles détenues par chaque individu, c'est la possibilité technique de les rendre interopérables entre elles. Les partisans de l'interopérabilité y voient deux avantages. Le premier, concerne la sécurisation des échanges et en corollaire l'identification certaine de l'interlocuteur. Le second avantage tient au fait que l'interopérabilité permettrait aux acteurs économiques de fournir des services adaptés à l'individu par une connaissance de son mode de vie et de ses centres d'intérêt. Cette faculté d'interopérabilité existe déjà par la création d'un UID (Unique Identifier ou identifiant unique) pour chaque personne.
Par ce système, la personne pourrait gérer de façon plus simple la diffusion de ses données et améliorer en retour ses entrées/sorties régulières entre monde réel et cyberespace. Or, le développement de l'utilisation d'une identité numérique nécessiterait avant toute chose un consensus entre les services. À ce propos, la « National Identity » (l'identité nationale) pourrait devenir l'identité numérique de confiance au sein de la société avec son extension virtuelle.
Dans le dessein de faciliter les échanges, une IRM (Identity Relationship Management), à savoir la gestion de la relation d'une identité, devient un moyen incontournable. L'IRM devrait permettre à tous les acteurs publics comme privés d'interagir. Cette identité régalienne, rénovée, pourrait par exemple se décomposer en une identité spécialisée accompagnée d'identités spécifiques et cloisonnées.
Il est possible de dégager trois axes forts dans cette réforme : caractère universel de l'identité,

maîtrise de ses informations personnelles et enfin fiabilité des informations fournies.

En 2012, la Commission européenne a publié un projet de règlement visant l'instauration d'une identité unique. Dans ce projet figure la mise en place d'un fournisseur d'identité numérique européen compétent au profit de l'ensemble des États membres de l'Union. Les rédacteurs de ce projet escomptent que ce fournisseur soit opérationnel à l'horizon 2019.

Les modalités définies de cette identité rénovée seront a priori placées sous le sceau de l'influence du « business model » dominant du moment. La définition du schéma directeur dans ce cas de figure sera primordiale. En effet, un schéma de nature dirigiste limiterait les initiatives. À l'opposé, des initiatives non coordonnées augmenteraient d'une manière inconsidérée le nombre d'identités. Il serait opportun que l'identifiant unique soit utilisé par les entreprises dans le but d'empêcher la création d'identités par chaque acteur. Enfin, la participation de l'État ou de l'Union européenne comme autorité régulatrice dans l'attribution des identités favoriserait l'essor d'un cercle de confiance vertue

B
ARTICLE 04

LE Big Data, AVENIR DE LA SECURITE ?

Intervenants :
Monsieur Jean-Paul PINTE, réserviste citoyen de la gendarmerie en cybersécurité
Monsieur Mathieu DESSUS, expert sécurité chez Splunk
Monsieur Vincent LAURENS, Head of Security Business Development at SOGETI Luxembourg
Monsieur Éric CAPELLARI, responsable de la cellule e-fraude pour la Société Générale
Monsieur Reda GOMERY, responsable des activités Data, Business Intelligence & Analytics au sein de l'entité Risk & IT Advisory

Résumé des interventions :
Le Big Data révolutionne le domaine de la sécurité informatique : surveillance du réseau, authentification et autorisation des utilisateurs, gestion des identités, détection des fraudes, contrôles de sécurité, etc. Il permet aux RSSI et DSI de corréler l'information pour avoir une représentation la plus fidèle possible des vulnérabilités et menaces. Comment la mise en œuvre du Big Data permet-elle de détecter, comprendre, analyser et répondre aux cybermenaces ?

I Une nouvelle ère

La surcharge informationnelle qui caractérise le Big Data croît de manière exponentielle. Ces énormes bases de données revêtent des caractéristiques souvent résumées par les trois « V » : volumétrie, variété et vélocité. Il s'agit d'un mouvement de données très varié et extrêmement rapide. Plus qu'un phénomène, ces Big Data sonnent l'entrée dans une nouvelle ère. L'intérêt de ces données réside dans le fait qu'elles puissent être réutilisables. Aussi la pertinence des moyens de recherche est-elle au cœur des débats et des stratégies de data mining.

Le problème des moteurs de recherche exploitant le Big Data demeure la performance. En effet, la difficulté réside dans l'identification optimale des indicateurs les plus pertinents tout en ayant à l'esprit que la donnée n'est pas un but mais un moyen.

II Davantage de sécurité en ligne

Un des objectifs de l'exploitation des Big Data peut être de déceler

les comportements déviants en traitant la masse des données.
Jadis, la détection d'un comportement déviant se basait sur des scénarios d'attaque qui étaient implémentés à l'aide de bases de données relationnelles telle que l'analyse des variations inhabituelles, l'exfiltration d'informations, les mouvement anormaux, etc. Dans l'optique actuelle, il s'agira de déceler l'enchaînement de comportements licites susceptibles de caractériser les actes préparatoires à une attaque. Le cas de la recherche portant sur la fraude bancaire illustre la grande diversité des sources. Dans cet exemple, les malfaiteurs utilisent des moyens licites pour faire des opérations illicites. Ce cas démontre à l'évidence la nécessité d'aller plus loin, y compris et surtout au sein des connexions licites, pour détecter des actions illicites.
Toutefois, encore faut-il déterminer un pattern d'attaque. Il est ainsi possible de rechercher dans les Big Data à la condition d'être précis dans l'objet de ses requêtes.
La lutte contre la fraude grâce à l'exploitation du Big Data participe à la production de sécurité. Cependant, au préalable, il serait indispensable de s'assurer de l'intégrité des systèmes d'information faces aux attaques potentielles dont ils pourraient être la cible. Par ailleurs, les coûts inhérents à l'exploitation des Big Data sont encore de nature à peser sur les décisions des dirigeants d'entreprise.

III Un investissement rentable pour les chefs d'entreprise

La prise en compte des données non structurées (réseaux sociaux, mail, vidéos, photos) devient de nos jours techniquement possibles. Si les technologies d'analyse (analytics) sont matures, leur capacité à prendre en compte la sécurité des systèmes d'information n'est pas totalement acquise. En effet, lorsque des Big Data alimentent des machines à corrélations profondes, la prise en compte de la SSI génère des complications. Pourtant, la sécurisation des Big Data devient un enjeu en raison des risques déjà constatés dans certains modes d'attaque comme l'insertion de fausses données. Par ailleurs, la sécurisation des Big Data et l'exploitation de ces derniers pour créer de la sécurité (anti-fraude, *etc.*) demeurent des démarches coûteuses. C'est la raison pour laquelle, au sein des entreprises, les départements marketing ont tout intérêt à exploiter de manière massive les Big Data dans le dessein de favoriser un retour sur investissement orienté vers un marketing de type prédictif. Il s'agira d'identifier des critères favorisant la constitution de groupes de recherche de nature prédictive. Un système de prévision prend sa source à partir de modèles comportementaux biens connus, tout en étant en mesure de créer de nouveaux modèles issus des caractéristiques les plus récentes. Au final, l'usage des Big Data par les services marketing est de nature à optimiser les gains commerciaux, permettant ainsi de dégager un profit affecté au financement de l'insertion de la SSI dans l'exploitation des Big Data.

Conclusion

Nous assistons à l'avènement du métier nouveau de « data scientist ». Cette fonction ne se résume pas seulement à la capacité à capter, stocker ou rechercher une donnée clé au sein du Big Data. Elle consiste avant tout à localiser la donnée à forte valeur ajoutée. Le « data scientist » doit cultiver un certain pouvoir de conviction à destination de ses dirigeants pour réussir à les sensibiliser au financement de l'exploitation des Big Data. Cette capacité de mobilisation sous-tend deux objectifs : améliorer la sécurité de l'entreprise notamment à travers la lutte contre la fraude en ligne, apporter au service marketing de nouveaux éléments propres à élaborer des stratégies commerciales anticipatives. Une partie des gains procurés par les données à forte valeur ajoutées doit faciliter le financement des systèmes de sécurité d'information présents dans les outils d'exploitation.

L'influence grandissante des réseaux sociaux va de pair avec les informations drainées par les objets connectés. La révolution numérique génère un nombre toujours croissant de données qui sont autant de points de vulnérabilité et de risques d'attaque combinés. Les attaques à l'e-réputation d'une entreprise font désormais parties des risques plausibles en raison du transfert des données qui s'opère vers le cloud depuis son système d'information, sans barrière physique.

ARTICLE A 05

Cyberextorsion : du cryptolocker à la rançon en bitcoins

Résumé des interventions :
D'ici 2018, on estime que le marché du cloud devrait croître chaque année de 29 %. Ce service permet de réduire les coûts de fonctionnement et de stockage d'une organisation mais pose la question de la sécurisation des données placées sur des serveurs distants, situés en dehors de l'entreprise. Les notions de classification des informations et de confiance se doivent de compléter les dispositifs technologiques de protection des données.

Le rôle de l'ANSSI

Confier ses données à un service de cloud, c'est faire le choix de l'externalisation. Cette décision, devenue incontournable, demande une prise en compte des risques encourus et des garanties afin de s'assurer qu'elles ne seront pas volées, réutilisées à mauvais escient ou bien encore marchandées. Dans le cadre de la confiance numérique, il est nécessaire de choisir un prestataire dont l'intégrité peut être prouvée.

À ce titre, l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) propose un référentiel public d'exigences pour les prestataires de clouds. Une première version a été publiée au cours de l'année 2014 pour appel à commentaires, lesquels ont été pris en compte pour la rédaction d'une nouvelle version.

Une phase expérimentale, en conditions réelles, est également en cours auprès de prestataires candidats qui sont ensuite sélectionnés. Les critères de qualification de l'ANSSI concernent d'une part les compétences, qui peuvent être insuffisantes, et d'autre part la confiance, qui doit leur être impérativement associée. Les compétences se vérifient par la

Intervenants :
- Florence PUYBAREAU, journaliste indépendante
- Didier GRAS, RSSI, BNP Paribas
- Yann TOURDOT, chargé des qualifications des produits de sécurité RGS, ANSSI
- Stéphane MORUCCI, directeur de SWID (MEITO)
- Philippe COURTOT, PDG de Qualys
- Thierry FLORIANI, CISO, Numergy

conformité avec les exigences du référentiel. La confiance est estimée en s'appuyant sur des informations et enquêtes administratives. Le site de l'ANSSI propose un catalogue des prestataires qualifiés. Cette démarche réglementaire s'inscrit dans les prémices d'un processus de sécurisation du cloud.

Les autorités administratives sont déjà, conformément au Référentiel Général de Sécurité (RGS), dans l'obligation de travailler, dans le cadre de leurs téléservices et de leurs échanges avec les usagers, avec des prestataires de cloud qualifiés. Le rôle de l'ANSSI est de parvenir, dans ses recommandations, à concilier les besoins et demandes des commanditaires, les contraintes des offreurs de services ainsi que les impératifs en matière de sécurité. Tout organisme peut demander la réalisation d'un audit à l'ANSSI, laquelle évaluera la politique et les solutions techniques de protection des données et pourra engager une procédure de qualification.

La France privilégie une approche réglementaire alors que les Anglo-saxons préfèrent confier la résolution des problématiques liées à la sécurisation des données à l'initiative privée et aux avocats. La combinaison de ces deux conceptions participerait certainement à une meilleure efficacité dans la protection des données.

La typologie des clouds

Le cloud souverain, représenté par deux sociétés, Cloudwatt et Numergy, est financé par l'État. La Caisse des dépôts et consignations s'en trouve actionnaire avec une minorité de blocage. Les clouds provider stockent dans leurs datacenters des données dont la valeur est supérieure à celle de leur raison sociale. Dès lors, une protection juridique est requise.

Le cloud souverain ne respecte que la loi française. Les plates-formes sont sécurisées par des moyens de chiffrement, des firewall, des loadbalancers et tout outil technologique existant. D'autres entreprises françaises, privées, se trouvent sur le marché du cloud : OVH, Gandi et Ikoula, Qualys.

Les banques investissent dans les clouds internes. Selon son cycle de vie, l'entreprise peut avoir recours à des clouds externes, internes ou mixtes, dits hybrides. Selon les cas, la solution interne, externe ou hybride sera préférée à un cloud public ou privé, ou bien encore à un cloud national ou international.

Si la continuité de service prime, on choisira un cloud mondial. En cas de problème géopolitique et si on craint de perdre des données ou de ne pas pouvoir les récupérer, on choisira un cloud national. Seule une analyse des risques permet de déterminer quelle disponibilité-sécurité il est souhaitable d'appliquer à telle ou telle donnée, le tout selon leur nature les obligations réglementaires.

Toutes les entreprises ne sont pas en mesure de consacrer un budget conséquent à la sécurisation de leurs données. La haute performance a un coût. Cependant, les clouds souverains peuvent mutualiser et industrialiser les outils, travailler avec les fournisseurs pour proposer des offres, avec un niveau de sécurité « standard », qui soient accessibles à des PME. Pour les petites entreprise, le paiement à la consommation du service selon des besoins ponctuels offre une flexibilité permet de faire face aux fluctuations d'activité.

Des solutions de sécurité adaptées

Il existe trois types de gisements de données : les régaliennes (le casier judiciaire, la santé, les banques), les smart cities (les télécoms, l'énergie, l'eau, les transports…) et les pseudo-publiques, les GAFA (Google, Apple, Facebook, Amazon), dont l'objectif semble de s'emparer des deux premiers gisements de données. Les premières sont évidemment les plus recherchées sur le marché noir et sont donc soumises à de fortes contraintes de sécurité.

D'une manière générale, l'objectif est d'ajuster le niveau de sécurité en fonction de la valeur des données, qu'il faut donc classifier. L'opération est complexe et délicate. On peut restreindre de manière raisonnée la sécurité sur certaines données, la renforcer sur d'autres jugées plus sensibles.

Apposer à chaque donnée un système de sécurité aboutirait à en limiter l'accès, tandis que leur utilité intrinsèque est justement de pouvoir être utilisées. Le chiffrement a un impact sur les performances des systèmes d'information. Pour autant, rompre les liens entre les données pourrait constituer une première solution en les cloisonnant davantage. En effet, la prise en compte d'un seul type de données se révèle généralement peu exploitable. C'est l'association de deux types d'informations qui est intéressant. Par exemple, stocker dans le cloud des noms de patients et des pathologies, sans lien possible entre les deux, ne confère aucune valeur à ces données, qui ne présenteront donc aucun intérêt pour d'éventuels « capteurs ».

La localisation des données constitue, dans un contexte de compétition économique mondiale, un enjeu géopolitique très important. Tout client devrait exiger de son prestataire des informations sur la localisation (par exemple, uniquement en France ou en Europe) et la récupération immédiate, même si le volume est conséquent (en cas de besoin et d'effacement de toute trace après restitution). Ces garanties doivent figurer sur un document contractuel qu'il s'agira de lire consciencieusement avant toute signature. Le commanditaire doit toujours garder à l'esprit qu'il demeure le seul propriétaire ou responsable de ses données.

Si chaque entreprise assume individuellement la responsabilité de la sécurisation de ses données, elle peut intégrer des associations sectorielles qui seraient plus à même d'exercer une pression sur les gros acteurs du cloud (Google, Microsoft, Amazon, IBM...), dont les sièges se situent à l'étranger. Le tout est qu'ils apportent la preuve de leur niveau de sécurité. Il est également possible de s'adresser à des clouds providers qui ont conjointement élaboré un même cahier des charges européen.

La technologie actuelle permet d'inscrire sur les données un message furtif et indélébile qui peut faciliter la traçabilité et le repérage de données captées. Cela peut permettre de les « retrouver » des années après leur subtilisation.

Pour continuer à se développer, le cloud doit inspirer confiance. C'est tant à ses prestataires d'être en mesure de présenter des indicateurs de fiabilité qu'aux utilisateurs de faire preuve de vigilance et d'adapter leurs usages.

Ainsi, les bonnes questions doivent être posées. Dans le cas des agrégateurs de comptes, il s'agit de s'interroger sur le tiers auquel on cède ses identifiants et mots de passe : se trouve-t-il en France ou à l'étranger ? Il est primordial de sensibiliser les clients aux bonnes pratiques, tout en gardant à l'esprit que les données sont cédées gratuitement, quand bien même elles ont une valeur.

B
ARTICLE 06

Le rôle du cyber dans les conflits

Intervenants :
- Nicolas DIAZ, ICT Manager, FIDH
- Daniel VENTRE, Titulaire de la Chaire Cybersécurité et Cyberdéfense, CESDIP/CNRS
- Matthijs VEENENDAAL, Strategy researcher, NATO Cooperative Cyber Defense Centre of Excellence
- Dominique BOURRA, Expert en cybersécurité

Résumé des interventions :
Le cyber est aujourd'hui présent dans la grande majorité des conflits mais également en dehors. Il connaît un véritable processus d'institutionnalisation mais ne peut cependant pas être la seule dimension employée dans un conflit. Le cyber est le plus souvent utilisé à des fins de diplomatie coercitive, en vue d'éviter un affrontement armé direct, et ses acteurs sont toujours plus nombreux. On parle de guerre de l'information.
Or, l'utilisation croissante du cyber dans les conflits contribue à mettre en exergue un certain nombre de paradoxes, dont l'existence de partenariats insoupçonnés entre les États. Elle alimente également un pan récent de l'économie : celui de la cybersécurité et de la cyberdéfense.

« Rien de tel qu'une bonne cyberguerre pour relancer l'économie et engendrer le chaos ». Tel est le postulat de départ entourant la réflexion sur le rôle du cyber dans les conflits.

Le contexte entourant le cyber :
A l'image de l'opposition entre les États-Unis et la Russie sur les questions cyber, certains spécialistes parlent aujourd'hui de l'existence d'une cyberguerre froide.

En outre, un nombre important de pays ne sont pas encore dotés de technologies de cyber et n'ont pas réfléchi à la manière d'en user dans ou en dehors des conflits.
Malgré tout, on constate qu'un certain nombre de pays, dont la France et les Etats-Unis, sont en train de considérer le cyber comme un espace à part entière et en font une zone de conflits et d'affrontements. La meilleure preuve en est l'institutionnalisation de la cyberdéfense.

Désormais, on estime qu'il n'y aura pas, ou ne pourra y avoir, de conflit ou de maintien de la paix sans la dimension cyber. Le cyber fait dès lors partie intégrante du conflit.

La prise en compte du cyber dans les conflits :

Le cyberespace est un espace constitué de trois couches : une couche physique, matérielle (des infrastructures, du hardware) ; une couche intermédiaire (les logiciels, où il y a du codage) et une couche psychocognitive (des contenus, du sens).

Lorsque l'on va imaginer utiliser le cyberespace dans ou en dehors d'un conflit, les capacités pour l'exploiter de manière pleine et totale ne seront pas nécessairement réunies sur les trois dimensions.

Si l'introduction du cyber dans le conflit semble acquise pour beaucoup d'États, il n'est cependant pas imaginable de l'impliquer systématiquement.

De manière générale, les forces armées rejettent le concept de cyberguerre. Si un conflit uniquement cyber n'est pas concevable, en revanche, chaque conflit armé sur la planète comprend désormais une dimension cyber (systèmes d'armes informatisés, mise en réseau…).

Les acteurs investis dans le conflit ne sont pas uniquement des acteurs militaires et étatiques mais également des acteurs non étatiques agissant via des réseaux publics.

Le développement de la multiplicité des acteurs cyber est ici à souligner. Le cyber occupe un rôle dans le conflit mais aussi en dehors. L'utilisation du ver Stuxnet par les États-Unis et Israël contre l'Iran, en l'absence de guerre ouverte, peut illustrer ce dernier point. Il s'agit alors d'une opération de force se déroulant en temps de paix. Le cyber sert de plus en plus à éviter la guerre en permettant l'exécution d'opérations de force et de pression. Le terme usité est celui de diplomatie coercitive.

Mais si le cyber ouvre la voie à de nombreuses opportunités, cela n'empêche pas les États de s'interdire des opérations par peur de possibles effets non maîtrisés. Pour reprendre le cas de Stuxnet, son utilisation a certes entraîné le blocage de certaines centrifugeuses iraniennes contribuant au développement du programme nucléaire, mais il a dans un second temps poussé l'Iran à se doter de capacités cyber, faisant de ce pays la seconde puissance cyber mondiale selon des sources américaines.

Le cyber permet alors de mener des opérations de perturbation ou de destruction ciblées.

La difficulté à cerner cet environnement tient à la multitude d'acteurs pouvant chacun faire des choses différentes. Le mercenariat pourra exister dans le cyber à l'image de certains acteurs individuels, de loups solitaires, comme il en existe dans les actions terroristes.

Le concept de cyberguerre est pour beaucoup un abus de langage car l'utilisation du cyber ne répond pas à une configuration de guerre.

La montée en puissance du cyber :

Bien que ne comptant que 7 millions d'habitants, Israël est aujourd'hui une des principales puissances en matière de cybernétique et de cybersécurité. Le pays comprend près de 250 entreprises très avancées en la matière et 10 % des investissements mondiaux relatifs à la cybersécurité sont centrés sur des sociétés israéliennes. Le pays représente à lui seul 5 % du marché mondial. Cet essor remonte aux années 2000. Depuis, Israël est devenu le pays au monde le plus soumis aux cyberattaques. En 2014, les attaques ont notamment été surmultipliées à l'occasion des 50 jours de l'opération « Tsouk Eitan » Bordure protectrice visant des infrastructures critiques israéliennes. 70 % de ces attaques ont été commanditées par le Qatar. En outre, Israël est un des rares pays au Monde à procéder plusieurs fois par an à des exercices de simulation de crise majeure sur le plan cybernétique, montrant ainsi que malgré sa position, le pays ne se sent pas invulnérable.

Les paradoxes :

L'opération « Tsouk Eitan » a mis en avant un paradoxe, le fait que le Qatar, principal acteur

visé, soit équipé en cybersécurité par les puissances occidentales. Le cyber met parfois en lumière des soutiens inattendus. Dès lors, de nombreux pays peuvent se sentir menacés. Le cyber favorise le développement d'alliances en dehors des prises de positions officielles.

A cela s'ajoute le paradoxe consistant aujourd'hui à voir que certains Etats ont pris l'habitude de surveiller les journalistes.

Mais derrière les enjeux de cyberdéfense et les cybermenaces, une véritable économie est en train de se créer. On parle d'institutionnalisation.

Dans le cyber, les acteurs se permettront des actions qu'ils n'auraient pas tenté ailleurs.

L'important est de parvenir à sortir de la lecture binaire classique des conflits cyber. Ces derniers sont en effet nettement plus complexes à percevoir.

Il en va de même avec le cas de Stuxnet qui n'était, en réalité, pas une cyberguerre mais davantage une opération de guerre de l'information, psychologique, correspondant à la troisième couche du cyber. Les médias ne seraient alors qu'une simple composante de cette couche psychocognitive.

Un autre paradoxe réside dans le contrôle des organes de presse tandis que les comptes terroristes en ligne se développent à profusion au vu de tous.

Conclusion :

Le cyber est donc bien un nouvel espace de conflictualité mais à la différence des autres espaces, les acteurs n'y séjournent pas et la victoire qui peut y être acquise n'est pas définitive. On parle d'avantage compétitif. Le cyber n'a alors pas de véritable rôle stratégique au sens où il ne permet pas de terrasser un adversaire. Il permet seulement de conserver un temps d'avance. Le cyber est aujourd'hui un plus nécessaire mais la majorité des conflits demeure sous la forme conventionnelle, létale.

De plus, tous les acteurs ne sont pas armés pour se battre dans le cyber. A l'heure actuelle, ce dernier est plus que jamais un outil au service du terrorisme. Les terroristes se servent de la troisième couche pour mener des guerres d'informations. L'intérêt est alors de prendre en compte cette couche trop souvent négligée.

A l'avenir, il faudra craindre les attaques combinées contribuant non pas à faire des cybermorts mais bien des morts.

ARTICLE 07

THREAT INTELLIGENCE : quels outils et quelles méthodes ?

Résumé des interventions :
Dans le domaine de la cybersécurité, il est impossible d'agir sans disposer au préalable de renseignements. L'objectif est de connaître les intentions et les manières d'opérer de ses adversaires. Dès lors, les acteurs sont en mesure de prévenir les attaques.
Les renseignements s'appuient sur différentes sources. Leur partage et leur mise à disposition doivent être encadrés afin d'améliorer la cybersécurité. L'effet final recherché reste bien de détecter les attaques et d'y répondre.

I- La qualité et l'origine du renseignement cyber

Le Renseignement d'Intérêt Cyber (RIC) ou d'Origine Cyber (ROC) ne concerne pas que le renseignement technique. Il s'agit également de prendre en compte les groupes d'acteurs auxquels on a affaire. Il est possible de rechercher des éléments sur les tactiques, outils et procédures des agresseurs. Il existe donc des éléments techniques, comme les marqueurs réseaux et marqueurs fichiers, mais également des éléments d'environnement.
Le modèle économique du « diamant de Porter » (expliquant pourquoi certaines nations sont plus compétitives que d'autres dans des domaines d'industrie) permet de mieux orienter la recherche et d'aborder les éléments d'environnement relatifs à la qualité du renseignement. Cette dernière est essentielle car elle permet de rentrer dans une phase d'anticipation et de prévision. Ainsi, en s'appuyant sur des règles de probabilité, notamment à partir des structurations par la recherche, il est possible de développer des prévisions sur les attaques cyber.

Intervenants :
- David BIZEUL, Airbus Defence and Space Cybersecurity, Head of CSIRT
- Charles RAMI, responsable technique chez Proofpoint
- Valéry MARCHIVE, journaliste, rédacteur en chef adjoint LeMagIT/TechTarget
- Thibaud SIGNAT, responsable avant-vente Europe,SE Manager FireEye
- William DUPUY, chef du Calid, ministère de la Défense
- Thierry BERTHIER, chercheur, chaire de cyberdéfense & cybersécurité Saint-Cyr

En matière de cybersécurité, le renseignement recherché est de quatre types. Il concerne les modes d'attaques des assaillants, les outils utilisés par ceux-ci, les attaques émergentes et enfin les différents marqueurs se rattachant tant aux outils qu'aux types d'attaquants.
Les sources d'informations sont multiples. Le renseignement cyber s'appuie naturellement sur la catégorie de renseignements d'origine cyber (ROC). Il s'agit à la fois d'un travail de veille mais aussi d'observation visant à développer les compétences.
En matière de prévision, les éditeurs sont à la recherche des manières d'opérer et des produits proposés par les attaquants cyber. Au besoin, ils vont les chercher à des fins de consultation et vont parfois même les acquérir sur le dark web. Cette dernière source pose bien souvent des questions d'éthique puisqu'elle est susceptible de participer au financement de l'adversaire.
Pour autant, c'est en se trouvant au plus près de cet adversaire que l'on peut apprendre au mieux afin de pouvoir s'en protéger. Il est ici possible de citer l'exemple du site Zone-H qui offre l'accès à un historique d'attaques sur différents sites web.
Les autres sources, en matière de renseignement, sont celles résultant de travaux de recherche ainsi que les acteurs étatiques à même d'échanger sur certaines problématiques.
Le recueil de ce renseignement n'a d'intérêt que dans la mesure où il est utilisé. Il faut donc le partager avec d'autres acteurs en vue de construire la cybersécurité.

II- Le partage du renseignement visant une meilleure cybersécurité

Le partage du renseignement est une évidence. Il doit être organisé non seulement en fonction des contenus mais également des destinataires.
En effet, les éditeurs conviennent qu'il n'est pas possible de tout partager. Les enjeux économiques, voire de sécurité nationale, sont réels. Aussi, il est primordial de définir au préalable les modes de diffusion tout en gardant un œil sur la manière dont le renseignement est susceptible d'être utilisé. On touche à certaines « cultures pays » qui peuvent varier sensiblement d'un pays à l'autre.
Certaines entreprises redoutent que les difficultés qu'elles ont rencontré en matière de cybersécurité soient rendues publiques. Au-delà de la problématique du client, les portails collaboratifs (les plates-formes des éditeurs) de type Fire-eye permettent d'échanger et de mettre à disposition des informations. Pour ce faire, l'accès est restreint et les droits des clients sont encadrés. Dans ces relations, l'un des objectifs est d'éviter que la connaissance acquise sur l'adversaire ne parvienne à ce dernier même par transitivité.
Au-delà des aspects techniques et pratiques de l'échange de renseignements, c'est avant tout la confiance entre partenaires qui est recherchée. Elle est le socle d'un renseignement de qualité en matière de sécurité. Le facteur humain se révèle indispensable.
Il est évident qu'au niveau des éditeurs, la confiance dans un client est quelque chose qui se construit. La confiance s'établit entre partenaires (offre/demande), au sein d'un secteur particulier (aéronautique, militaire…), mais également au niveau étatique.
Le partage du renseignement vise à rentrer dans une démarche proactive. Ainsi, un travail sur les marqueurs permet de mettre en évidence les phases de détection d'attaques. Ces marqueurs servent à identifier des structures conduisant à cibler des attaquants. Il est alors possible de passer à une phase de modélisation des groupes d'attaquants et d'envisager les réponses aux agressions.
L'aspect technique est le premier ingrédient de la prévention. L'aspect humain est quant à lui indispensable pour passer à l'action, pour prendre des décisions.


FIC
2015

B
ARTICLE 08

Cyberextorsion : du cryptolocker à la rançon en bitcoins

Intervenants :
- Daniel GUINIER, réserviste citoyen de la gendarmerie, expert en cybercriminalité près la Cour Pénale Internationale de la Haye
- - Nicolas BUNOUST, RSSI au conseil général de la Loire-Atlantique
- Lazaro PESJACHOWICZ, président du CLUSIF
- Eric BULLIER, chief operating officer, Seclab
- Ludovic PETIT, Chief security officer, Huawei
- Edward SAVAGE, head of cybersecurity consulting, PA Consulting

Résumé des interventions :
La sensibilisation (awareness, en anglais) des individus aux questions de cybersécurité constitue un élément crucial de toute politique de sécurité prétendant à une certaine efficacité. Il s'agit de former les acteurs économiques et toute la chaîne de l'entreprise : dirigeants, employés mais aussi clients. Les techniques et les méthodes de sensibilisation sont très variées. Les intervenants dans ce domaine sont également très diversifiés : formateurs spécialisés, associations, professionnels de la SSI, etc.

I - Changer le comportement individuel, une nécessité

Le facteur humain est central dans les questions de cybersécurité. En effet, 80 % des pertes sont dues à des attaques dans lesquelles le facteur humain est intervenu. Les usages changent, les comportements doivent aussi évoluer. En l'absence de protection, l'utilisateur devient certes une victime potentielle mais aussi, contre son gré, le possible co-auteur de l'infraction, les botnets fonctionnant effectivement grâce aux ordinateurs non protégés.

Le traitement du facteur humain passe par une intervention dans le processus RH de l'entreprise. Former et investir dans l'humain se révèle au final plus rentable et durable qu'une solution informatique de sécurité. Il s'agit bien d'informer et non d'évaluer les individus. Il est nécessaire de comprendre l'impact potentiel de la formation envisagée sur l'entreprise. La tendance peut être de sensibiliser en faisant peur. Néanmoins, il est sans doute plus pertinent d'accompagner les usages de façon neutre et de responsabiliser le per-

sonnel en exposant les risques sans dramatiser à l'excès.
Les outils de sensibilisation sont nombreux : films, séances d'information, bandes dessinées, serious games, etc. D'une manière générale, les utilisateurs sont demandeurs de bonnes pratiques. Les démonstrations dynamiques fonctionnent particulièrement bien avec les techniciens. Il s'agit de montrer que l'action de sensibilisation est bénéfique pour le business. D'ailleurs, les dirigeants sont également concernés par ces actions, du fait de leur responsabilité légale et civile. Les éléments de langage doivent être adaptés au public. Il convient d'être créatif car les campagnes « classiques » n'ont que peu d'impact dans ce domaine très particulier. L'utilisateur doit être mis en position d'apprenant et ce, de manière ludique : jeux de rôle, scénettes, quizz sont appréciés. Un questionnaire final permet de juger le niveau acquis et d'identifier les utilisateurs qui ont le plus besoin d'informations.

II - TPE/PME : une action à mener

Les entreprises ne sont pas égales devant le risque. Les TPE et PME sont en général moins sensibilisées et peuvent sous-estimer les risques. Elles ont, en conséquence, tendance à y consacrer moins de moyens. Elles sont davantage dans l'immédiateté, leur priorité demeurant la production. Elles cumulent des problèmes de planification, de maturité et de moyens face au risque. Il apparaît nécessaire de mieux former les dirigeants aux enjeux de sécurité qui ne constituent pas pour eux une fin en soi, l'essentiel étant de pérenniser l'entreprise. Le Club de la Sécurité de l'Information Français (CLUSIF) propose un espace dédié aux utilisateurs. Les fournisseurs en sont délibérément exclus, ce qui permet d'échanger de manière plus franche et ouverte. L'alerte sur une menace fonctionne d'abord d'homme à homme et pour ce faire, il est nécessaire d'avoir un espace d'échange.

III - Mesurer la sensibilisation

Toute action de sensibilisation devrait être évaluée. C'est pourquoi, il est important de disposer d'outils permettant d'estimer l'état d'avancement d'une action en cours. Des indicateurs qualitatifs existent. Associés à des questionnaires, ils permettent de juger de l'état de vigilance obtenu. Par exemple, il peut être intéressant de demander au public-cible ce qu'il pense avoir retiré de la sensibilisation dont il a fait l'objet. Estime-t-il notamment que celle-ci a un rapport direct avec son travail ? En mettant l'accent sur la responsabilité individuelle des utilisateurs dans leur quotidien, les actions de sensibilisation parviennent à provoquer de saines réactions.

B
ARTICLE 09

Réseaux énergétiques : comment assurer la sécurité du producteur au consommateur ?

Intervenants :
- Bertrand GARÉ – L'informaticien – Rédacteur en Chef
- Patrick BALDIT – CEA – Chef du service des technologies de l'information et de la communication,
- Louis MARINOS – ENISA – Senior Risk Management,
- Ayhan YILDIZ – Erdf,
- Josyane LOURDIN – INEO – Directeur projets avant vente,
- Thierry CORNU – Sogeti – Responsable offre cybersécurité industrielle d'Euriware.

Résumé des interventions :
Les réseaux intelligents ou smart grids apportent des avantages en termes de pilotage et d'efficience de l'outil industriel. Toutefois, leur mise en œuvre se révèle très complexe pour assurer le contrôle, la sécurité et la sûreté du système industriel. En ce sens, la détection de vers informatiques tels Stuxnet, le plus connu d'entre eux, a davantage fait prendre conscience de la nécessité de sécuriser de manière optimale les systèmes de contrôle et d'acquisition des données (SCADA).

I – État des lieux et contraintes propres à l'industrie

Les SCADA posent des problématiques en termes de sûreté et de sécurité. Pour les surmonter, il faut opérer une véritable défense dans la profondeur, c'est-à-dire installer des systèmes de sécurité qui s'orientent de l'extérieur vers l'intérieur. La pose de sondes et de diodes sur les réseaux énergétiques permet de palier les problématiques de sécurité et de sûreté liées aux SCADA. Il s'agit de mettre en place un réseau de cybersécurité au-dessus du système industriel, les diodes assurant un rôle d'interface. Deux autres problématiques se posent, celle de la sécurisation d'automates parfois âgés de 20 ans, en parfait état de fonctionnement, mais aussi celle des prochains équipements, en collaboration avec les industriels. La progression en terme de sécurisation n'est pas la même selon les secteurs d'activité, en raison de la complexité des infrastructures industrielles existantes. Les nouvelles installations industrielles confient la responsabilité de la sécurité des sys-

tèmes industriels à la Direction des Systèmes d'information (DSI) ou à la Direction Industrielle (DI).
Il est difficile sur le plan technologique de procéder au chiffrement des données dans les systèmes industriels qui exigent des automates une réactivité de l'instant pour des raisons de sûreté. En effet, les opérations de déchiffrement créent des temps de latence trop longs pour un réseau industriel. La réflexion s'orienterait davantage vers l'usage d'une solution certifiée. Cette certification authentifierait le poste informatique à l'origine de l'envoi d'une information au bon automate. Cette solution apparaît davantage conforme aux contraintes techniques que le chiffrement de bout en bout.

II – La notion de défense en profondeur

Nous pouvons la définir comme une démarche de compartimentation interne au réseau industriel.
Toutes les entrées possibles du système et les postes de travail sont à protéger pour empêcher l'intrusion de virus. Les mesures de protection, impossibles à garantir à 100 %, doivent être complétées par un logiciel de détection qui soit en mesure de signaler rapidement toute intrusion ou tentative d'intrusion. Le système de défense en profondeur fonctionne sur plusieurs couches dirigées par un système de supervision. Le principe de défense en profondeur se traduit ainsi par une architecture en couches dite « système d'oignon » : les moins sensibles en périphérie, les plus sensibles au centre, puis graduellement des systèmes intermédiaires dans des couches au milieu. Pour compléter cette défense en profondeur, l'analyse des logs semble déterminante pour détecter les éventuelles entrées malveillantes. Au final, la notion de défense en profondeur dépasse largement l'antivirus installé sur les PC. L'installation de sondes aura pour objet de procéder à un maillage à grande échelle pour détecter les comportements anormaux : dérouter du flux électrique vers un point donné pour le neutraliser, détecter les faux-positifs et leurres... Nous voyons bien que les sondes et diodes sont déterminantes dans cette notion de défense en profondeur. Ces matériels devraient être plus facilement accessibles sur le plan financier pour les PME / PMI en raison de la plus grande vulnérabilité de ces dernières. Pour mémoire, la prise en compte de tous les aspects sécurité oscille entre 15 et 20 % des prix en fonction des prix globaux (ex : cas des compteurs Linky).

III – La présence des prestataires extérieurs

Les prestataires qui interviennent sur toutes les installations des grands opérateurs de réseaux énergétiques se doivent d'être des opérateurs de confiance. À cet effet, l'Agence Nationale des Systèmes d'Information (ANSSI) met en place des processus de labellisation de confiance à destination des prestataires en charge de la maintenance des systèmes d'information sur une emprise industrielle. Toutefois, le prestataire extérieur qui intervient sur l'ensemble des systèmes d'information d'une grande entreprise voit son périmètre s'arrêter aux passerelles qui relient l'informatique d'entreprise à l'informatique industrielle.
Les prestataires extérieurs doivent être contrôlés pour s'assurer qu'ils respectent les préconisations de l'ANSSI en matière d'hygiène informatique. Dans le prolongement du contrôle du prestataire extérieur, le choix de la maintenance sur site ou à distance par ce dernier est à prendre aussi en considération. Un arbitrage est à faire au cas par cas en termes de coût / sécurité, sachant que la probabilité du risque augmente à mesure que le nombre d'interventions s'effectue à distance.
Il convient de souligner le cas particulier du réseau Linky. ERDF a dû tenir compte des

compteurs électriques Linky implantés dans les domiciles des particuliers. Sur ce cas précis de compteurs pilotables à distance, l'opérateur, pour sécuriser au mieux le réseau de distribution, a décidé de fournir les outils ad hoc de maintenance aux entreprises agréés. En outre, la chaîne Linky dispose d'une chaîne sécurisée par l'apport de logiciels déportés.

Le prochain défi qui attendra les industriels est de réussir à intégrer à la fois leur système avec un système externalisé. Il s'agira pour eux de gérer les opérations quotidiennes et la sécurité d'un système d'intégration de type cloud privé ou hybride hébergé ailleurs.

ARTICLE A 10

Prévenir et détecter les fuites d'information, une illusion ?

Résumé des interventions :
Le Cloud s'est considérablement développé ces dernières années. Il présente bien des intérêts en terme de facilité pour les entreprises et de réduction des coûts. Cependant, le Cloud a rapidement laissé la place à de nombreuses craintes quant à la sécurisation des données qu'il contient. L'accès au Cloud étant peu coûteux, les entreprises ont trop souvent tendance à négliger la question sécuritaire. Compte-tenu des enjeux, une démarche de responsabilisation des entreprises doit être menée.

Le terme de Cloud recouvre un grand nombre d'aspects différents. Le plus souvent, on fait référence aux données et applications qui y sont stockées.

Les usages du Cloud:
Le Cloud regroupe des technologies de filtrage et de sécurisation partout à travers le Monde. Ce développement permet aux différentes filiales à distance d'avoir accès à Internet en local de là où elles sont, le tout sans avoir à passer par un réseau privé ; de pouvoir protéger un utilisateur partout où il se trouve ; de protéger les applications placées dans le Cloud ; d'améliorer la qualité du filtrage ; et d'obtenir une visibilité plus globale sur l'entreprise.
Le « nuage » contribue à une réduction des coûts ainsi qu'à une meilleure adaptabilité des systèmes d'informations. De même, la réactivité des entreprises s'en voit améliorée.
Mais en parallèle de ces avantages, un frein majeur apparaît : la question de la sécurisation des accès et des données, notamment lorsque le Cloud se situe à l'étranger. La pratique d'un chiffrement maîtrisé est alors une des solutions envisageables.

Intervenants :
- Sergio LOUREIRO, CEO and co-Founder, SecludIT
- Damien BANCAL, Rédacteur en chef, Zataz
- Gaël KERGOT, Directeur Commercial pour l'Europe du Sud, CypherCloud
- Jean-Nicolas PIOTROWSKI, Président fondateur, Itrust
- Frédéric BENICHOU, Directeur Europe du Sud, Zscaler
- Lionel FEREMBACH, Product Line Manager HySIO : Infogérance, Cloud et Cybersécurité, Thalès

L'évolution du Cloud, l'exemple du groupe Thalès :
Dans le cadre de ses activités d'infogérance, Thalès a eu, dès 2008, l'occasion de réfléchir à l'intégration d'une offre de Cloud pour ses clients. Le groupe a cherché à développer les fonctions de sécurité propres à ses Clouds en misant sur des solutions à base d'open source. Maîtrisant alors au mieux sa plate-forme, Thalès a été à même de conclure des engagements forts auprès de ses clients à la fois en terme de disponibilité, de performance et de sécurité.
Il faudra cependant prendre en compte les différences de sensibilité des informations. Il conviendra d'effectuer le chiffrement adéquat, en évitant les impacts fonctionnels sur les applications.

Les bénéfices et la sécurité du Cloud auprès des entreprises :
Face aux différentes menaces existantes, le chiffrement du Cloud s'impose aujourd'hui comme une nécessité pour les entreprises. Il demeure malgré tout coûteux.
La sécurité n'est en effet pas la même qu'à l'intérieur de l'entreprise. Mais l'optimisation des coûts étant légion, certains Clouds présentent des niveaux de sécurité extrêmement faibles. Cette frénésie du rendement nuit à la sécurité. Les bonnes pratiques doivent donc être appliquées rapidement. En effet, la majorité des systèmes de stockage en ligne présentent une perméabilité inquiétante.
A cela s'ajoute le cas du Wifi public qui se révèle être encore moins sécurisé.
Les spécialistes parlent d'une « disparition du périmètre ». Auparavant, les données demeuraient au sein de l'entreprise et étaient plus facilement sécurisables. Or aujourd'hui, les données et les utilisateurs sont de plus en plus mobiles. De plus, certaines entreprises insèrent parfois dans le Cloud des informations très confidentielles. Tout cela contribue à la disparition dudit périmètre de sécurité.
Il convient alors de différencier la sécurisation de l'accès au Cloud, du réseau, du contenant et également du contenu du Cloud. La sécurisation du contenu, à savoir des données comprises dans les applications, est une solution.
Malgré l'existence de ces craintes, le Cloud s'impose désormais comme un backup indispensable pour les entreprises.
Il convient, en outre, d'accompagner davantage les entreprises cherchant à souscrire au Cloud. Cela permettra en amont d'effectuer des études de sécurité.

Pour ce qui est du Cloud public, il a le plus souvent vocation à être le plus standard et le moins cher possible. Dès lors, les niveaux de sécurité vont de pair. Le plus important est de sécuriser correctement les applications avant de les placer dans le Cloud. On parle ici de « défense en profondeur », du fait de sécuriser l'application dès sa création. Le chiffrement n'étant pas toujours aisé, il va de soi que les données critiques, confidentielles, n'ont pas leur place au sein d'un Cloud public. Un Cloud privé confié à un infogérant sera plus adapté.
Toute une politique de sensibilisation sur ces questions doit donc être menée dans les entreprises.

L'intérêt du chiffrement des données :
A l'heure actuelle, les Clouds publics ont un coût de revient assez bas. Le chiffrement représente un surcoût qui peut cependant se révéler rapidement rentable s'il est choisi avec soin. L'entreprise doit alors nécessairement effectuer une équation. En effet, plus de la moitié des entreprises ne sécurisent pas la sauvegarde placée dans le Cloud. Pour autant, les études révèlent que la majorité des entreprises ayant subi une perte majeure de leurs données ont été conduites à la fermeture, d'où l'intérêt du chiffrement.

Les fonctions de sécurité se voient de plus en plus déportées

dans le Cloud. Pour rappel, l'établissement du Patriot Act permet au FBI de collecter, librement et si nécessaire, l'ensemble des données émanant d'une technologie américaine. Dès lors, la sécurisation des données ne dépend plus du lieu de leur hébergement. Ce n'est donc pas parce qu'il est situé en France que le Cloud sera pour autant souverain. A cette fin, il devra regrouper uniquement des produits labellisés par l'ANSSI ou des produits européens. Mais dans certains cas, la législation américaine sera à même de passer au-dessus de la législation européenne.

Conclusion :
On se situe aujourd'hui dans un modèle d'entreprise étendue : le Cloud. Depuis environ cinq ans, un nouveau paradigme de sécurité est apparu. Il ne s'agit plus d'une défense périmétrique mais davantage d'une défense en profondeur. On se réfère alors à des technologies de supervision.
Les systèmes de protection comprennent des failles tandis que les budgets de sécurité n'évoluent pas.
Face à ces problématiques, il y a dans la plupart des cas des remèdes. Le chiffrement en fait partie.
En somme, la supervision apparaît plus que jamais nécessaire afin d'être à même de détecter les attaques et d'y répondre. Sur ce point, l'ANSSI tente régulièrement de présenter de nouvelles solutions.

B
ARTICLE 11

Règlement européen sur la protection des données personnelles quelles conséquences ?

Animateur :
- Stéphane CHOISEZ : Avocat - Aslani & associés
- Sébastien GAMBS : Chercheur sur la Sécurité des Systèmes d'Information - Université de Rennes 1 et Inria
- Garance MATHIAS : Avocate - Cabinet Mathias, propriété intellectuelle et industrielle et protection des données
- Olivier MESNARD : services de lutte contre la Fraude, EY France
- Laure ZICRY : Cyber Risks Practice Leader - Gras Savoye

Résumé des interventions :
Le règlement européen prévu pour 2015 répond à la multiplication des traitements de données personnelles et à la nécessaire protection de la vie privée de chacun. Toute personne devra désormais être informée de façon intelligible sur ses données personnelles inventoriées afin de pouvoir agir en connaissance de cause, notamment en cas de faille informatique.
Pour assurer cette transition technologique, juridique et éthique, les entreprises devront recruter des Data Protection Officers (DPO) aux responsabilités plus larges que les CIL. La responsabilité est élargie à tous les acteurs de la chaîne, entreprises responsables du traitement, sous-traitant et DPO. De nouvelles polices d'assurance intègrent les coûts générés par l'obligation de la notification.

En octobre 2013, la commission des libertés civiles de l'UE a voté une révision des règles actuelles sur la protection des données dans l'Union Européenne afin de renforcer le contrôle des citoyens sur leurs données personnelles et d'accroître la protection des données traitées par les autorités policières et judiciaires. Les négociations tripartites entre le Parlement, le Conseil et la Commission en vue de conclure un accord final sur le nouveau règlement européen devraient débuter en juin 2015. Celui-ci remplacera les diverses législations nationales par un ensemble unique de règles. Ces nouvelles dispositions devraient permettre aux entreprises de travailler plus facilement au-delà des frontières, en assurant que les mêmes règles s'appliquent dans tous les États membres.

Droits individuels sur les données personnelles

L'exercice du contrôle de chacun sur ses données personnelles n'est réalisable que si il est possible de donner son consentement éclairé. Chaque citoyen devra être donc informé de façon intelligible (langue, style) de la collecte de ses données à caractère personnel et de la durée pendant lesquelles celles-ci seront conservées.

La maîtrise des données personnelles s'accompagne du droit d'y accéder, de les rectifier ou de les effacer (droit à l'oubli) et de s'opposer au profilage. Chacun doit être en mesure de déposer une réclamation auprès de l'autorité de protection des données compétente, d'engager une action en justice et obtenir réparation. Enfin le Conseil doit définir les conditions qui permettront la portabilité de ces données.

L'obligation de la notification systématique et individuelle en cas de faille informatique est un élément clé. Celle-ci devra apporter les informations nécessaires et pratiques permettant à la victime de prendre les dispositions nécessaires. Le règlement prévoit en particulier que cette notification devra indiquer l'identité du Data protection officer (DPO) pour qu'il puisse être contacté, les donnée clairement identifiées et l'action à prévoir. Deux notifications sont prévue, celle aux autorités de contrôle et une autre destinée aux personnes concernées

Accès aux données personnelles et effacement virtuelles des frontières nationales

En cas de failles de données, les réseaux informatiques en démultiplient les conséquences. Lors de la détection et de la recherche de fraudes, les opérateurs vont avoir accès à de nombreuses données. En effet, la collecte d'informations portera sur les données de gestion, le croisement de fichiers, l'exploitation des boites mails, les données bureautiques, les logs. Par ailleurs, les investigations porteront sur de nombreuses données territoriales induites par l'internationalisation économique. Les enquêteurs devront considérer la répartition des systèmes par pays, la localisation de la maison mère inter ou extra communautaire, la nationalités des travailleurs et des victimes. Force est de constater que le traitement législatif devient toujours plus complexe.

Délégation du traitement de l'information et permanence de la responsabilité

La pratique d'externalisation est courante. L'article 77 du futur règlement dispose que les responsables du traitement et les sous-traitants qui y participent deviennent solidairement responsables. En aucun cas le transfert de risque ne veut dire transfert de responsabilité. Si le sous-traitant ne respecte pas les instructions du responsable du traitement, alors ce dernier sera considéré comme responsable conjoint et encourra les mêmes sanctions. L'externalisation ou la délégation n'exonèrent en rien les entreprises donneuses d'ordre de produire la documentation nécessaire à l'identification des données personnelles. L'article 28 de la proposition de règlement du parlement européen stipule en effet que tous les responsables du traitement et les sous-traitants conservent une trace documentaire de tous les traitements effectués sous leur responsabilité. Ces informations reprennent les systèmes mis en œuvre et l'analyse d'impact1. Cette obligation de traçabilité documentaire générera un cumul des données auprès de chaque acteur.

Des évolutions contractuelles et professionnelles

Le règlement introduit deux concepts importants : celui de la protection de la vie privée dès la conception (privacy by design)2 et celui de la protection de la vie privée par défaut (privacy by default)3. Pour respecter ces deux obligations les entreprises devront désigner un DPO qui

remplacera au sein des entreprises le Correspondant informatique et Liberté (CIL). Ses compétences sont élargies à tous les aspects de la conformité de traitement de données à caractère personnel, dès la conception de celui-ci. Il sera aussi le maître d'œuvre de nouveaux rapports au sein des entreprises. Par ailleurs, en cas de failles informatiques, c'est sa propre responsabilité civile qui sera engagée.
Au-delà de l'impact sur leur chiffre d'affaires annuel et de leur image de marque, les sanctions prévues à l'encontre des entreprises pourront aller jusqu'à 100 millions d'euros ou l'équivalent de 5% de leur chiffre d'affaires annuel mondial. C'est pourquoi les assurances proposent désormais des polices intégrant tous les coûts de gestion de la crise (cabinet d'avocat qui va rédiger la lettre de notification, mesures prises pour combler la faille, messagerie, services, défense devant l'autorité de contrôle qui va diligenter une enquête...). Certaines assurances proposent même la gestion de crise externalisée et la coordination de l'ensemble des intervenants.

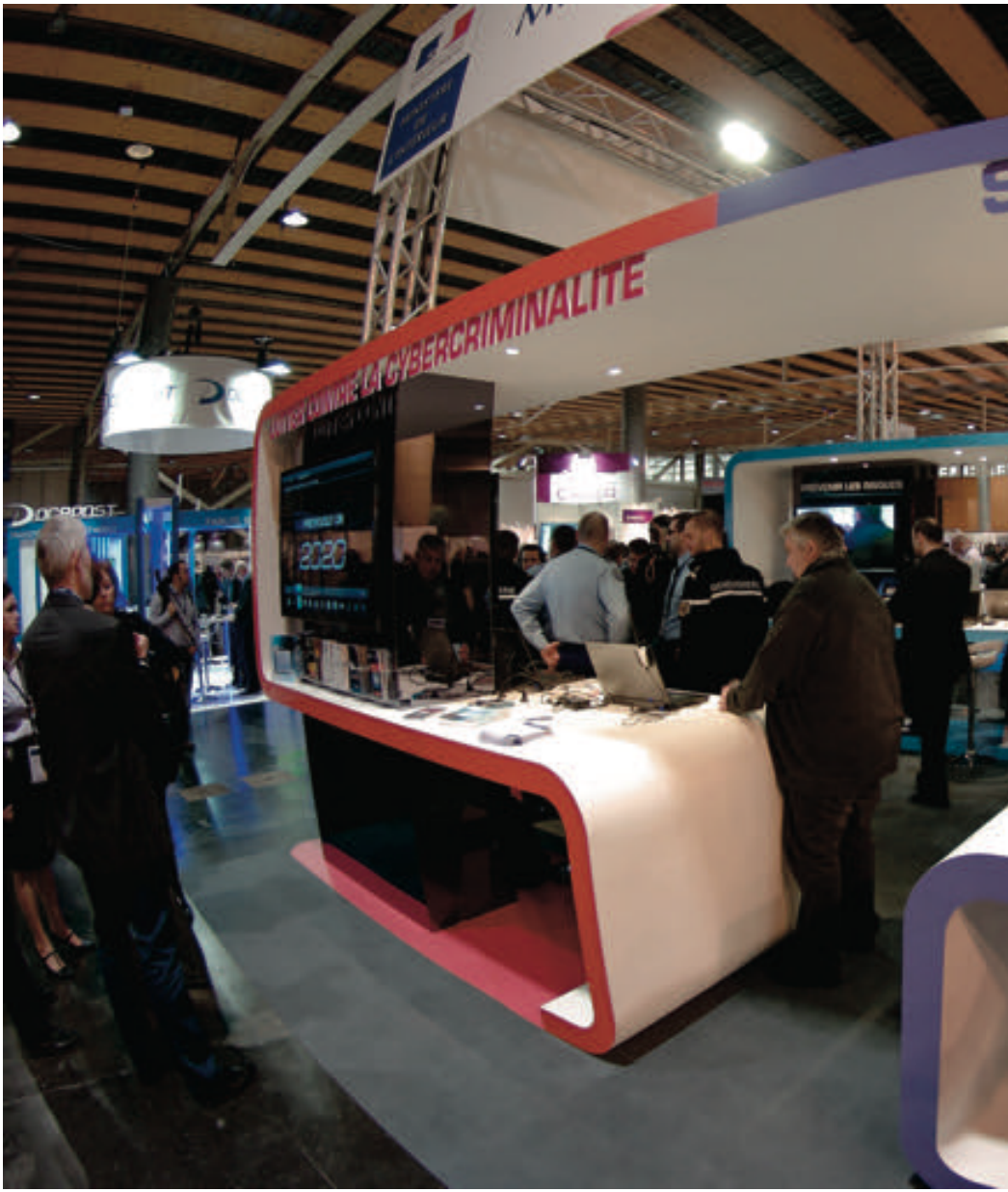
Conclusion :
Des questions restent en suspens notamment s'agissant de l'articulation de l'obligation de notification de la clause de confidentialité pour certaines entreprises ou encore de la protection de données sensibles. Comment trouver le bon rapport entre le règlement européen et des réglementations entreprises ?
Le système de prévention par l'obligation d'une notification systématique et individuelle est une bonne chose. Mais celui-ci devrait-être déclenché dès la perte du moindre support (comme une clé USB). Le coût pour les entreprises de cette mesure n'est pas estimé. Afin de réduire ces dépenses, il pourrait être envisageable de minimiser les fuites en ciblant le minimum d'informations nécessaires.

Glossaire :

1 L'analyse d'impact ou système d'analyse de risques à réaliser en interne remplacerait les procédures actuelles à base de formalité administratives préalables auprès de l'Autorité de protection des données.

2 La protection de la vie privée dès la conception vise à agir de manière proactive et préventive, avant qu'une nouvelle technologie n'entraîne de nombreuses violations de la protection des données.

3 Quiconque traite de données personnelles doit garantir par défaut le plus haut niveau possible de protection de ces données aux personnes concernées.


CYBERCRIMINALITE
2020

B
ARTICLE 12

Le coût réel de la cybercriminalité ?

Intervenants :
- Alain ESTABLIER, rédacteur en chef, Security Defense Business Review
- Dominique LOISELET, Sales Director France and North Africa, Blue Coat
- Yann LEBORGNE, Security Engineer Manager, CISCO
- Alain BOUILLE, président du CESIN
- Alvaro Alexander Soto, CEO, Digital Forensics and Security Laboratory
- Alexis CAURETTE, Head of Cyberdefense, Information Security Consulting and Audit, Bull

Résumé des interventions :
Le coût réel de la cybercriminalité est difficile à évaluer. Toute entreprise victime de cybercriminalité n'est pas automatiquement consciente de l'attaque. Lorsqu'elle l'est, l'entreprise communique rarement sur le sujet en raison du risque de perte de crédibilité afférant à la sécurité.
Ce facteur est prédominant dans la difficulté à évaluer le coût réel. Cependant, des évaluations sont possibles et laissent entrevoir un marché gigantesque de près de 445 milliards de dollars par an. Le montant du préjudice inquiète les assurances, les entreprises, mais aussi l'État car au-delà des aspects financiers, ce sont des emplois qui sont menacés.

L'évaluation du coût d'une cyberattaque est une chose ardue. Un certain nombre de facteurs rentrent en jeu comme le coût de remise en service, l'assurance, ou simplement le fait de savoir que l'on a été attaqué.
Voulant se prémunir contre ce risque, l'entreprise peut décider de s'assurer. Apparaissent alors d'autres questions, comme la nature des prestations possibles, ou l'évaluation du préjudice.

1- Une difficile évaluation

Selon les estimations, le coût réel de la cybercriminalité varie de 375 à 575 milliards de dollars. La Société McAfee table sur 445 milliards de dollars. Dès lors, on peut se demander quelles sont les causes d'une telle variation ?
Il existe trois types de menaces dominantes : les menaces de type mafieux, celles émanant des hackivistes et celles relevant du cyberespionnage. La menace mafieuse

est difficile à estimer. L'activité des hacktivistes a un coût relativement faible car elle se limite souvent au défaçage de sites. Concernant le cyberespionnage, l'estimation ne repose que sur des extrapolations.
De plus, les coûts peuvent être évalués à court terme ou à long terme. Le piratage de cartes bancaires est un bon exemple de coût à court terme, alors qu'une mauvaise publicité ou une image dévaluée aura un impact peut-être plus tardif mais également plus conséquent et difficilement évaluable.
La cybercriminalité occasionne aussi des coûts indirects sur la victime bien évidemment, mais également sur les banques et les assureurs. A cela s'ajoute le coût de remise en service du système.
Le coût d'impact réel est lui aussi difficile à évaluer, en raison du fait que les entreprises ne sont parfois pas conscientes d'en être victimes. Lorsque l'on sait que l'impact financier est inversement proportionnel à la visibilité de l'attaque, il est aisément possible de comprendre la difficulté à estimer le coût total de la cybercriminalité ainsi que la disparité des estimations.
A cela s'ajoutent encore les coûts relatifs à la mise en place des systèmes de protection, et ceux concernant les levées de doute. De fait, combien dépense-t-on pour la création de sécurité ? Il ne faut pas minimiser la portée et l'impact potentiels des attaques. Cependant le problème de la non-détection des attaques rend difficile l'évaluation d'un ROI (Return Of Investment, retour sur investissement) en la matière.
Les assurances occupent donc un rôle majeur pour les entreprises afin de les garantir contre les pertes financières dues à ces attaques.

2- Comment s'assurer et pourquoi?

Les assureurs ont bien pris en compte les risques liés à la cybercriminalité. L'entreprise transfert ainsi le risque résiduel à l'assureur. Or, l'estimation du patrimoine immatériel de l'entreprise se trouve au cœur de cette problématique de l'assurance.
Ainsi, deux questions principales font leur apparition. Quelle est la valeur de la donnée ? Quelle est la masse exacte de données perdues?
Le dédommagement de l'entreprise se fait en fonction de ces deux paramètres. Mais la difficulté de leur évaluation demeure problématique. L'autre inconnue est de savoir le prix auquel un secret de fabrication peut être estimé. De même, comment l'évaluer sans en révéler la portée (et la nature) à l'assureur ?
Enfin, et en dernier lieu, la perte d'exploitation n'est pour l'instant pas remboursée par les assurances. Cependant, cela sera peut-être le cas dans le futur. C'est une des pistes envisagées par les acteurs majeurs de la profession.

3- Une vision différente de l'assurance

La conception de l'assureur est différente aux États-Unis et en Europe. Cela influe sur la façon dont il effectue ses prestations. Outre-Atlantique, les assurances se cantonnent au rôle de prestataires de remboursement. En effet, le risque est évalué en fonction des protections mises en place. Le coût du transfert du risque résiduel, lié à la cybercriminalité, est chiffré. Le cas échéant, l'entreprise est remboursée pour le dommage.
En Europe, il en va différemment. En effet, l'assureur effectue ce travail mais fournit également d'autres services. Il accompagne l'entreprise dans le sinistre, par exemple en fournissant une expertise en matière de police technique et scientifique cyber, mais également en termes de conseils.
Il faut cependant garder à l'esprit que, bien que la déclaration d'une attaque soit obligatoire, il demeure que 90 % de ces attaques restent masquées et non quantifiables.

B
ARTICLE 13

Comment améliorer la sécurité du code ?

Intervenants :
Vincent CASSE, Full-stack developer, OVH.
Rodolphe ROBERT, Responsable sécurité des projets et applications, AREVA.
Yann SERRA, Grand reporter, L'informaticien.

Résumé des interventions :
Les applications, si elles ne sont pas sécurisées, offrent des points d'accès pour les hackers. Il est donc nécessaire d'exiger des fournisseurs des standards de sécurité. S'agissant des développeurs, il est nécessaire de prendre en compte la sécurité au moment de la programmation pour éviter d'avoir à revenir ultérieurement combler des failles.

Les risques pesant sur les codes

Areva est soumis à énormément de réglementations et, en tant qu'opérateur d'importance vitale (OIV), à des obligations fortes de la part de l'ANSSI en matière de sécurisation des applications. Certaines sont en effet très critiques. Areva doit renforcer la sécurité de ses systèmes d'informations et notamment sur la partie « applicatifs ». Elle doit être en mesure de prouver à l'ANSSI que les normes sont respectées dans ce domaine. Areva ne fait pas de code et sous-traite ces questions. L'entreprise demande au développeur de démontrer qu'il n'y pas de faille dans leur process, notamment par des audits de code. OVH, quant à lui, produit du code. La sécurité de ce dernier fait partie de son travail. La gestion du risque est forcément différente que pour une entreprise qui touche au nucléaire. En revanche, il est nécessaire de sécuriser le code vis-à-vis du client.
Chez Areva toute la sécurité est conditionnée par des analyses de risque (une sécurité au juste besoin). Toutes les applications n'ont

pas la même criticité. Les efforts de sécurisation ne sont donc pas les mêmes selon les applications. Il y a une gradation dans l'effort consacré à éradiquer les failles suivant la sensibilité de l'application. La sécurisation existe cependant toujours. Certaines applications ont une durée de vie longue, il faut assurer le même niveau de sécurisation dans le temps.

Il existe un panel très large de failles de sécurité. Certaines failles sont plus récurrentes. Par exemple, on va trouver des failles d'injection en tous genres assez régulièrement. Dans le web, il y a un échange des deux cotés. L'utilisateur va pouvoir fournir des éléments. Les éléments d'échange peuvent avoir potentiellement des failles. Il y a énormément de développement sur java script et on voit également beaucoup d'attaque sur ce système. C'est une technologie ancienne mais qui connaît toujours ce type d'attaques. Ces attaques pourtant très connues restent possibles car certains développeurs ne visualisent pas tous les risques. Dans d'autres cas, on doit agir sur des codes que l'on ne connaît pas forcément et que l'on ne maîtrise pas entièrement. Il est alors possible que le développeur oublie des détails ou pense que des sécurités existent déjà (alors que ce n'est pas exact).

S'agissant des anciennes applications, certaines s'appuient sur des langages quasi disparus, en tout cas inconnus des jeunes hackers. Bien souvent, ces systèmes sont plutôt étanches, sans connexions vers l'extérieur. Pour les développeurs, il est très dur de comprendre du code qui est devenu ancien. La meilleur façon de faire est de documenter la programmation du code (dire à quoi correspond chaque ligne de code). En automatisant des tests, on est en mesure de voir si les modifications ont cassé quelque chose à l'application. Il est également utile d'avoir une personne qui a une vision globale du code.

Certains codes anciens fonctionnent parfois mieux que des choses plus récentes. C'est le cas par exemple dans le système bancaire où des codes ont été créés par des personnels qui étaient des banquiers. Pour les entreprises, on est parfois contraint de maintenir des applications alors même que plus personne ne connaît les codes. Changer ces applications anciennes doit faire l'objet d'une réflexion préalable car cela coûte cher et nécessite des délais. En tout cas on ne peut pas faire du « quick and dirty » dans une entreprise comme Areva.

Chez OVH, la sécurité est le point le plus important. Si il y a une faille, il va falloir y revenir lors de la maintenance et au final cela reviendra plus cher que de la réparer dès la programmation. La sécurité, quoi qu'il en soit, nécessite du temps, et donc de l'argent.

La prévention, une tâche essentielle mais complexe

Chez Areva, on met sous supervision les applications sensibles via un SOC (Security Operation Center). On surveille en temps réel et on est ainsi informé lorsqu'un comportement suspect a été détecté. Cela suppose des outils mais aussi des personnels. Il est également nécessaire de se concentrer sur les applications les plus importantes. Le monitoring « basique » est externalisé et il existe une équipe dédiée d'experts au sein de l'entreprise.

Selon OVH, la meilleur astuce est de découper le code de manière restreinte de façon à que chaque morceau de code n'accède pas à tout. Si on travaille sur le web, on peut faire du monitoring, qui est très efficace. Il existe également des logiciels qui vont indiquer les différents pics de connections sur certains fichiers qui devraient être privés. Areva évite d'utiliser des codes en open source car on n'en connaît pas la provenance et parce qu'il y a des problématiques de maintenabilité derrière. Si les prestataires utilisent des codes open source, il leur est demandé de les tester et de prouver que l'application livrée est

exempt de vulnérabilité. Les fournisseurs, parfois, négligent de le signaler qu'ils utilisent des composants open source.

Chez OVH en revanche, l'open source est très utilisée. Les codes open source permettent de pouvoir lire le code et de s'assurer qu'il n'y a pas de soucis, notamment de vérifier que des back doors n'existent pas. Des audits sont également faits pour s'en assurer.

Pour éviter le retro-engineering, il est éventuellement possible de complexifier le code. Pour autant, le souci est qu'il y aura toujours quelqu'un pour aller voir ce que le processeur fait et comprendre le code. C'est donc une perte de temps car cela n'offre pas de garantie de protection. Un hacker motivé finira par comprendre le code et trouvera une faille. Le point le plus important est d'être conscient que l'on peut avoir des failles dans un système et donc il faut que la conséquence de ces failles soit minime.

Des efforts sont faits par les développeurs pour sécuriser le code et éviter les failles. Pour autant, l'interconnexion est désormais mondiale et les attaques peuvent venir de partout : le nombre d'assaillants potentiel est d'autant plus important que les accès à internet se développent dans le monde. Il est donc de plus en plus important de sécuriser les applications.


7ÈME FORUM INTERNATIONAL
DE LA CYBERSÉCURITÉ
20 ET 21 JANVIER 2015
LILLE GRAND PALAIS

B
ARTICLE 14

Mobilité et sécurité : Peut-on trouver un équilibre ?

Intervenants :
- Pierre LUBET – Altana – Avocat associé,
- Patrick CHAMBERT – C2S – Groupe Bouygues – RSSI / Responsable du centre de sécurité groupe,
- Xavier DE KORSAK – Harmonie Technologie – Directeur opérationnel,
- Sébastien LAURENS – Société Générale – Architecture Anel, Infrastructure Security Leader
- Daniel FAGES – Stormshield – VP Engineering
- Frédéric ZINK – Orange cyberdéfense – Directeur de l'activité « infrastrucutre et mobilité »

Résumé des interventions :
Thème devenu central à l'ère de la mobilité des salariés tant physique que numérique, cette table ronde a pour objet de sensibiliser les dirigeants sur les choix qu'ils sont amenés à faire pour d'une part assurer la sécurité de leur système d'information et d'autre part préserver la capacité d'innovation de leurs collaborateurs. En effet, ces dernières années est apparue une évolution majeure dans le domaine de la mobilité interne. Managers et salariés veulent embarquer certains éléments, accéder à différents systèmes d'information de l'entreprise. La problématique ne se résume pas au BYOD (bring your own device) ni au COPE (Corporate Owned, Personally Enabled). Le collaborateur bridé dans son action par des applications sécurisées sera tenté d'utiliser son propre appareil à des fins professionnelles. Une enquête récente démontre que 63 % des utilisateurs mêleraient des applications personnelles et professionnelles dans leur propre appareil. Il devient nécessaire de réfléchir d'une manière plus globale en prenant comme fil directeur la sécurisation de l'envoi des DATA.

I. État des lieux de la sécurité

Des études menées sur le long terme montrent que 80 % des failles de sécurité proviendraient d'une négligence des salariés. Ainsi, les outils de travail des collaborateurs sont souvent pénétrés par des hackers dans le but de perpétrer des actes de malveillance. La mobilité conduit à revoir la notion de périmètre de sécurité. Avant la mobilité, il existait des bastions pour sécuriser un lieu ou une information. Nous assistons maintenant à une décentralisation du périmètre de sécurité. De nos jours, l'informa-

tion doit pouvoir circuler en sécurisant son environnement. Dans le catalogue des données à sécuriser figurent les SMS et la voix. La pratique montre que le téléphone sécurisé est désuet car il n'est pas en mesure de répondre à l'usage courant de son utilisateur. Il arrive que ce type de téléphone soit purement et simplement mis de côté par le salarié qui, pour des raisons d'efficacité et de souplesse, aura recours à un système personnel ou à une solution détournée. L'usage se confond ainsi avec l'application, comme par exemple la capacité de surfer sur le Net et d'envoyer des tweets. Les fabricants des terminaux et smartphones ont voulu sécuriser ces produits sans donner la faculté aux usagers de personnaliser les mesures de protection. L'arrivée massive de nouveaux terminaux constitue donc un challenge pour les sociétés en charge du développement des solutions de protection et de sécurité. Jusqu'à présent, la sécurisation des ordinateurs portables fonctionnait uniquement dans le système Windows. Les nouveaux terminaux et systèmes d'exploitation introduisent davantage de complexité. Au final, la posture sécurité devrait être plutôt orientée vers la la protection de la donnée, de l'information que de l'appareil en tant que tel.

II. La confusion des genres

La distinction entre les terminaux professionnel et personnel a pour objet de séparer les sphères professionnelles et privées. Toutefois, il est difficile de s'opposer aux demandes des utilisateurs, surtout des décideurs, qui souhaitent accéder à ces deux sphères sur un même appareil tout en bénéficiant d'un niveau de sécurité maximal. La présence côte-à-côte de données personnelles et professionnelles sur des terminaux (smart phone, portables…) implique des conséquences d'ordre juridique. Ce mélange des genres pose toute une série de questions : qu'est-ce-que l'entreprise s'interdit de surveiller ? De sauvegarder sur le plan personnel ? Les BYOD ont suscité au début un vif succès.

Actuellement, il est constaté de la part des salariés une préférence pour l'emploi d'un terminal professionnel. Bon nombre d'entre eux ont pris conscience que des éléments de nature intrusive installés sur leur téléphone privé permettaient d'accéder à des informations personnelles. De réelles problématiques sont posées en matière de data privacy.

III. Les stratégies de sécurisation

Il est préconisé de ne pas sécuriser uniquement les solutions pour Mobile Device Management (MDM) tels que les accès à l'entreprise. À ce titre, les portails d'accès ne sont accessibles que par certaines applications que l'entreprise aura préalablement remises aux salariés. Il s'avère tout autant contre-productif de compliquer l'usage de l'appareil au risque que l'intéressé utilise en sous-main d'autres moyens. Le chef d'entreprise doit aussi réfléchir, dans sa stratégie de sécurisation, au périmètre d'accès de ses collaborateurs en fondant ses choix sur l'emploi occupé et la place dans la hiérarchie. S'agissant de l'aspect mobilité et de la sécurisation, la gestion de la flotte des téléphones mobiles nécessite des solutions adaptées à la sécurité périmétrique de l'entreprise.

B
ARTICLE 16

Cyberdéfense « as à service », avenir de la sécurité

Animateur :
Michel Picot, journaliste, BFM Business
Intervenants :
Alain Bouillé, président du CESIN
Bruno Brocheton, vice-président du CIGREF
Jacques Marzin, directeur de la DISIC
Michel Van Den Berghe, directeur général de Orange Cyberdefense,
Loïc Guezo, directeur du développement chez Trend Micro

Résumé des interventions :
La cyberdéfense peut être définie comme le processus métier qui s'appuie sur la prévention, la détection et la réaction. Dans une entreprise, l'externalisation (outsourcing, en anglais) des services de cyberdéfense est devenue incontournable. Ces services s'articulent autour de conseils, d'intégration et de gestion de services. Ce « business model » repose sur une offre qui se veut de plus en plus globale et personnalisée pour répondre à une demande de clients qui doivent cependant conserver les aspects stratégiques de leur gouvernance.

I – La confiance et la transparence comme base de l'offre de service

Au-delà de toute offre technique au profit d'un client, il s'agit de prime abord d'instaurer une confiance entre les deux parties. Cette confiance, naissant de l'échange, permet une personnalisation de l'offre avec un processus et un outillage adaptés aux clients. Bien entendu, le fournisseur de solutions offre des compétences et un cadre juridique qui permettent de gagner en réactivité par rapport à l'évolution des risques et des menaces.

Le prestataire doit également s'assurer des qualités de son futur client. Elles sont tout particulièrement appréciées lors des premières crises traversées avec le fournisseur. Le prestataire doit pouvoir disposer de tous les événements qui touchent son client, ce qui peut se traduire par une clause « d'alerting ». La confiance peut se renforcer lors de ces événements.

A noter que les clients peuvent avoir la possibilité de demander des

audits sur leur prestataire afin de mieux apprécier leurs qualités. De même, certains clients demandent la possibilité d'évaluer, voire de noter, la qualité du service. Enfin, toute entreprise doit pouvoir également disposer de la possibilité de changer de prestataire. Ce changement a un coût : un coût financier mais aussi celui de l'adaptation à une nouvelle structure. Le client doit avoir conscience qu'il doit rester en capacité de récupérer l'ensemble de ses données. Il faut donc, lors de la conclusion du contrat, envisager la réversibilité. Ces possibilités et options touchent une nouvelle fois à la confiance et à la transparence qui associent les deux parties.

II- Un service toujours plus global et personnalisé

Au niveau de l'offre, il s'agit de s'inscrire dans une démarche de performance de sécurité avec une approche globale des outils pour un coût raisonnable. Aujourd'hui, le marché a atteint une certaine maturité et les coûts pour les clients sont avantageux. On constate aussi une spécialisation dans cette offre notamment sur le cloud qui propose des architectures intéressantes.

L'avenir se porte sur le développement de « l'alerting » et dans la capacité de développer la proactivité en exploitant les opérations de reporting. Dans ce dernier cas, il s'agit notamment de faire corréler des événements qui se passent à l'échelle planétaire. Le prestataire travaille avec son client pour identifier des scénarios, les risques et menaces qui peuvent lui être propres et les solutions qui peuvent être apportées aux différentes situations.

Ces évolutions permettent de développer le partenariat avec les clients, d'offrir un panel de compétences extrêmement large. Il s'agit de comprendre le métier du client, ses attentes et le rassurer. Il faut rentrer dans une méthodologie propre au client et c'est bien là le but du « as a service ».

III- La taille de l'entreprise, une condition de l'externalisation des services

Les entreprises évoluent et s'agrandissent. La sécurité est une des opportunités pour faciliter voire garantir la croissance de l'entreprise. La ressource en compétences de « sécurité cyber » est rare et généralement captée par les éditeurs, laissant peu d'opportunités aux entreprises de disposer de ladite ressource en interne. Par ailleurs, la spécialisation et la mise à disposition de moyens tels que le cloud incitent les entreprises à externaliser leur cybersécurité.

Pour les plus grandes entreprises, il est possible d'opter pour une solution hybride. Il s'agit ainsi de disposer de compétences en interne et dans le même temps de faire appel à l'externalisation notamment dans les phases dites « de pic de charge » ou sur la prévention et la détection des menaces. En tout état de cause, il est primordial que l'entreprise dispose d'une gouvernance et qu'elle définisse sa stratégie sans en faire porter la responsabilité sur un quelconque prestataire de service.

Pour les entreprises plus modestes, l'externalisation semble s'imposer de facto avec pour seule limite le maintien d'une ligne stratégique qui lui est propre notamment dans le choix du type de réaction face à une attaque cyber.

Ainsi, l'externalisation de la cyberdéfense dépendra non seulement de la taille mais également de la criticité du secteur de l'entreprise.

B
ARTICLE 17

Gestion des filières de sécurité et protection de l'information

Intervenants :
Rémy FEVRIER – maître de conférence, CNAM
Didier BENZA - responsable des systèmes d'information, INRIA
Mathieu GILLLON – responsable interdépartemental DSSI, préfecture Nord-Pas de Calais,
Guillaume DERAEDT - responsable sécurité de systèmes d'information, CHRU Lille
Romain BEKMANN - responsable département juridique.

Résumé des interventions :
Devant la difficulté constatée pour s'assurer de la protection des échanges de données et de la confiance à accorder aux moyens de protection de l'information scientifique et technique, des experts de la cybersécurité exposent cette problématique à travers une analyse des risques, des impacts sociaux et une approche juridique.

Les échanges d'informations contribuent à optimiser chaque étape du processus d'innovation.
Il est important de se demander à chaque moment avec qui se pratiquent les échanges. La question doit également porter sur la manière dont il faut, entre grands donneurs d'ordres, en assurer la sécurité et dont on peut concilier la protection de l'information scientifique et technique et la recherche développement.

Quelle attitude des dirigeants par rapport à cette problématique ?
L'attitude des dirigeants vis à vis de la sécurité des informations financières et personnelles, qui constituent des informations stratégiques à conserver pour la bonne santé de l'entreprise, est très variable.
Après des centaines de conférences sur la protection de l'information et de données, on constate que le dirigeant va écouter mais que ce n'est pas pour autant qu'il va consa-

crer à ces questions le budget permettant d'agir. La responsabilité civile et pénale du chef d'entreprise est un aspect majeur auquel il faut sensibiliser les dirigeants. De plus en plus, le juge s'intéressera à la personne qui aurait pu empêcher que les informations ne soient volées.
Il est indispensable de faire des analyses de risques et des études d'impacts sociaux. Dans un hôpital, à titre d'exemple, il faut savoir mesurer l'impact de ces risques. L'idée est de faire des tableaux de bord et d'écouter en fonction de la stratégie de l'établissement. Quand une entreprise veut garder une avance compétitive, elle doit être assurée de ne pas divulguer ses informations. Enfin, la question du degré de confiance à accorder à un interlocuteur se pose.
Les concurrents ont des moyens financiers importants. C'est la première chose que les fraudeurs vont essayer de savoir. Certains ne veulent pas mettre cette information en ligne car ils estiment que cela peut mettre en cause leur stratégie et leur développement économique. Si une entreprise cherche un financement, elle ne doit pas donner l'information à ses concurrents. Pour autant, les clients ont le droit et l'obligation d'être informés : la transparence est indispensable pour le business.
Dans le monde de la santé, c'est la CNIL qui fixe les règles. Il n'est possible d'avoir accès aux informations d'un patient seulement lorsqu'il est soigné dans l'établissement, dans le pôle. Si le patient arrive inanimé, les urgentistes doivent pouvoir accéder à son dossier médical pour permettre les soins les plus adaptés pour le patient. Ils en en d'ailleurs le droit. Il faut donc savoir faire preuve de flexibilité.
Il faut aussi accepter l'éventualité que des employés rappelés en urgence en pleine nuit oublient leur carte-pass. Il fut donc prévoir des dispositions dérogatoires pour les faire tout de même pénétrer dans l'établissement au moyen d'une autre forme d'identification.
Les données de recherches sont extrêmement sensibles car il y a des appels d'offres à la clé et des informations ultra confidentielles.
Les efforts portent plutôt vers la recherche de solutions pour sécuriser sans être trop lourd car il est nécessaire d'être réactif face à la concurrence internationale, y compris sur les recherches médicales.

Qu'est ce qu'une information sensible ?

C'est une information dont la divulgation au delà d'un certain périmètre entraîne un préjudice. Celui-ci est parfois très facile à mesurer. Le grand problème reste le facteur humain. Une entreprise peut dépenser de sommes très importantes pour sécuriser ses informations sensibles, mais si un seul de ses employés parle trop sur un réseau social ou répond à un mail frauduleux et diffuse sans le savoir un des plans confidentiels de l'entreprise, tout cela devient caduc.
La classification de l'information dépend de l'émetteur mais cela reste est un choix stratégique qui doit être porté par le plus haut niveau. C'est une décision qui nécessite un aval politique et un minimum d'investissement moral de l'entreprise pour que tout puisse se mettre en place. Il n'est pas nécessaire par ailleurs de protéger et classifier une donnée qui pourrait être rendue publique.
Un autre risque existe, celui des personnes extérieures (stagiaires, prestataires de service, visiteurs) qui ne connaissent pas les règles de sécurité.
En termes de recherches de financement, les données sont davantage de nature à rassurer l'interlocuteur donc elles ne sont pas vraiment confidentielles. En revanche, d'autres informations ne doivent pas être connues hors de l'entreprise. Si celle-ci communique trop d'informations, le risque est de voir ces informations divulguées. Il faut donc pouvoir communiquer sur la finalité et l'objectif, mais sans jamais dévoiler le processus. De la sorte, l'entreprise qui reçoit les

informations ne pourra rien dévoiler qui soit de nature à porter atteinte aux données confidentielles du prestataire.
Il ne faut pas se lancer dans l'innovation pour innover, mais surtout pour apporter quelque chose de nouveau.

Quelles solutions à ces problématiques de confidentialité ?
Il n'y a pas de solution miracle.
Pour un prestataire, il faut absolument préserver la confiance des partenaires. Il peut arriver qu'une entreprise de protection de données ne soit pas certaine de pouvoir assurer la protection complète demandée, alors même que le caractère secret des informations est vital. Dans ces cas là, il est possible de souscrire une assurance pour évaluer la valeur des données par l'assureur.
Le facteur humain reste un facteur déterminant en termes de fragilité. Il faut faire entrer dans les consciences une réelle responsabilité collective. Les enjeux humains et financiers aujourd'hui sont les plus importants tandis que les mesures et précautions restent les mêmes : analyses des risques, maîtrise de la diffusion de l'information et de sa structure, moyen humain et technique.

Conclusion
78% des pertes d'informations stratégiques au sein des entreprises sont dues à des pertes involontaires et non à des piratages. Il s'agit de bavardages, d'erreurs humaines...
98% des professionnels utilisent Internet pour leurs travaux de métier. Parmi eux, 82% utilisent leurs propres équipements tandis que 75% externalisent leurs données.
90% ont entendu parler de hacking.
Enfin, 83% des professionnels ne connaissent pas leurs propres responsabilités pénales en matière de diffusion d'informations.

ARTICLE 18

Santé rime-t-elle avec sécurité ?

Résumé des interventions :
70% de la population accorderait plus de confiance à un avis médical dispensé sur Internet qu'à un médecin. Pourtant, les données personnelles de santé et les systèmes d'information intégrés dans les équipements bio-médicaux constituent un véritable enjeu de sécurité. Les risques sont réels mais encore trop souvent sous-estimés, tant par les professionnels de santé que par les patients, et une prise de conscience globale de ces problématiques s'avère nécessaire pour les limiter.

I – Les risques numériques dans le domaine de la santé

Les données de santé sont sensibles et, pour une grande part, confidentielles. Elle ont une grande valeur sur le marché noir des données et intéressent beaucoup les géants du numérique. En premier lieu, si les flux sont sécurisés, comme l'impose la loi, il est impossible de procéder au chiffrement de plusieurs millions d'entrées d'une base de données. Le système demeure donc intrinsèquement vulnérable.

Si le corps médical tient par principe à ce caractère confidentiel (secret médical), il est encore insuffisamment au fait des spécificités du numérique, par méconnaissance. Confronté à l'urgence d'une situation, un médecin n'utilisera pas sa connexion sécurisée, avec une carte à puce CPS et son code PIN, trop contraignante et chronophage. Il demandera, par exemple, l'avis à un confrère par sa messagerie personnelle en utilisant son téléphone ou sa messagerie Gmail. Pour bénéficier de matériel plus performant que celui de l'hôpital, un médecin peut préférer étudier à domicile un dossier qu'il aura préalablement en-

Intervenants :
- Benoît LOUVET, avocat au Barreau de Paris,
- Michel DUBOIS, OSSI, service de santé des armées,
- Philippe LOUDENOT, RSSI, Ministère de la Santé,
- Fabien DACHICOURT, RSSI, Correye, DroupePictime,
- Nicolas DUVINAGE, OCLAESP.

registré sur son ordinateur personnel. De même, ayant accès au système d'information de l'établissement hospitalier, il peut outrepasser ses droits et consulter le dossier informatique de patients autres que les siens. Il arrive également que des données restent visibles sur des écrans d'ordinateur accessibles par tout un chacun dans l'enceinte de l'établissement et que des photographies d'écrans soient prises pour récupérer les données médicales. Les contentieux à ce sujet se multiplient. Un autre exemple édifiant est celui de l'utilisation d'une plate-forme non sécurisée par des praticiens qui avaient contourné l'intervention du DSI ou du RSSI (l'article L1111-8 du Code de la santé publique prévoit un agrément des hébergeurs des données de santé publique, dont la liste est publiée sur le site de l'Agence des systèmes d'information partagés de santé). Pour le professionnel de santé, la priorité reste le soin et la santé du patient, pas la sécurité, dont il ne mesure pas toujours les enjeux.

Une autre problématique concerne les données dans les appareils biomédicaux, dont la maintenance et la supervision sont réalisées à distance, souvent à l'étranger. Deux plate-formes ont été piratées aux États-Unis : on ignore la nature des données piratées et ce qu'elles sont devenues. D'autre part, on ne s'interroge pas sur l'anonymisation des clichés ainsi envoyés ni sur l'usage qu'il pourrait être fait des données transmises. Le danger est encore plus prégnant en ce qui concerne leur revente sur le marché de l'occasion, pour l'Europe de l'Est ou l'Inde : le plus souvent, les données ne sont pas effacées avant la cession des appareils. La maîtrise des données qui transitent par les objets connectés consacrés au Quantified self est également une illusion : si Google, Apple, Microsoft etc, garantissent une chaîne de transmission sécurisée, on peut s'interroger sur le sort final des données et leur traitement par les développeurs et les grands fournisseurs des applications. Or, ces questions vont se poser de manière de plus en plus aiguë, les géants du Net investissant massivement dans le domaine de la santé. D'une manière générale, la multiplication des interconnexions augmente les risques de perte et de captation.

Négligence, manque d'informations sur le fonctionnement des réseaux informatiques, résistance à l'authentification forte pour des raisons d'impératifs professionnels sont autant de causes qui menacent la confidentialité des données, lesquelles peuvent alors fuiter ou être volées.

Enfin, les appareils biomédicaux (scanner, échographe, pousse-seringue..) peuvent subir l'attaque d'un virus ou être piratés. Une prise en main à distance pour changer les paramètres est envisageable. Les conséquences peuvent être graves. Des expériences ont été réalisées : il est techniquement possible de prendre le contrôle à distance d'un pacemaker pour en modifier les variables ou d'un pousse-seringue automatique pour changer les dosages.

Même si l'acte n'était pas malveillant, à Épinal, les programmes de radiothérapie avaient été modifiés en interne : il a été reconnu que le bug informatique provoqué par cette manipulation a été en partie responsable de l'irradiation de plusieurs patients. Cela prouve la grande vulnérabilité des logiciels et l'usage criminel qui peut donc en être fait.

II – Les moyens de lutte

Plusieurs pistes sont préconisées. Il serait souhaitable d'améliorer la formation des professionnels de santé, de les sensibiliser aux risques existants afin qu'ils modifient leurs comportements. Les services de sécurité informatique ont un rôle important d'accompagnement pour les inciter aux bonnes pratiques et éviter les mésusages. Dans un secteur où les obligations ne sont pas toujours bien vécues, il est nécessaire de réaliser ce travail de persuasion pour obtenir une adhésion aux mesures de sécurité, actuellement perçues comme des contraintes. Le dia-

logue entre le monde de la santé et le monde du numérique devrait être amélioré. En effet, c'est par des échanges véritables entre les acteurs des différents métiers que les progrès pourront se réaliser.

Néanmoins, il est également indispensable de proposer aux praticiens des solutions de sécurité adaptées à leurs besoins et aux réalités de leur métier. Ainsi, l'utilisation de la carte CPS (carte d'identité professionnelle électronique attribuée aux professionnels de santé certifiés par leurs ordres) pourrait être simplifiée en intégrant une technologie de contact qui maintienne le même niveau de sécurité. Le patient, en tant qu'utilisateur, notamment des objets connectés, doit également faire preuve de vigilance.

Les budgets consacrés à la sécurisation des données devraient également être plus conséquents, quelle que soit la taille de l'établissement, ses moyens humains et financiers. Effectivement, les organismes étant nécessairement de plus en plus interconnectés, l'interopérabilité exige des niveaux de sécurité équivalents.

Si une réglementation existe (CNIL, Code de la santé publique, décret de 2007 sur le traitement confidentiel médical dans les systèmes d'information de santé, pré-requis de base de l'hôpital numérique...), elle est encore trop souvent déclarative. Les sanctions et les contrôles, pratiqués par des entités externes, sont encore peu nombreux. Le scandale ayant un impact sur la réputation de l'établissement est redouté, les manquements ponctuels au respect strict de la sécurité le sont moins. Des procédures civiles plus fréquentes, sur le modèle des class actions aux États-Unis, pourraient entraîner des conséquences financières à même de convaincre de l'utilité d'investir dans la sécurité. Les assureurs peuvent également constituer un argument de poids pour limiter au maximum les risques. Par ailleurs, si la politique des systèmes d'information de l'État s'applique aux établissements publics, ce n'est pas le cas pour les organismes privés. C'est pourquoi une politique sectorielle est nécessaire. C'est dans ce sens que l'Asip (Agence des systèmes d'information partagés de santé) a entamé des travaux. Un référentiel est en cours d'élaboration en collaboration avec des professionnels de la santé, des juristes, des fournisseurs et des associations de patients. Chaque texte est soumis à commentaires avant publication officielle. Cependant, si un cadre normatif s'impose, il est intéressant de noter que le modèle américain s'est auto-régulé sans intervention de l'État. Il en est ainsi de la loi PIPA (Protect Intellectual Property Act).

Autre initiative : tous les CHU ont rédigé un cahier des charges commun, issu d'un groupe de travail composé de RSSI et d'ingénieurs bio-médicaux, qui a été transmis au ministère de la santé puis à l'Asip.

Une harmonisation des systèmes de santé et de la réglementation européens permettrait d'optimiser les coûts et d'exercer, en ayant un poids plus important sur le marché, une pression plus importante sur les fabricants des équipements bio-médicaux, de manière à ce qu'ils intègrent à leurs dispositifs, dès leur conception, des systèmes de sécurité, tels que des certificats d'authentification, des mises à jour régulières des logiciels. Trop d'interlocuteurs limitent encore la question de la sécurisation numérique à une question matérielle ou considèrent qu'elle relève uniquement de la CNIL, le monde de la santé étant supposé en être affranchi.


THALES


gether • Safer • Everywhere

C
ARTICLE 01

SOGETI - Les nouvelles cibles des hackers : les systèmes industriels et les objets connectés

Intervenants :
- SOGETI (SOciété pour la Gestion de l'Entreprise et Traitement de l'Information)

Résumé des interventions :
Toute révolution industrielle se construit sur une nouvelle technique, ce qui entraîne l'apparition de nouveaux risques. La révolution numérique n'échappe pas à ce constat. Au fil des ans, des risques d'un genre nouveau sont apparus.
Au début des années 2000, on parlait de risques sociaux. Dès 2008, les risques ont davantage été liés à la mobilité. Mais depuis 2010, ces risques sont à associer aux analytics (big data) et au cloud.
Dès lors, dans une société où tout s'accélère, l'apparition de risques liés à l'Internet des objets est à craindre.

Les objets connectés
La société Sogeti a publié plusieurs ouvrages traitant des objets connectés et a choisi d'orienter ses travaux sur la protection, à la fois des technologies de l'information, mais aussi de l'Internet des objets. Cela revient à sécuriser les data centers, les applications (en temps réel pour les systèmes industriels ; embarquées pour les objets connectés), les données et les utilisateurs.
De ce fait, cinq préoccupations de sécurité sont apparues : le déni de service, l'absence de confidentialité, les modifications non autorisées des fonctions de l'objet, le non-respect de la confidentialité des données privées, et l'atteinte à la protection industrielle.
De ces cinq préoccupations de sécurité découlent dix problèmes majeurs de cybersécurité parmi lesquels se trouvent les API (Application Programming Interfaces) non sécurisées, disposant d'une authentification trop fragile ; l'absence de

chiffrement des données stockées…
Afin de résoudre ces difficultés, une méthode a été élaborée. Elle consiste tout d'abord à analyser les risques avant de définir la cible de sécurité. Par la suite, il faut concevoir les produits de manière sécurisée, penser à sécuriser le codage des applications, à tester les produits, et enfin à effectuer des tests d'intrusion avant d'évaluer le produit concerné.
Il est possible d'illustrer cela par un cas concret. Par exemple, les objets connectés communiquent souvent entre eux via les courants porteurs, car cette solution de communication se révèle plus simple que de déployer des systèmes sans fil.
La question posée était de savoir si ce mode de transmission est sécurisé. Or la réponse est négative. En effet, un ingénieur a réussi, en à peine un moins, à prendre la main sur le système de communication.

Les systèmes industriels
La principale menace visant les systèmes industriels est le sabotage. De ce fait, il existe plusieurs critères de sécurité. Classifiés par ordre d'importance croissante, il s'agit de la confidentialité, de l'intégrité et de la disponibilité.
Certains équipements ou systèmes (PLC, Programmable Logic Controller, et RTU, Remote Terminal Unit) ont des vulnérabilités spécifiques. De plus, le parc d'équipements est très hétérogène. Les protocoles spécifiques, utilisés dans le monde industriel, ne sont pas sécurisés et les contraintes d'exploitation rendent impossible la transposition de la sécurité « classique » dans ce milieu.
Pour répondre à ces besoins particuliers, il faut tout d'abord comprendre les « besoins métier », puis cartographier le système et les installations matérielles.
Ensuite, les mesures techniques seront déclinées en architecture de sécurité sur les quatre niveaux du système industriel, sachant qu'il sera utile de travailler sur les connexions entre ces niveaux.
Plusieurs principes clés se dégagent en vue d'assurer la sécurité des systèmes industriels, comme le fait de respecter l'architecture de zonage propre aux systèmes industriels, de penser la politique de patch, de veiller à la programmation des automates et de mettre en œuvre des produits de sécurité, spécifiques au monde industriel.
Cependant, la sécurité ne peut être qu'informatique. Il faut également mettre en place des mesures organisationnelles, rédiger un plan de maintenance, définir une politique d'accès sécurisé aux locaux ainsi que des automates programmables. Il convient également de définir et de tester les plans de continuité et de reprise d'activité.
Ceci fait, il faudra toujours garder à l'esprit que le scénario classique d'attaque d'un système industriel demeure la prise de contrôle de l'ordinateur d'un utilisateur connecté au système.

C
ARTICLE 02

ATOS :un leader de premier plan en cybersécurité (5 mois après l'intégration du groupe BULL)

Intervenants :
- Christophe MORET,Vice-président ATOS CYBERSECURITY
- Zeina ZAKHOUR – CTO ATOS CYBERSECURITY

Résumé des interventions :
La technologie fait évoluer les menaces dans leur forme, ce qui oblige les entreprises à ajuster leurs stratégies de défense, en privilégiant la protection des données sensibles et une réactivité en temps réel. L'avènement du cloud soulève de nouvelles problématiques de sécurité et impose une modularité dans la gestion de la sécurité. Entreprise mondiale, le Groupe ATOS développe un portefeuille d'offres permettant de faire face aux différentes menaces en ciblant les enjeux de leurs clients.

I – Les problématiques :

1° L'apport de la technologie

Les menaces n'ont pas changé, c'est la technologie qui a changé, autrement dit la façon dont les menaces prennent forme, et, par conséquent, les moyens à mettre en œuvre pour se défendre. Il n'est plus possible d'avoir une politique de sécurité unique au sein des entreprises et des administrations simplement parce que le budget ne peut pas croître à la même vitesse que les menaces. De même, la masse des données à protéger croît de manière quasi exponentielle. L'évolution de la protection tend donc vers une approche de l'analyse de risques touchant les données à protéger absolument. Il faut mettre les moyens autour de ces environnements particulièrement importants plutôt que d'essayer de protéger tout le système. Il faut cibler la sécurité. Une administration aura à protéger les données personnelles des administrés, tandis qu'une industrie aura plus à cœur de protéger ses brevets et ses méthodes de

fabrication. Pour les États, ce sera la protection des infrastructures critiques. Dans tous les cas, il est également question de réputation à protéger.

2° L'avènement du cloud

Dans le même temps où les technologies changent, les menaces se focalisent sur certains modes d'action (exemple des dénis de service). Aujourd'hui, toutes les entreprises qui souhaitent évoluer doivent s'orienter vers le cloud. Il faut cependant que cette évolution vers le cloud prenne en compte la problématique de la sécurité. Le défi consiste à savoir sécuriser les données critiques ou privatives conservées dans le nuage informatique mais aussi à identifier qui accède à quoi, comment et pourquoi. Il faut également prendre en compte la veille en matière de sécurité pour s'adapter en temps réel aux nouvelles évolutions de la menace. C'est une course contre les hackers. Il faut donc avoir une stratégie assez agile au niveau de la gestion de sa sécurité, afin de pouvoir s'adapter aux différentes menaces.

3° Le facteur temps

Le fait que tout le monde soit attaqué est une fatalité. Si l'entreprise n'est pas victime d'attaques, c'est qu'elle n'a rien à cacher. Le problème n'est pas d'empêcher ces attaques mais de les détecter et de réagir avant qu'il ne soit trop tard, avant que les données ne soient sorties, avant que, à l'autre bout de la planète, le même produit soit vendu 4 fois moins cher. Aujourd'hui, on sait que l'on va être attaqué mais on ne sait pas quand ; c'est un constat et non plus une question. Il faut donc être prêt à détecter en temps réel et à réagir en temps réel. La bonne gestion et la connaissance du big data sont essentielles pour pouvoir gérer ce volume d'événements en temps réel, y détecter les évolutions puis y réagir dans les temps..

II - Des solutions :

1° Le Groupe ATOS

Avec l'intégration du Groupe BULL, le Groupe ATOS comptabilise 9 milliards de chiffres d'affaire et 90 000 employés. Il est présent dans plus de 70 pays, avec une forte implantation en Europe. L'intégration du groupe BULL apporte une très forte complémentarité géographique, d'offres et de marchés au Groupe ATOS. Le Groupe possède 6 security Operation Center (SOC) dont 3 en Europe, où se trouvent les experts et les analystes œuvrant 365j/365 et 24h/24h pour protéger les données et les infrastructures. ATOS est partenaire des JO depuis les années 90 pour tout ce qui a trait à l'environnement informatique de l'événement. Tous les 2 ans, une équipe de plus de 3000 experts mobilisés sécurise entre 30 et 60 sites de compétition, villages, etc., et plus de 200 000 identités numériques.

Fort de ses compétences, le Groupe ATOS offre un portefeuille qui permet de répondre aux diverses problématiques de ses clients selon la formule protect & detect et analyze & mitigate :

- Security governance : mise en place d'une gouvernance de la sécurité qui s'adapte, avec des analyses de risque qui prennent en compte le corps business des entreprises.
- Situational awareness : mise en place d'une approche de sécurité intégrée, de manière à ce que les attaques soient analysées dans les centres de sécurité, et traitées.
- Digital Identity & Access : mise en place d'un dispositif modulable pour s'adapter aux changements des métiers et des fonctions internes d'une entreprise avec la gestion des identités.
- Secure communications : mise en place d'un système de sécurisation des communications et des échanges.

2° Le smartphone HOOX

L'exemple du smartphone HOOX développé par le Groupe ATOS, prend en compte la sécurité des postes mobiles.

Quantité de données extrêmement critiques y sont stockées. Ce smartphone permet ainsi de communiquer en toute sécurité (texte et voix), et de protéger les données de son utilisateur. Il est entièrement crypté, avec authentification biométrique. La sécurité est telle qu'il est complexe de répondre à une demande d'écoute légale sur ce genre de smartphone.

3° EVIDIAN IDENTITY & ACCESS MANAGEMENT : la solution de cybersécurité

La suite Evidian IAM a été classée par le kuppingerCole comme Overall Leader, product Leader et Innovation Leader dans son rapport de novembre 2014. Orientée processus métier, intégrée et modulaire, elle apporte une gestion des identités et des accès de bout en bout, permettant ainsi d'appliquer une politique évolutive sur un grand nombre d'utilisateurs, ressources, organisations et dispositifs. L'Identity management est véritablement devenu le cœur du problème de l'entreprise, le danger n'est pas de savoir où sont les données mais plutôt de savoir qui accède aux données, comment, et quelles informations sont accessibles. C'est toute la problématique de l'authentification, de l'autorisation, de la gestion des annuaires, et de la connexion des annuaires entre eux.

C
ARTICLE 03

2015 : l'année de la supervision continue («Continuous Monitoring») et de la sécurité analytique via le cloud souverain Qualys

Intervenants :
APhilippe COURTOT – PDG QUALYS

Résumé des interventions :
Résumé de l'intervention : les entreprises s'appuient sur des architectures distribuées, complexes et hautement dynamiques. Tandis que les réseaux s'étendent et que les périmètres deviennent prépondérants, les pirates trouvent en permanence de nouvelles attaques.
Pour anticiper ces attaques et assurer le maintien du niveau de sécurité, l'adoption d'un modèle de sécurité continue est devenu essentiel. Il permet de surveiller et d'analyser les menaces en permanence et d'alerter les services d'intervention.

Les architectures orientées cloud, associées à de puissantes ressources analytiques en temps réel cherchent à répondre à la problématique d'échelle résultant du paradigme de la supervision continue tout en ayant le souci de coûts maîtrisés. De surcroît, la sécurité continue via un environnement cloud souverain devient une réalité pour de nombreuses institutions et grandes entreprises.

La supervision continue, associée à de puissantes ressources analytiques en temps réel, offre de réels bénéfices. Pour cela, il est important pour les entreprises de commencer à intégrer cette approche de supervision dans leur programme de sécurité. En effet, la sécurité continue et fournie par une offre de cloud souverain peut devenir maintenant une qualité.

Aujourd'hui, nous sommes déjà dans le cloud et nos infrastructures imposent des changements. Pourtant nous sommes en position défensive puisque la sécurité vient toujours après. Du point de vue de la société Gartner, les ar-

chitectures cloud ont désormais toute leur place, surtout depuis que les malfaiteurs se sont organisés. Repenser la sécurité est avant tout une question d'architecture. Il faut avoir des systèmes beaucoup plus sophistiqués. Le rapport de Neil Mac Donald en 2014 met toutes les facettes de la sécurité dans un ensemble cohérent pour une meilleure visibilité. 80% des attaques sont dues aux faiblesses des applications web.

Selon la société Gartner, la première idée consisterait à cartographier l'entreprise puis à la faire analyser par des services de protection. Il faut une architecture Cloud qui met les machines en parallèle, bâtie sur cloud « back-end » extensible, virtualisé ouvert et supportant une corrélation en temps réel.
Pourquoi cette notion de cloud souverain ? Qualys sécurité dispose de deux data centers, l'un situé en Suisse et l'autre implanté aux États-Unis, afin de garantir son indépendance. Philippe Courtot estime à 50% le marché d'outsourcing en Europe et voudrait consolider les data-center . A ce titre, il manque de personnels spécialisés.

Les avantages de ces solutions intégrées d'accès global sont nombreux. Elles permettent notamment la maîtrise les coûts. Il existe une meilleure corrélation et une analyse en temps réel lorsque ces solutions intégrées sont mises en œuvre. Dans le cloud, les nouvelles fonctions arrivent vite et les fournisseurs contrôlent l'infrastructure. Au final, ce modèle se révèle plus efficace. Il s'agit d'une nouvelle forme de calcul qui obéit en cela aux dispositions édictées par le Patriot Act aux États-Unis.

C
ARTICLE 04

MICROSOFT ; LA DEFENSE EN PROFONDEUR.

Intervenants :
Yann DUCHENNE, architecte des offres identité et sécurité, Microsoft
Vincent MARTIN, responsable des offres identité et sécurité, Microsoft

Résumé des interventions :
comporte une solution de sécurité adaptée. Mais surtout, Microsoft se distingue aujourd'hui par sa prise en compte tout à la fois de la sécurité périmétrique et de la défense en profondeur des systèmes

Microsoft et la sécurité :
Microsoft étudie les attaques « cyber » sur les plans juridique et technique. L'objectif est d'anticiper pour mieux protéger les infrastructures. L'entreprise dispose d'un site dédié à SEATTLE. Elle élabore un rapport de sécurité tous les six mois.
Microsoft est un acteur responsable. L'entreprise agit en toute transparence (Microsoft trust center). Co-fondateur du centre des experts de la cyber-sécurité, l'entreprise entend éduquer et former à la lutte contre les cyberattaques. La sécurité est présente sur toutes les applications Microsoft, plus particulièrement dans les domaines de la protection des infrastructures, de la sauvegarde des données et de la gestion des identités et des accès. La sécurité est intégrée dans les produits. Elle est également proposée via le cloud, les outils et l'accompagnement. Cette vision correspond à la mise en pratique de la pensée de Bruce SCHNEIER : « la sécurité n'est pas un produit mais un process. » (exemples : Windows 10 et le certificat de Microsoft pour sécuriser le cloud)
Microsoft entend innover pour sécuriser toujours mieux. C'est dans cette optique, par exemple, qu'est conçue une solution de détection des comportements anormaux.

La sécurité périmétrique contre la défense en profondeur :
Aujourd'hui, il faut changer de paradigme. La sécurité périmétrique n'est plus suffisante car l'ennemi peut être à l'intérieur (c'est le cas de 40% des attaques, Forester 2013). Le système est poreux, rendant difficile le blocage périmétrique. L'informatique est mobile. Des données sont stockées dans le cloud.
La technologie apporte cependant des opportunités pour obtenir une défense en profondeur. La défense en profondeur ne remet pas en cause la sécurité périmétrique. Il y a deux aspects principaux : la gestion de l'identité de manière hybride et la protection de la donnée. Par rapport à des menaces externes, le client cherche des produits sécurisés. Pour faire face à des menaces internes, on doit assumer des brèches et limiter la contagion. Enfin, la liberté de l'utilisateur induit parfois des mauvaises pratiques qui peuvent remettre en cause les procédures de sécurité les plus abouties.

Les services de Microsoft :
Microsoft dispose d'une équipe dédiée à la sécurité. Trois axes principaux sont suivis : la mobilité, les solutions cloud et le modèle de défense pro-actif. L'entreprise développe des partenariats avec d'autres acteurs comme l'ANSSI. Les observations issues d'un travail de quatre ans permettent d'arriver à certaines conclusions. Tous les secteurs apparaissent menacés, la compromission d'un compte entraîne une escalade nécessitant la mise en place de contre-mesures et les vulnérabilités sont souvent évidentes. Il est nécessaire de rappeler les mesures d'hygiène informatique basiques qui permettent de limiter très substantiellement les risques.
La méthode MICROSOFT consiste à évaluer, sécuriser, réduire les menaces. Ses offres de sécurité s'articulent autour de trois missions : protéger/détecter/ répondre.

C
ARTICLE 05

Quelle coopération entre les agences de sécurité européennes ?

Intervenants :
- Guerric PONCET, journaliste, Le Point.
- Mickael HANGE, Président du BSI (Bundesamt für Sichereit in der Informationstechnik), agence fédéral de sécurité informatique allemande.
- Guillaume POUPARD, Directeur général de l'ANSSI.

Résumé des interventions :
La coopération entre les pays membres de l'Europe apparaît nécessaire d'un point de vue financier mais aussi pour une plus grande efficience en matière de sécurité informatique.
Cette coopération ne peut cependant être totale et ce afin de garantir la souveraineté de chaque nation. La cryptographie en est un exemple. La question du transfert de compétence de la cybersécurité à l'Europe apparaît ainsi naturellement.

La coopération entre les États européens est nécessaire en matière de cybersécurité. En effet, nos intérêts étant liés, notre défense l'est aussi. La puissance individuelle de chaque État ne peut permettre la production de logiciels et d'équipements de cybersécurité pour faire face à chaque menace. Ensemble, cette mise en place de solutions de sécurité est possible. Or, la souveraineté des États impliquant une maîtrise totale de leurs communications. Le partage des solutions cryptographiques se trouve être une des limites à la coopération inter-étatique. Il en résulte la question du transfert de la compétence de lutte contre la cybersécurité au niveau européen.

I. Une nécessaire coopération

La coopération entre les agences de sécurité est nécessaire en raison des intérêts communs entre États européens. Ceux-ci se situent à trois niveaux. D'une part, un marché européen vaste est à conquérir pour nos solutions de cybersécurité. Ensuite, il n'est pas possible

pour un seul pays de développer des équipements de cybersécurité mais ceci est envisageable à l'échelle européenne. Enfin, la confiance qui doit s'établir entre les différents acteurs européens de la cybersécurité peut permettre une réaction plus rapide et plus efficace face aux menaces. Il s'agit donc d'une relation gagnant-gagnant.

Le couple franco-allemand est un bon exemple de cette coopération. Il est par ailleurs souvent utiliser pour illustrer le moteur de la coopération européenne. L'Allemagne montre sa volonté de coopérer notamment par le biais du développement d'une plate-forme de coopération.

Pour l'ANSSI, il est nécessaire de coopérer et il existe un besoin en outils nouveaux pour faire face à une éventuelle cyberguerre. Il faudra dans ce cas « des hommes, de la technique et des processus ». Les processus sont obligatoires, ils deviennent complexes et des exercices sont primordiaux pour tester les concepts. Le développement de politiques de sécurité, de concepts, d 'équipements et de standards de travail est indispensable. L'entraînement de Response Team communes afin de lutter contre des attaques est également très important. Notre techno-industrie doit se trouver au centre de notre défense.

La SSI européenne est une réalité que l'on doit développer. L'ENISA, l'agence européenne de sécurité des systèmes d'information, forme la fondation de cette coopération. De plus, la directive NIS, adoptée par le conseil de l'Union européenne, place la cybersécurité dans le domaine des secteurs stratégiques.

II. Les limites de la coopération

La collaboration ne peut être totale : la souveraineté des États réside également dans la sûreté de leurs communications. Monsieur Hange a posé la question pertinente : « Les alliés sont-ils des ennemis ? » C'est une véritable interrogation au regard de certains cas concrets récents. A titre d'exemple, en 2013, le logiciel Regin, utilisé par les Américains et le Royaume-Uni, a été employé pour espionner la société BELGACOM. Edward Snowden a confirmé que le GCHQ avait déjà attaqué BELGACOM par le passé.

Afin de coopérer efficacement, il convient de souligner qu'une grande confiance est nécessaire. Ce genre d'événements porte préjudice à cette confiance et diminue l'efficacité des échanges. Le domaine de la défense est lui aussi critique. La sécurité des communications d'un État repose beaucoup sur la cryptographie. C'est donc également un des points de non-coopération au sein des acteurs étatiques de la cybersécurité.

III. Le transfert de compétence au cœur de la problématique de sécurité

La réponse à une attaque étatique ne peut être efficace qu'à partir du moment où l'entité a atteint sa taille critique. Selon l'ANSSI, la taille critique se trouve entre 400 et 500 millions d'habitants. C'est uniquement à partir de ce volume que le secteur économique peut entrer en concurrence avec les autres acteurs en matière de production de solutions logicielles et matériels informatiques. L'Union européenne comptant 507,4 millions d'habitants au 1er janvier 2014, cette taille critique est facile à atteindre sous réserve d'arriver à un consensus des États-membres.

Or, pour pouvoir produire des solutions autonomes de cybersécurité, les États doivent opérer un transfert de compétence en matière de cybersécurité de l'État vers l'Union Européenne. Ce transfert de compétence induit un transfert technologique, lequel suppose à son tour une perte de souveraineté. Ainsi, les limites de la coopération freinent le processus de transfert de compétence et finalement la mise en place de solutions européennes de cybersécurité. La question de la mutualisation des dispositifs de défense et d'attaque

dans le cyberespace se pose. Pour l'ANSSI, cette mutualisation n'est pas d'actualité. Cependant, l'amélioration des mécanismes de confiance est constante, notamment avec la création en 2012 d'un CERT Europe (certificat électronique européen) ayant pour mission de protéger les institutions européennes. Ce genre d'initiative est génératrice de confiance.

Glossaire :

ANSSI : Agence nationale de sécurité des systèmes d'information
CERT : Computer Emergency Response Team.
ENISA : European Network and Information Security Agency.
NIS : Network and Information Security.
GCHQ: Government Communications HeadQuarter, service de renseignement électronique du gouvernement britannique.

C
ARTICLE 06

La nouvelle stratégie de cyberdéfense de l'OTAN

Résumé des interventions :
L'OTAN, comme chaque État, n'a pas eu d'autres choix que d'intégrer le vaste domaine du cyberespace dans le champ de sa politique de défense qui s'articule autour d'une volonté d'actions communes entre pays. Toutefois, le continuum sécurité-défense implique également de s'interroger sur la relation qui existe entre les cybermenaces et le droit des conflit armés.

Intervenants :
Nicolas ARPAGIAN, rédacteur en chef de la revue "Prospective stratégique" et Maître de conférences à l'ENSP
Général d'Armée Aérienne PALOMEROS, Cdt Suprême Allié pour la Transformation OTAN (Norfolk, Virginie).

I- La cyberdéfense, part intégrante des politiques de défense

Le cyberespace constitue un domaine à part entière, sans frontière mais avec cependant des limites. La responsabilité et l'autonomie de chaque pays de l'Union européenne demeurent essentielles dans l'approche de toute stratégie de défense et cela est particulièrement vrai en matière de cyberespace. Il n'est alors pas étonnant de constater que l'aspect cyber est ainsi abordé au sein même du concept stratégique de l'OTAN. Ce sujet s'étant un peu estompé depuis la chute du Mur de Berlin, il revient sur le devant de la scène avec la crise ukrainienne.

Néanmoins, il convient de revenir sur deux notions essentielles que sont la défense coopérative et la défense collective. Cette dernière consiste à se doter des moyens pour protéger les systèmes de contrôle, de surveillance mais également les systèmes d'armes. Il s'agit pour l'OTAN de détenir tous les moyens de défense collective qui garantissent une intervention rapide en tout lieu et en tout temps. La sécurité coopérative vise quant à elle à

assurer un partenariat avec de nombreux pays, mais aussi avec des organisations internationales telles que l'Union européenne, l'Union africaine ou bien encore l'Organisation des Nations Unies. Il s'agit d'améliorer les échanges d'informations et les retours d'expérience, notamment dans le domaine de la cyberdéfense. Toutefois, pour contrer les menaces cyber, il s'agit d'aller bien au-delà de l'échange d'informations, il convient de mettre en place des actions communes.

II– Agir en commun, une nécessité

La volonté des États de mutualiser leur cyberdéfense s'exprime toujours davantage. Cette question est d'autant plus importante dans le cadre des missions du SACT, lesquelles visent à évaluer ce qui a pu être fait en réaction aux événements passés ou actuels mais aussi en prévision des menaces à venir. Le travail en commun est forcément source de davantage d'efficience. Dans le domaine de la cyberdéfense, la réalité s'avère bien plus complexe et délicate à mettre en œuvre.

Le centre d'excellence de Tallinn est ainsi un exemple concret de bonne coopération, au même titre que la Smart Defence. Les avancées se font cependant à trop petits pas, car ce domaine est et demeure avant tout du ressort régalien. Les coopérations bilatérales, a contrario, s'avèrent toujours plus aisées et efficaces, a l'instar des nombreux partenariats américano-britanniques. Une meilleure compréhension du cyberespace nécessite donc de véritablement capitaliser l'expérience accumulée au cours des différentes opérations multinationales.

La protection des systèmes de l'OTAN passe également par la veille et l'alerte. A ce titre, l'OTAN propose son aide à tout pays la sollicitant, même s'il n'est pas membre de l'organisation. Les échanges d'informations cyber sont cruciaux et sont même de plus en plus fréquents entre pays de l'OTAN. Au cours de l'année 2014, un exercice « cyber coalition » a ainsi concrétisé ce type de coopération en réunissant plus de 32 pays, 80 organisations et plus de 700 intervenants. Cet exercice s'appuyait sur le pôle d'expertise estonien. La diversité de points de vue des acteurs de l'exercice s'est avérée très stimulante s'agissant de l'analyse stratégique. L'objectif à poursuivre est l'interopérabilité et la mutualisation dans le domaine du renseignement et du cyberespace, sans trop perturber les activités de préparation opérationnelle des différents pays. Sortir de ses frontières et penser à plusieurs permettent un enrichissement sans égal, a fortiori lorsqu'il s'agit de personnes, de nationalités et de cultures différentes.

Tous les pays de l'OTAN se sont engagés à investir dans leur Défense. L'Union européenne a également un rôle et une responsabilité, en plus d'une carte à jouer dans le domaine du cyberespace. Les grands acteurs économiques doivent être davantage associés et participer plus souvent aux exercices de l'Organisation.

III- L'application du droit des conflits aux cybermenaces

Le continuum sécurité-défense apparaît de plus en plus pertinent, avec une menace cyber présente quels que soient les conflits, notamment à l'occasion des conflits hybrides de type semblable à celui de la crise ukrainienne. Plus concrètement aujourd'hui, la problématique majeure consiste à appliquer le droit des conflits armés aux cybermenaces.

L'article 5 du Traité de Washington précise que toute attaque contre un pays est une attaque contre l'OTAN. Par conséquent, comment réagir à l'occasion d'une cyberattaque contre un pays de l'OTAN ? Au plan formel, les chefs d'États ont déjà confirmé que rien ne s'opposait à ce que des attaques cyber d'une certaine intensité ou gravité puissent être considérées comme une véritable attaque contre un pays. La question qui

se pose en permanence est celle du niveau de déclenchement de l'article 5. Comme pour la dissuasion nucléaire, cette question reste dans un certain flou afin de laisser une grande liberté d'action aux différents pays.

Glossaire :

SACT : Supreme Allied Commander – Transformation (commandant suprême allié Transformation). C'est un des deux commandants stratégiques de l'OTAN. Il contribue à identifier et prioriser les futurs besoins capacitaires et en matière d'interopérabilité tout en étudiant de nouveaux concepts et de nouvelles doctrines.

Smart Defence : initiative de l'OTAN qui vise à promouvoir plus de cohérence et d'efficacité dans les dépenses de défense des États membres.

C
ARTICLE 07

CYBERSECURITE : Le rôle des offreurs globaux dans la fédération des acteurs et l'émergence d'une industrie de confiance – Groupe SOPRA-STERIA

Intervenants :
Didier BOSQUE, Innovation Manager, SOPRA-STERIA.
Ihame CHOUKRANI, Directeur Cybersécurité, SOPRA-STERIA
Jean-Luc GIBERNON, Directeur Défense, SOPRA-STERIA
Olivier VALLET, Directeur infrastructure & Security Services, SOPRA-STERIA

Résumé des interventions :
Il est important de pouvoir accompagner dans une logique de confiance les clients qui sont confrontés à la transformation numérique. La sécurisation des nouvelles infrastructures numériques est essentielle.
Depuis le début du mois de janvier 2015, une filiale dédiée à la gestion des infrastructures du cloud et à la cybercriminalité a été créée. Plus de 700 experts intégrés dans deux grands centres récemment construits œuvrent dans la cybersécurité.

L'ensemble des acteurs économiques ressent le besoin croissant de bénéficier, en tant que client, d'une offre plus sécurisante. Dans cette optique, il convient de développer un partenariat avec CEA TECH. Des solutions existent sur le marché mais la filière manque d'experts et il serait intéressant de fédérer l'ensemble des écoles d'ingénieurs. Enfin, il faut un régulateur pour mener ces rapprochements. Un travail étroit avec ANSSI, qui joue ce rôle en France, s'avère nécessaire pour avoir le niveau d'accréditation indispensable.
La menace est de plus en plus forte. Les attaquants ont l'avantage sur les défenseurs. Nous sommes dans une lutte où il faut se regrouper, se fédérer, s'organiser autour d'une défense collective.
Pour bâtir cet écosystème, trois axes ont été arrêtés :
En matière de formation, les entreprises de service numérique d'une certaine taille ont un besoin d'ingénieurs.
En matière de recherche le besoin

existe également et il est nécessaire de travailler avec des écoles, des laboratoires.
Le développement économique.
Dans le domaine de la défense, nous sommes dans une situation de confrontation permanente.
Il y a un besoin d'interopérabilité, d'une défense collaborative avec un volet stratégique et procédural et un autre volet plus technique et opérationnel.
Le groupe SOPRA-STERIA joue un rôle à la fois d'architecte, d'intégrateur et de développeur de solutions de sécurité dans la mise en œuvre d'un programme de supervision des systèmes d'information des données aux profits du ministère de la Défense.
Le groupe évolue dans un pôle de compétitivité et dans une logique de développement de la cybersécurité.
Il agit dans une logique fédérative en direction de la filiale aéronautique et spatiale autour du programme Albratros. Ce projet a pour objectif de faire émerger une filière cybersécurité.
Trois projets sont lancés dans cette logique coopérative :
Le premier, Box of PME, a pour objectif de bâtir un système d'intelligence économique.
Le second est le Laboratoire de cybersécurité, travaillant sur l'analyse et la façon de circonscrire les attaques.
Le dernier programme mobilise la recherche et la formation à la cybersécurité (pour limiter les failles dues au facteur humain).

ARTICLE C 08

Attaques ciblées
Cyber espionnage
Posture de défense adaptées

Intervenants :
Cyrille BADEAU Director Southern Europe, CISCO

Résumé des interventions :
Les attaques ciblées qui ont pour but le cyber espionnage ne représentent qu'une petite partie de toutes les cyber attaques. Aujourd'hui, les deux premières filières industrielles ciblées sont les industries pharmaceutiques et les entreprises chimiques. Elles sont convoitées à cause de leurs secrets de fabrication. L'entreprise CISCO présente en quoi elle détient aujourd'hui les meilleurs taux de détection.

Il ne faut jamais espérer contrer l'attaque du premier coup. Pour parvenir à agir, il est nécessaire d'analyser préalablement le risque de cyber attaque

Répartition des attaques en volume :
Les motivations qui sous-tendent les attaques sont les suivantes (décembre 2013) :
62% relèvent du cybercrime (72,6% en 2014)
34% sont commises dans le cadre du « hacktivisme » (17,8% en 2014)
3% concernent du cyberespionnage (8,2% en 2014)
1% peuvent être assimilées à du cyber warfare (1,4% en 2014)

Ainsi, les attaques ciblées qui ont pour but le cyber espionnage ne représentent qu'une portion très réduite des cyber attaques. Aujourd'hui les deux premières filières industrielles ciblées sont les industries pharmaceutiques et les entreprises chimiques. Ce sont notamment les secrets industriels et les brevets (qui ont souvent néces-

sité des investissements lourds) qui motivent les cyber attaquants.

Les attaques dans la pratique

Prenons l'exemple d'un investisseur qui souhaite investir 2 millions de dollars dans un pays pour produire des chaussures de sport. Il doit acheter beaucoup de machines, embaucher un grand nombre d'ouvriers dont le coût horaire soit le plus bas possible et construire les infrastructures. Pour autant, le produit doit être étudié et ira sur un marché concurrentiel, qui pèse des milliards de dollars et dans lequel se placent en position forte 4 ou 5 acteurs qui sont très puissants et bénéficient d'années d'investissements en recherche/développement. Il serait plus simple, si c'est possible, d'acquérir directement les savoir-faire et les technologies pour concurrencer ces géants, sans dépenser d'argent en recherches. Les risques sont grands pour les principaux acteurs du marché de se voir pillés. Ce pillage a d'ailleurs un effet direct dans les pays où sont implantées les usines, avec à la clef du chômage et des baisses de revenus fiscaux. Pour l'investisseur véreux, il est finalement plus facile de consacrer une partie de ses 2 millions de dollars à payer des hackers pour lui donner ce dont il a besoin. Il est également possible, en payant des attaquants, de faire en sorte de détourner les clients de l'entreprise historique et de les capter frauduleusement.

Il existe par exemple un logiciel espagnol nommé FOCA qui, si on lui donne un nom de domaine, travaille toute la nuit et le lendemain propose un plan d'attaque.

L'attaque sera lancée lorsque l'attaquant aura la certitude que la prise de point d'ancrage ne sera pas détectée. Si le réseau est bien protégé, les hackers attaqueront selon d'autres angles. L'usage débridé d'Internet au sein de l'entreprise ciblée permet souvent de trouver des point d'ancrage favorables pour une attaque.

Si à la maison un collaborateur tend à utiliser toujours les mêmes mots de passe, il est à parier qu'au travail, les mêmes mots de passe seront utilisés. Les attaques vont se faire via des mails, via des objets connectés comme les téléphone, les bracelet enregistreurs de performances etc...

Dès lors, il est essentiel d'être alerté lorsqu'une attaque débute ou est en cours. Pour avoir une vision complète de l'étendue de la menace, il faut tout fouiller, tout vérifier. Pour faire une comparaison parlante, il convient d'agir comme une force d'intervention qui fouille tous les recoins de chaque pièce d'une maison avant d'en sortir et d'annoncer que toute menace est écartée.

L'important est ce qui se passe à l'intérieur , la manière dont une attaque est conduite et progresse. Il faut cesser de se concentrer sur la porte qui est censée empêcher de rentrer.

Conclusion

L'idée est que le process protège tout le système 24 heures sur 24. Si un processus démarre alors qu'il était jusqu'alors inconnu, il est rentré immédiatement dans la cartographie des menaces potentielles. CISCO vend beaucoup de produits et de technologies qui signalent les compromission, qu'elles viennent d'un mail, d'une console ou d'un autre point d'accès. Chaque indication de compromission doit faire ensuite l'objet d'une analyse pour en identifier les contours et en mesurer les risques. CISCO annonce le meilleur taux de détection sur le marché.

C
ARTICLE 09

La maîtrise des données, l'enjeu majeur de la transformation numérique

Intervenants :
Alexandre GARRET, Directeur général délégué d'ORANGE CYBERDENSE
Gilles BERTHELOT, Responsable de la sécurité des systèmes d'information - SNCF Réseau
Philippe COURTOT – PDG de Qualys
Frédéric ZINC, Directeur de l'activité « infrastructure et mobilité » d'ORANGE CYBERDEFENSE
Frédéric Malagoli, Gestion vulnérabilité d'ORANGE

Résumé des interventions :
Il a été créé en deux ans presque autant de données que depuis l'existence de l'homme. Ces données sont de plus en plus éparpillées, hébergées sur des bases dont la localisation et les mesures de sécurité restent inconnues. A cela s'ajoute le désarroi des entreprises face à la vulnérabilité de leurs systèmes. Pour endiguer ces difficultés, les fournisseurs de solutions de cybersécurité ont alors développer des services souverains, à l'instar d'Orange.

I – Les raisons du développement des services souverains

A titre préliminaire, il est important de s'attarder sur la notion de « service souverain » qui peut se définir par le biais de trois grandes caractéristiques, à savoir la localisation des données, leur l'étanchéité vis-à-vis de l'extérieur et la capacité à opérer cette solution de bout en bout. Autrement dit, et à titre d'exemple, un service souverain français se doit de garder les données de ses clients en France, de manière sécurisée tout en les administrant avec du personnel français. Le « service souverain » ne doit pas être confondu avec la « solution souveraine » en ce qu'il n'inclut pas une maîtrise entière des solutions techniques. En proposant des services et non des solutions, Orange n'a ainsi pas choisi une technologie française mais américaine avec l'entreprise Qualys, n'empêchant nullement de valider un haut niveau d'étanchéité et de localisation des données.

Pour quelles raisons proposer ces services souverains ? Il existe une

certaine attente des clients sensibles à la souveraineté et à la sécurité mais aussi des clients contraints de choisir des solutions souveraines. Les OIV sont notamment dans ce cas. Les besoins se font donc ressentir et l'offre se fait, logiquement, plus grande et plus variée.

II – L'existence de trois modèles de services souverains proposés par ORANGE

L'opérateur Orange offre divers services souverains mais trois retiennent l'attention : le SOC souverain, Calypso, et le Mobile Network Intrusion Detection System.

Le SOC existe déjà depuis plusieurs années, décliné du modèle low cost au plus complexe comme le cockpit sécurité qui se résume à une alvéole complètement étanche pour des services très critiques. Orange a repris ce dernier modèle et y a ajouté la caractéristique de souveraineté aux fins de créer un écosystème de confiance. Il s'agit de garantir à ses clients, le transport de la donnée, en les faisant transiter sur ses réseaux privés en étant réactif face aux attaques et proactif dans la prévention. Orange s'appuie sur un certain nombre d'observateurs déployés un peu partout sur le réseau.

Basé sur la technologie proposée par Qualys, Calypso, lui, est un service de gestion des vulnérabilités qui scanne les systèmes d'exploitation des clients. Il permet de garantir la localisation en France des données, données principalement de configuration et de résultats des scans qui contiennent donc la liste des vulnérabilités des systèmes d'informations des clients. Cette plate-forme réalise en moyenne un milliard de scans par an, soit un volume atteignant les 500 milliards d'informations relatives à la sécurité. En sus de cette plate-forme technique, Orange propose d'autres services tels que le « vulnerability operation center » qui se résume à des équipes dédiées exploitant les résultats produits par Calypso pour apporter de l'expertise et produire des rapports aux clients sur l'état des vulnérabilités de leurs systèmes.

Directement construit en mode souverain, la solution « Mobile Network Intrusion Detection System » permet de sécuriser la mobilité. Il est vrai qu'il existe des offres classiques, voire même des offres beaucoup plus évoluées en termes de sécurité mais qui sont toutes concentrées sur le device (mobile). De facto, le client est dépendant du modèle, de l'OS, des applications intégrées, etc. En revanche, il y a un point de concentration de tous ces objets : le réseau mobile. Par ce biais, quantité d'informations sont extraites pour apporter de la sécurité et identifier les risques. Une nouvelle fois, le service reste souverain par l'hébergement sur les DataCenter Orange et par la gestion des équipes de l'opérateur.

III – SNCF Réseau, l'exemple d'un client

SNCF Réseau fait partie des OIV. Des obligations découlent de ce statut. Un décret du 27 mars 2015 impose ainsi aux OIV de mettre en place des systèmes de détection des intrusions dont ils font l'objet et de procéder à des audits en faisant appel soit à l'Agence Nationale de la Sécurité des Systèmes d'information (ANSSI), soit à des prestataires labellisés.

Avant de choisir le prestataire avec lequel elle allait travailler, l'entreprise SNCF Réseau a établi deux constats. Le premier est que l'entreprise est tournée vers la production centrique qui a tendance à privilégier le fonctionnement à la sécurité. Tout ce qui est détection de vulnérabilité qui permettrait d'avoir une meilleure lisibilité de la sécurité passe après la disponibilité des services auprès des clients. Le second constat fait référence au périmètre étendu de la SNCF en termes de couverture. Par conséquent, le traitement de vulnérabilité sur les systèmes d'information doit passer par l'industrialisation pour permettre un service souple et adaptatif. Par ailleurs, SNCF Réseau, étant

un opérateur stratégique de l'État, ne peut pas se permettre de divulguer des données sensibles et en particulier ses vulnérabilités. Les dirigeants ont donc fait le choix pragmatique d'aller vers une solution souveraine avec un partenaire de confiance, Orange, à partir d'une solution leader du marché, Qualys. Cette décision avait bien pour objectif d'héberger à la fois leurs données, d'avoir des infrastructures localisées en France et d'avoir des opérateurs techniques français ayant une réelle maîtrise sur toute la mise en sécurité de leurs vulnérabilités.

Le rythme auquel SNCF Réseau utilise la solution est soutenu car il est prévu un scan par mois des IP de productions ainsi que des scans à la demande pour répondre à diverses questions : qu'est ce qui est exposé ? quelle est la surface d'exposition pour telle ou telle faille ? Le scan permet alors d'informer le manager et d'aider la production à traiter les vulnérabilités.

Glossaire :

OIV : opérateur d'importance vitale. Ce sont des entreprises dont l'activité est jugée stratégique pour la nation.
SOC : Security Operations Center.
OS : operating system (système d'exploitation)

C
ARTICLE 10

Les stratégies de lutte anti-cybercriminalité

Résumé des interventions :
La cybercriminalité représente désormais un véritable défi pour de nombreux pays. Les cas de l'Allemagne, du Royaume-Uni et de la France ont ici été analysés. Bien que chacun ait sa vision de la question et des moyens de lutte à mettre en œuvre, une des perspectives communes est de parvenir à une coopération la plus étendue possible pour obtenir une lutte efficiente. Tout doit être entrepris afin que l'ensemble des acteurs concernés disposent d'un niveau de compétence adapté à l'évolution des menaces. Des politiques plus orientées vers les victimes sont également envisagées.

Les États sont de plus en plus contraints d'élaborer des stratégies de lutte contre la cybercriminalité. En Europe, des pays comme l'Allemagne, le Royaume-Uni et la France ont choisi d'axer leurs politiques sur cette problématique et de multiplier les coopérations.

L'enjeu de la problématique en Allemagne

Le déploiement du cyber à travers le monde a contribué à l'apparition de nouvelles infractions comme la pédopornographie, les cas d'usurpation d'identité, la vente de drogue, d'armes, d'explosifs en ligne, ou bien encore les phénomènes de radicalisation.

De tels problèmes sont pris très au sérieux par les autorités allemandes qui ont mené, en 2013, une étude sur un important échantillonnage de cas de cybercriminalité afin d'en évaluer les conséquences sur l'économie. L'étude montre que les forces de police n'ont connaissance que d'une infime partie des infractions commises en ligne. En effet, nombre de victimes ignorent l'existence des cyberattaques dont elles ont fait l'objet. Une des priorités

Intervenants :
- Sabine VOGT, Head of Direction Serious and Organised Crime, BKA
- Jean-Yves LATOURNERIE, Chargé de la lutte contre les cybermenaces, Préfet
- Jamie SAUNDERS, Director, National Cyber Crime Unit
- Denis FORTIER, Directeur de la rédaction, AEF Sécurité Globale

est alors de faire prendre conscience à la population des risques courants dans le cyber, comme celui du phishing, d'autant plus que les connaissances techniques des criminels ont tendance à s'accroître.
Dans un monde où les interconnexions sont croissantes et où la maison connectée est le symbole du futur, l'Allemagne est devenue un pays très dépendant de l'industrie cyber. Elle se doit d'y faire respecter un certain nombre de règles. L'anonymisation des données apparaît comme un des principaux défis. A cela s'ajoute un enjeu économique visant à limiter les pertes financières causées à certains secteurs. Ainsi, on voit que la lutte contre la cybercriminalité comprend des objectifs à la fois politiques, économiques, militaires mais aussi scientifiques. A cette fin, l'Allemagne a mis en place un office fédéral pour la sécurité informatique. Ce dernier fournit des informations aux forces de police allemandes et élabore des stratégies de lutte issues des analyses effectuées à partir de cas d'attaques informatiques. L'office réalise un important travail de collecte d'informations et accentue ses efforts sur la mise en œuvre de stratégies de prévention, stratégies auxquelles les plus jeunes doivent être associés. Pour parvenir à identifier les cybercriminels et les empêcher de nuire, l'Allemagne dispose également d'un centre national de cyberdéfense auquel l'agence allemande de sécurité est associée. Le choix de mettre en commun les compétences des deux entités a été fait afin d'obtenir une lutte plus efficace. Le pays associe de nombreuses autres agences et met en avant le fait qu'une alliance entre les agences nationales des différents États pourrait être une solution intéressante.
L'office tente par la même occasion d'établir davantage de liens avec les industries, elles-mêmes plus qu'inquiètes face à la menace que représentent les groupes cybercriminels. Une des stratégies est d'expliquer aux différents acteurs, pouvant être ciblés par les hackers, les précautions à prendre pour limiter les risques de cyberattaque.
Au niveau mondial, les autorités allemandes considèrent qu'un échange plus rapide d'informations entre les différents services de police est primordial. L'élaboration d'une coopération internationale luttant contre la cybercriminalité favoriserait une meilleure jonction des initiatives. L'Europe, par le biais d'Europol, a cherché à le faire avec l'instauration de la plate-forme « J-CAT » (Joint Cybercrime Action Taskforce) qui contribue au partage de données. Il s'agit là de la structure de coordination spécialement dédiée à l'anticybercriminalité au sein de l'Union Européenne et au-delà. Une extension de cette initiative à l'international est aujourd'hui nécessaire. Des efforts en terme de formation des enquêteurs sont également à entreprendre en vue d'améliorer leurs connaissances et leurs compétences.

Les stratégies de lutte au Royaume-Uni

En 2013, la « National Crime Agency », agence destinée à coordonner les différents services de lutte contre le crime organisé, a été créée au Royaume-Uni, aux côtés de nombreuses autres agences privées. Elle regroupe à la fois des enquêteurs traditionnels et des personnes ayant des compétences spécifiques en matière de lutte contre la cybercriminalité. Tout l'enjeu est de parvenir à maintenir un haut niveau de compétences chez ces experts.
Le Royaume-Uni affiche des intentions claires : devenir une terre hostile à la mise en œuvre des projets des cybercriminels. Il s'agit là de la première des priorités. Des efforts sont aussi portés sur la recherche des origines de l'engrenage de la cybercriminalité et sur l'amélioration des moyens de défense accordés aux victimes. Pour y parvenir, le Royaume-Uni a pris pour habitude de collaborer avec la France et l'Allemagne. Les pays développent en commun des techniques de cryptographie et partagent

leurs banques de données sur les malwares et les botnets. Ils cherchent ainsi à envoyer un signal fort aux cybercriminels.
En somme, la stratégie adoptée par le Royaume-Uni repose sur trois challenges : parvenir à construire une coopération à l'échelle internationale, pénétrer puis détruire le marché de la cybercriminalité, et faire en sorte que l'industrie d'Internet réduise les attaques et protège mieux les utilisateurs.
Il convient de ne pas focaliser les enjeux uniquement sur la lutte contre les cybercriminels, mais aussi de se pencher davantage sur la situation des victimes.
Actuellement, les forces de police locales ne sont pas suffisamment armées pour répondre aux demandes relatives à la cybercriminalité. Il reste donc du chemin à parcourir pour s'adapter à cette forme de criminalité mouvante.

Les priorités du Ministère de l'Intérieur français

La France a, quant à elle, pour objectif de lutter contre toutes les formes de cybercriminalité. Elle cherche à améliorer sa cyberdéfense en protégeant notamment les opérateurs d'importance vitale, les intérêts nationaux permettant la continuité de la vie de la nation, et les systèmes d'informations des petites et grandes entreprises comme des particuliers.
Afin de coordonner les actions des différents services du ministère traitant de la question, l'initiative a été prise de désigner une entité chargée de mettre tous les éléments de cybersécurité en cohérence, à la fois en ce qui concerne la politique menée que les adaptations aux évolutions constatées. Ce nouvel acteur doit veiller à ce que les objectifs fixés soient atteints avec le minimum de perte d'efficacité possible du fait de la dispersion des actions entre services.
Pour autant, il n'est pas encore question de créer, à côté de l'ANSSI, une agence spécialisée dans les cybermenaces. Seule une petite équipe est chargée de mettre en synergie les services concernés. La stratégie est donc de tout faire pour disposer d'une vision claire et actualisée des cybermenaces.
Pour y parvenir, le ministère a mis en place la réalisation annuelle d'un rapport sur l'état des menaces dans le cyberespace. Les statistiques françaises des crimes et délits ne prenant pas en compte cette dimension cyber, l'idée est d'établir, pour l'avenir, des indicateurs relatifs aux faits constatés en cyberdélinquance et en cybercriminalité.

C
ARTICLE 11

Cyber risques : quelles priorités pour

Intervenants :
Vincent TRELY, président, APSSIS
Jimaan SANE, technology, media and business underwriter, Beazley
Christophe FICHET, avocat, cabinet Simmons & Simmons
Philippe LOUDENOT, fonctionnaire de la sécurité des système d'information des ministères sociaux

Résumé des interventions :
Le monde de la santé est pleinement exposé à la problématique des cyber attaques, les données contenues par ces établissements relevant d'une stricte confidentialité. L'enjeu de l'atelier est de comprendre l'importance et la gravité des attaques informatiques qui touchent ces données , mais aussi la nature de l'intérêt que portent à ces dernières les cyber délinquants.

Le monde de la santé brasse quantités d'informations relatives à la vie privée de millions de personnes. Protégées par la loi et le secret médical, ces informations suscitent la convoitise de certains criminels. Chacune constitue une donnée secrète qui pourrait être définie comme étant la correspondance entre une identité et une pathologie, quelle qu'elle soit. A titre d'exemple, une programmation de rendez vous est d'ores et déjà considérée comme une donnée secrète. Les plans de développement des hôpitaux ne sont pas secrets puisqu'ils sont en ligne. Toutes les données à l'intérieur des centres hospitaliers ne sont pas secrètes non plus. Ce que nous appellerons « donnée secrète » concerne donc surtout les données liées aux patients (dossiers médicaux, carnets de rendez-vous, résultats d'analyses et examens...).

Un dossier médical a une valeur estimée à 250 dollars en termes de revente sur les marchés délinquants. Il contient en effet des données très

utiles comme les adresses, les numéros de téléphone, le numéro de sécurité sociale, les données concernant les assurances maladies, les renseignements sur les pathologies et les arrêts maladie, sur les médecins déjà visités, etc. A l'heure actuelle, aucun cas de plainte pour des dossiers mis en ligne sur Internet n'a encore été recensé en France. Il faut souligner que la loi française impose des conditions strictes de sécurisation de ces données.
Si les établissements de santé sont aujourd'hui des cibles, il faut souligner que les données des appareils connectés achetés, par exemple, dans des magasins de sport spécialisés, contiennent également des données « médicales » et deviennent des cibles. Ils sont classés comme des appareils de confort et de bien-être et leurs constructeurs ne sont pas soumis aux mêmes obligations en termes de sécurisation des données recueillies.
La marge de progression des hôpitaux en matière de cybersécurité est pour autant largement perfectible. C'est nécessaire car dans le monde médical comme ailleurs, l'heure est à la numérisation et à l'échange de données entre professionnels (et, dans une certaine mesure, patients). Les directeurs de centres hospitaliers prennent progressivement conscience de cette nécessité et des efforts sont faits pour améliorer la cyber sécurité des établissements. Des grandes directives sont données par le biais de la politique de protection et de sécurité des documents détenus par l'Etat baptisée « Politique générale des système d'information du monde de la santé ».

Les directeurs des hôpitaux et les responsables des sociétés qui y interviennent portent la responsabilité de la sécurisation des domaines qui les concernent. Il y a un risque légal bien réel si les choses ne sont pas faites en pleine conformité avec les obligations légales déjà évoquées.
Les experts visiteurs de la haute autorité de santé détiennent ainsi le pouvoir de fermer un service hospitalier s'ils y découvrent une faille du système d'information. C'est une possibilité nouvelle puisqu'auparavant un hôpital ne pouvait être fermé que pour des raisons liées à la sécurité médicale des patients. Dans le domaine des hôpitaux comme ailleurs, nul n'est censé ignorer la loi, notamment les responsables d'établissements.

ARTICLE C 12

Adopter une vision d'attaquant pour protéger votre patrimoine

Intervenants :
- Yanne COURCOUX, directrice de la MEITO
- Tiphaine LEDUC, Chef de projet Cyber & animatrice de la Table ronde
- Sébastien HERNIOTE, IMOSSYS
- Nicolas JOLIVET, TOVALIS
- Fabrice CLERC, 6Cure
- Guillaume PRIGENT, DIATEAM

Résumé des interventions :
Certaines entreprises peuvent se trouver démunies face à une attaque Cyber. Cette conférence permet de dérouler différents scénarios d'attaque, en se mettant dans le rôle de l'attaquant, et les méthodes de défense qui leur sont adaptées. Il s'agit d'adopter de bons réflexes pour réagir efficacement, selon une approche pragmatique, via l'analyse de la menace et la hauteur de ses enjeux. Quatre mesures-phares à mettre en œuvre sont présentées en fonction du type d'attaque. Faciles à mettre en place, elles s'adressent à tous les types de structure qui pourront ainsi maîtriser leur budget en ciblant leurs vulnérabilités.

I – Les scénarios d'attaque :

L'audit technique de sécurité permet d'adopter le point de vue de l'attaquant (les thèses d'intrusion) pour évaluer la sécurité du système d'information. Ce sont deux approches qui, in fine, mettent en capacité des experts d'identifier des vulnérabilités, de les exploiter et de les coter. Ces vulnérabilités peuvent être identifiées sur des systèmes d'information, sur certaines cibles ou produits.

Les vulnérabilités qui ouvrent une porte d'entrée dans un système sont multiples. Elles concernent tous les services applicatifs exposés sur Internet (portail WEB, niveau de sécurisation des CMS – Content Management System – déployés sur certains sites), mais aussi le système d'information en lui-même, avec les services WIFI utilisés pour relier deux points géographiquement proches, ou le réseau LAN (Local Area Network).

Le but de ces experts est d'exploiter jusqu'au bout ces vulnérabilités afin

d'estimer et de classer la criticité de ces vulnérabilités sur l'aspect de la facilité ou au contraire de la complexité de leur exploitation. Pour ce faire, ils vont se poser des questions telles que : quelles doivent être mes compétences ? Me faut-il du matériel spécifique ? Ai-je besoin de complicité en interne ? Puis ils vont évaluer la qualité de l'impact s'ils devaient exploiter cette vulnérabilité. Il existe aussi l'évaluation des produits de sécurité, en se plaçant toujours du point de vue de l'attaquant. À ce propos, des prestations d'audit existent. Ainsi, l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) essaie de réguler ces prestations en délivrant des labels à des sociétés de confiance, tels que la qualification PASSI (Prestataire de l'Audit de la Sécurité des Systèmes d'Information) ou bien du label CESTI (Centre d'Evaluation de la Sécurité des Technologies d'Information).

Un attaquant a aujourd'hui beaucoup de moyens de collecte pour récupérer des informations et reconstituer l'environnement de l'entreprise, via par l'exemple l'OPEN DATA. L'attaquant peut très bien se déplacer physiquement, capter les réseaux WIFI, observer les entrants et les sortants, puis faire des attaques d'ingénierie sociale pour récupérer des informations un peu plus précises. Ce dernier est encore à la phase de planification lorsqu'il réalise de petites attaques informatiques pour compléter davantage ses informations. L'objectif de l'attaquant est d'analyser en premier lieu l'entreprise et toutes ses dépendances tant à l'extérieur qu'à l'intérieur, de manière à concentrer son offensive sur un élément qu'il aura ciblé au regard de son analyse.

La logique de l'attaquant a changé. Bon nombre d'attaques ont pour objectif premier de prendre à contre-pied les dispositifs existants de protection, de sécurité ou de détection. L'attaquant ne va plus chercher à réaliser une intrusion dans le système d'information (SI), ni à voler des données ou à les détruire. Il va plutôt chercher à bloquer le système d'information de l'entreprise. Il est important de se rendre compte que les buts de guerre de l'attaquant sont différents des modes opératoires qu'il pourrait a priori utiliser et contre lesquels nous cherchons à nous prémunir. Si l'entreprise oriente sa sécurité pour se protéger des intrusions, des visites indésirables, elle aura mis en place des systèmes de détection qui vont pouvoir surveiller les signaux d'intrusion informatiques et mettre en œuvre des systèmes de contre-mesure. Si l'attaquant choisit plutôt de bloquer le système de l'entreprise, notamment les flux entrants et sortants, les dispositifs de surveillance déployés à priori ne seront pas adaptés à cette nouvelle stratégie d'attaque. Il faut donc mettre en œuvre des outils adaptés de manière à mieux détecter ce type d'attaque appelé « déni de service » ou « déni de service distribué ». Les premières attaques de ce genre ont été des attaques massives, dites de flooding : elles consiste à envoyer de manière simultanée une très grosse quantité d'informations en apparence légitimes de manière à saturer et bloquer d'emblée le système d'information visé. Il existe des variantes beaucoup plus discrètes et plus astucieuses à ces attaques, dites attaques « pulsantes ». Au lieu d'observer une augmentation significative des flux qui va saturer la bande passante de manière massive et continue, il y aura des pics d'attaques éphémères qui dureront quelques secondes voire un peu moins. L'attaquant s'est aperçu que ce type de mode d'action était plus intéressant car plus difficile à détecter du fait de son caractère éphémère. Pour autant, le système d'information visé mettra plus longtemps à récupérer. En cas de pulsations à intervalles réguliers, le système d'information va peu à peu accumuler du retard. Il va subir des pertes de performances qui passeront relativement inaperçues dans un premier temps, pour finalement bloquer totalement le système ou du moins entraîner

une dégradation suffisante des performances et le mettre en difficulté.
Il y a une différence entre le mythe et la réalité pour les systèmes d'information industriels tels que SCADA, ICS, SMART-GRID… Il est en effet coutumier de croire qu'ils sont sécurisés car totalement hermétiques à Internet. En réalité, selon une étude de POSITIVE TECHNOLOGIES qui a testé 50 infrastructures, 100 % des systèmes d'information industriels sont interconnectés ou connectables. En outre, 90 % de ces systèmes sont directement attaquables notamment par des outils tels que metasploit et 70 % des postes de supervision utilisent en parallèle des postes informatiques et de gestion. Il s'agira au final pour l'assaillant d'ajuster son angle d'attaque en fonction des possibilités qu'il a de pénétrer le système.

II - Des solutions défensives :
Le cyberespace est devenu un véritable milieu avec ses tempêtes en déni de service, ses pandémies virales, ses logiciels malveillants, ses conflits et bientôt ses guerres, ses cambriolages et ses hold-up. Tout organisme qui veut avoir pignon sur le Web se doit d'être sécurisé à la hauteur des enjeux et des risques qu'il est susceptible de rencontrer. La menace existe et s'amplifie, elle est plus ou moins forte en fonction de la cible. Les attaquants ont différents potentiels d'attaque : des attaques de faible niveau comme les campagnes d'effacement de sites non protégés, des attaques d'un niveau supérieur telles que le cyberespionnage et l'espionnage économique et enfin des attaques de cyberterrorisme ayant des conséquences physiques. Une des mesures fondamentales pour que les structures puissent se protéger a minima est d'avoir des systèmes et des logiciels rigoureusement à jour avec des patchs de sécurité effectivement appliqués. Il s'agit également de vérifier si les services inutiles sont désactivés car ils sont autant de portes d'entrée potentielles. Pour lutter contre l'espionnage économique, il faut en revanche faire appel à des postures défensives de lutte informatique avec des notions de supervision des systèmes, de détection des intrusions et de réaction, autrement dit s'articuler autour de technologies onéreuses.
Il est nécessaire d'identifier l'environnement dans lequel l'entreprise évolue, de manière à pondérer les corrections liées à la crédibilité des attaques qui peuvent avoir lieu. Le point de départ est donc de définir quelles sont les données sensibles de l'entreprise, pour ensuite imaginer des scénarios d'attaque.
Dans le contexte de disponibilités des données, il faut s'appuyer sur des solutions de sécurité qui vont pouvoir être déployées pour différents fournisseurs, chacun à leur niveau, afin d'optimiser le dispositif de défense et de neutralisation de ce type d'attaque, et offrir un dispositif « sans couture ». Cela implique que chacun puisse sensibiliser ses fournisseurs en vérifiant que chaque fournisseur à son niveau se trouve en capacité d'apporter une solution dimensionnée. A chaque niveau, un dispositif de filtrage devra être adapté pour une complémentarité intelligente d'outils moins chers et plus efficients.
Il faut mettre l'utilisateur dans la boucle, en renforçant tout particulièrement le firewall humain, par des publications, par de la sensibilisation initiale, par des formations ou de l'entraînement à la gestion de crise dans un environnement représentatif. Il s'agit de tester le comportement des équipes au moyen de jeux d'attaques-défenses, de jeux de tests de vulnérabilité ou d'exercices de « force brute » dans de véritables environnements de sites Web.

C
ARTICLE 13

Quelles solutions pour la sécurité des systèmes industriels ?

Résumé des interventions :
Les systèmes industriels sont présents dans presque tous les secteurs de l'industrie. Longtemps considérés comme étant insensibles aux attaques informatiques, ils sont devenus des cibles du fait de l'interconnexion croissante des réseaux. L'impact des attaques qui les touchent est potentiellement très important. Il est essentiel de prendre des mesures pour se prémunir contre celles-ci, éventuellement en allant au-delà des obligations légales en la matière.

Intervenants :
- Eric WEBER, chef du service produits de sécurité, Thales
- Thieyacine FALL, directeur de mission, Thales

Les systèmes industriels présentent des caractéristiques et des besoins très spécifiques, liés à la criticité des processus de production (performances, fiabilité, sûreté, maintenabilité, compatibilité). La réponse aux menaces informatiques doit donc intégrer ces contraintes en limitant au maximum l'impact sur la conduite et l'exploitation. Cette conférence, présentée par Thales, est l'occasion de faire le point, par la pratique et l'exemple, sur les solutions et les services de sécurité adaptés aux enjeux techniques, financiers et humains du secteur. Aujourd'hui les systèmes industriels sont dans tous les secteurs : industrie (alimentaire, chimie/pharmacie), énergie (production, distribution), Infrastructure et équipement, défense, santé, etc... Ils étaient autrefois ignorés mais sont devenus aujourd'hui la cible des hackers (cyberattaque dans le secteur de l'énergie norvégienne, dans une usine de métallurgie allemande, *etc...*).

Ces attaques produisent des effets dévastateurs en terme géopolitiques (pressions, conflits, renversements de régimes), hu-

mains, financiers (arrêts de production, destruction du process) mais aussi en termes de compétitivité et de réputation (non qualité, vol de savoir-faire). Deux attitudes sont à éviter : le déni de cyberattaque et l'excès de confiance en pensant être protégé par un pare-feu, un anti virus ou en se sentant invulnérable. Pourtant les risques sont partout. Les systèmes aujourd'hui sont complexes et fortement interconnectés. Ils sont hétérogènes car des fournisseurs différents utilisent des protocoles propriétaires, adaptés pour répondre aux besoins. Une fois déployés et qualifiés, ces systèmes sont figés. Ils sont également bâtis sur des standards sans mesures de sécurité (OS Microsoft sans patch, protocoles TCP, DNP3, OPC). Pourtant il s'agit d'un problème culturel. Le système a besoin de résilience et les systèmes industriels n'ont pas été conçus en intégrant le risque cyber. Les processus ne prennent pas en compte cette dimension. De plus, les personnels ne sont ni formés, ni sensibilisés.

Partant de ce postulat, plusieurs mesures sont à l'étude et figurent dans a loi de programmation militaire 2014-2019. En ce qui concerne les opérateurs d'importance vitale, (OIV), l'ANSSI a défini 12 secteurs stratégiques pour le pays :défense, énergie, transport, traitement de l'eau, industries critiques. Cela concerne plus de 250 entreprises.

Des dispositions phares ont été prises comme la notification des incidents de sécurité avec l'obligation pour les OIV de notifier les incidents significatifs intervenant sur leurs systèmes industriels critiques et la mise en place d'un SOC (Security Operation Center), interne ou externalisé, certifié par l'ANSSI et opéré depuis le territoire national. Un SOC constitue pour les équipes de sécurité ce qu'une tour de contrôle est au pilote d'avion : un système de détection, de prévention du risque, d'alerte et d'aide à la décision.

Il permet à l'entreprise de répondre à son objectif principal : garantir la continuité de ses activités métiers en s'adaptant au mieux et au plus vite aux contraintes et risques liés à l'hyper-connectivité. De plus, il établit l'obligation de se soumettre à des contrôles, par des prestataires certifiés par l'ANSSI, d'appliquer un ensemble de règles de sécurité (guide hygiène informatique de l'ANSSI, application des mesures détaillées par les systèmes industriels de l'ANSSI). Cela fera l'objet d'un décret d'application en 2015.

Pour réussir, des facteurs ont été identifiés pour la sécurisation d'un ICS (Industrial Control System) comme l'intégration de la sécurité dans les architectures, la régulation. Du côté des industriels, de nouvelles compétences sont à développer entre le monde IT et le monde industriel par les experts en cybersécurité des systèmes industriels. C'est pourquoi Thalès a défini trois étapes de la sécurisation chez les opérateurs. Tout d'abord, il faut réaliser un point précis sur l'état des équipements et des logiciels existants par un audit pragmatique de sécurité avec identification des zones à risques en intégrant tous les paramètres et en matérialisant l'impact d'une menace. Dans un second temps, le plan de sécurité doit être défini, phasé et appliqué. Il s'agit de le mettre en place en sécurisant les interconnexions, et en durcissant postes et serveurs. Une formation et une identification des personnels responsables est nécessaire. Enfin, il faut vérifier la bonne application du plan. Enfin, la 3ème étape consiste à maintenir le niveau de sécurité dans le temps : gestion de la sécurité, sensibilisation des acteurs, vérification régulière, amélioration continue de la sécurité.

ARTICLE C 14

Cyberextorsion : du cryptolocker à la rançon en bitcoins

Résumé des interventions :
Une rétrospective des attaques les plus marquantes de l'année 2014 permet de mieux comprendre, au travers de cas concrets, les évolutions futures des logiciels malveillants. Le marché noir de la vente d'outils destinés à dérober des données personnelles bancaires et d'authentification est une réalité. Afin de se prémunir contre ces attaques, il existe des solutions, tant pour le monde de l'entreprise que pour celui des particuliers.

Intervenants :
- Jean-Ian BOUTIN, malware researcher, ESET

I – Les risques numériques dans le domaine de la santé

Les données de santé sont sensibles et, pour une grande part, confidentielles. Elle ont une grande valeur sur le marché noir des données et intéressent beaucoup les géants du numérique. En premier lieu, si les flux sont sécurisés, comme l'impose la loi, il est impossible de procéder au chiffrement de plusieurs millions d'entrées d'une base de données. Le système demeure donc intrinsèquement vulnérable.

Si le corps médical tient par principe à ce caractère confidentiel (secret médical), il est encore insuffisamment au fait des spécificités du numérique, par méconnaissance. Confronté à l'urgence d'une situation, un médecin n'utilisera pas sa connexion sécurisée, avec une carte à puce CPS et son code PIN, trop contraignante et chronophage. Il demandera, par exemple, l'avis à un confrère par sa messagerie personnelle en utilisant son téléphone ou sa messagerie Gmail. Pour bénéficier de matériel plus performant que celui de l'hôpital, un médecin peut préférer étudier à domicile un dossier qu'il aura préalablement en-

registré sur son ordinateur personnel. De même, ayant accès au système d'information de l'établissement hospitalier, il peut outrepasser ses droits et consulter le dossier informatique de patients autres que les siens. Il arrive également que des données restent visibles sur des écrans d'ordinateur accessibles par tout un chacun dans l'enceinte de l'établissement et que des photographies d'écrans soient prises pour récupérer les données médicales. Les contentieux à ce sujet se multiplient. Un autre exemple édifiant est celui de l'utilisation d'une plate-forme non sécurisée par des praticiens qui avaient contourné l'intervention du DSI ou du RSSI (l'article L1111-8 du Code de la santé publique prévoit un agrément des hébergeurs des données de santé publique, dont la liste est publiée sur le site de l'Agence des systèmes d'information partagés de santé). Pour le professionnel de santé, la priorité reste le soin et la santé du patient, pas la sécurité, dont il ne mesure pas toujours les enjeux.

Une autre problématique concerne les données dans les appareils biomédicaux, dont la maintenance et la supervision sont réalisées à distance, souvent à l'étranger. Deux plate-formes ont été piratées aux États-Unis : on ignore la nature des données piratées et ce qu'elles sont devenues. D'autre part, on ne s'interroge pas sur l'anonymisation des clichés ainsi envoyés ni sur l'usage qu'il pourrait être fait des données transmises. Le danger est encore plus prégnant en ce qui concerne leur revente sur le marché de l'occasion, pour l'Europe de l'Est ou l'Inde : le plus souvent, les données ne sont pas effacées avant la cession des appareils. La maîtrise des données qui transitent par les objets connectés consacrés au Quantified self est également une illusion : si Google, Apple, Microsoft etc, garantissent une chaîne de transmission sécurisée, on peut s'interroger sur le sort final des données et leur traitement par les développeurs et les grands fournisseurs des applications. Or, ces questions vont se poser de manière de plus en plus aiguë, les géants du Net investissant massivement dans le domaine de la santé. D'une manière générale, la multiplication des interconnexions augmente les risques de perte et de captation.

Négligence, manque d'informations sur le fonctionnement des réseaux informatiques, résistance à l'authentification forte pour des raisons d'impératifs professionnels sont autant de causes qui menacent la confidentialité des données, lesquelles peuvent alors fuiter ou être volées.

Enfin, les appareils biomédicaux (scanner, échographe, pousse-seringue..) peuvent subir l'attaque d'un virus ou être piratés. Une prise en main à distance pour changer les paramètres est envisageable. Les conséquences peuvent être graves. Des expériences ont été réalisées : il est techniquement possible de prendre le contrôle à distance d'un pacemaker pour en modifier les variables ou d'un pousse-seringue automatique pour changer les dosages.

Même si l'acte n'était pas malveillant, à Épinal, les programmes de radiothérapie avaient été modifiés en interne : il a été reconnu que le bug informatique provoqué par cette manipulation a été en partie responsable de l'irradiation de plusieurs patients. Cela prouve la grande vulnérabilité des logiciels et l'usage criminel qui peut donc en être fait.

II – Les moyens de lutte

Plusieurs pistes sont préconisées. Il serait souhaitable d'améliorer la formation des professionnels de santé, de les sensibiliser aux risques existants afin qu'ils modifient leurs comportements. Les services de sécurité informatique ont un rôle important d'accompagnement pour les inciter aux bonnes pratiques et éviter les mésusages. Dans un secteur où les obligations ne sont pas toujours bien vécues, il est nécessaire de réaliser ce travail de persuasion pour obtenir une adhésion aux mesures de sécurité, actuellement perçues comme des contraintes. Le dia-

logue entre le monde de la santé et le monde du numérique devrait être amélioré. En effet, c'est par des échanges véritables entre les acteurs des différents métiers que les progrès pourront se réaliser.

Néanmoins, il est également indispensable de proposer aux praticiens des solutions de sécurité adaptées à leurs besoins et aux réalités de leur métier. Ainsi, l'utilisation de la carte CPS (carte d'identité professionnelle électronique attribuée aux professionnels de santé certifiés par leurs ordres) pourrait être simplifiée en intégrant une technologie de contact qui maintienne le même niveau de sécurité. Le patient, en tant qu'utilisateur, notamment des objets connectés, doit également faire preuve de vigilance.

Les budgets consacrés à la sécurisation des données devraient également être plus conséquents, quelle que soit la taille de l'établissement, ses moyens humains et financiers. Effectivement, les organismes étant nécessairement de plus en plus interconnectés, l'interopérabilité exige des niveaux de sécurité équivalents.

Si une réglementation existe (CNIL, Code de la santé publique, décret de 2007 sur le traitement confidentiel médical dans les systèmes d'information de santé, pré-requis de base de l'hôpital numérique...), elle est encore trop souvent déclarative. Les sanctions et les contrôles, pratiqués par des entités externes, sont encore peu nombreux. Le scandale ayant un impact sur la réputation de l'établissement est redouté, les manquements ponctuels au respect strict de la sécurité le sont moins. Des procédures civiles plus fréquentes, sur le modèle des class actions aux États-Unis, pourraient entraîner des conséquences financières à même de convaincre de l'utilité d'investir dans la sécurité. Les assureurs peuvent également constituer un argument de poids pour limiter au maximum les risques. Par ailleurs, si la politique des systèmes d'information de l'État s'applique aux établissements publics, ce n'est pas le cas pour les organismes privés. C'est pourquoi une politique sectorielle est nécessaire. C'est dans ce sens que l'Asip (Agence des systèmes d'information partagés de santé) a entamé des travaux. Un référentiel est en cours d'élaboration en collaboration avec des professionnels de la santé, des juristes, des fournisseurs et des associations de patients. Chaque texte est soumis à commentaires avant publication officielle. Cependant, si un cadre normatif s'impose, il est intéressant de noter que le modèle américain s'est auto-régulé sans intervention de l'État. Il en est ainsi de la loi PIPA (Protect Intellectual Property Act).

Autre initiative : tous les CHU ont rédigé un cahier des charges commun, issu d'un groupe de travail composé de RSSI et d'ingénieurs bio-médicaux, qui a été transmis au ministère de la santé puis à l'Asip.

Une harmonisation des systèmes de santé et de la réglementation européens permettrait d'optimiser les coûts et d'exercer, en ayant un poids plus important sur le marché, une pression plus importante sur les fabricants des équipements bio-médicaux, de manière à ce qu'ils intègrent à leurs dispositifs, dès leur conception, des systèmes de sécurité, tels que des certificats d'authentification, des mises à jour régulières des logiciels. Trop d'interlocuteurs limitent encore la question de la sécurisation numérique à une question matérielle ou considèrent qu'elle relève uniquement de la CNIL, le monde de la santé étant supposé en être affranchi.

C
ARTICLE 15

Quel rôle pour le cyber dans les opérations militaires ?

Intervenants :
- John A. DAVIS, Major général, conseiller militaire supérieur en Cyber pour le Sous-Secrétaire à la Défense (Etats-Unis)
- Arnaud COUSTILLIERE, Contre-amiral, Officier général à la cyberdéfense - EMA cyber - Ministère de la Défense (France)

Résumé des interventions :
Les opérations militaires dans le cyberespace englobent la sécurité des systèmes d'information, la lutte informatique active et la guerre électronique mais recouvrent également de façon partielle les opérations d'information et le renseignement. Quels sont les doctrines et concepts d'emploi mis en place ? Comment ces opérations s'intègrent-elles dans la conception, la planification et la conduite des opérations militaires ? Quelles sont les organisations mises en place aux plans stratégique, opératif et tactique ?

Le Livre Blanc sur la Défense et la Sécurité Nationale du 29 avril 2013 reconnaît, comme dans sa précédente version, la vulnérabilité du cyberespace, « désormais, un champ de confrontation à part entière », fait état d'une typologie des cybermenaces, des risques afférents et par conséquent de l'effort nécessaire de développement des « capacités de cyberdéfense militaires » et d' « une organisation de cyberdéfense étroitement intégrée aux forces disposant de capacités défensives et offensives ». Il précise également que « toute politique ambitieuse de cyberdéfense passe par le développement de relations étroites entre partenaires internationaux de confiance ». Enfin, une doctrine de réponse française face aux agressions informatiques est également clairement exposée et pose la question de l'action militaire face à la cybermenace.

I-Définition de la menace

La cybercriminalité est, sans conteste, un problème d'envergure

mondiale. On constate une variété croissante de menaces dans le domaine du cyber, qui ont un impact sur différents types de cibles. Les sociétés et organismes du secteur public et privé sont régulièrement touchés par des cyberattaques de plus en plus sophistiquées. Les États-Unis ont fait face à divers types de cybermenaces touchant le système financier, le Département de la Défense (intrusion dans le site internet de la Navy), et le domaine des médias (Sony, plus récemment les sites Tweeter et Youtube du Centcoms). Les États-Unis ne sont pas des victimes isolées. On peut citer, à ce titre, l'attaque retentissante du réseau informatique de Saudi Aramco, la compagnie nationale saoudienne d'hydrocarbure causant la destruction de plus de 30 000 systèmes informatiques en 2012.

Par ailleurs, les attaques sont de plus en plus diversifiées. L'attaque de Sony, évoquée précédemment, est singulière et grave. Une entreprise du secteur privée a été mise à mal par un État étranger qui a associé destruction des systèmes, extorsion et intimidation. Le gouvernement américain l'a jugée inacceptable mais qui pour autant, a réagi avec prudence, par le biais de sanctions, pour éviter toute escalade. Dans le cas des sites Twitter et Youtube du Centcoms, on parle d'une activité criminelle relativement commune et de la dégradation de systèmes commerciaux plus vulnérables. Mais il n'est nullement ici question de menace vis-à-vis du système militaire : il n'y a pas eu de perte de renseignements classifiés, pas de pénétration du système militaire, pas d'impact opérationnel notable, si ce n'est celui sur les médias. Identifier et caractériser la menace doivent permettre d'y donner la bonne réponse.

II- Le combat numérique, au cœur du processus opérationnel national

Les différents modèles d'armées existants se doivent d'inclure des capacités de lutte dans le monde des réseaux. La menace terroriste actuelle pose un challenge commun et engage des combats sur de multiples théâtres extérieurs, sur le territoire national et, aujourd'hui, dans le monde virtuel. Le défi qui s'impose donc, en cyberdéfense, est de maîtriser son empreinte numérique, de procéder à des analyses sectorielles de risques, d'adapter ses méthodes et son organisation afin d'anticiper, de protéger et de réagir de manière efficiente en cas de cyberattaque.

A cette fin, le ministère français de la Défense dispose de l'EMA cyber épaulé par l'ANNSI qui, outre ses actions de conseil, de politique industrielle et de réglementation en matière de cybersécurité auprès des entreprises, veille à préserver la souveraineté, l'autonomie de décision et d'action dans les domaines politique, diplomatique et militaire et à protéger l'ensemble des infrastructures critiques. La signature d'un accord général de partenariat pour la recherche avec le pôle d'excellence cyber implanté en Bretagne s'inscrit dans le cadre du pacte Défense Cyber lancé à Rennes par le ministre de la Défense le 7 février 2014.

Les États-Unis ont défini au niveau national les rôles et les responsabilités. Trois acteurs opérationnels majeurs se distinguent. D'abord, le Département de la Justice, au travers du FBI, est compétent pour les questions de sécurité nationale sur le sol américain en relation avec les cybermenaces. Le Département de la Sécurité Intérieure coordonne la protection, la prévention et la riposte aux incidents cyber pour le pays. Enfin, le Département de la Défense (DoD), assure la défense de la nation contre les attaques dans tous les domaines, y compris le cyberespace. Le CYBERCOM, sous commandement interarmées de combat, subordonné à l'unité de commandement stratégique des États-Unis, a été créé en 2010 dans le but de renforcer l'action cyber.

Ces relations et partenariats sont à prendre en compte à quatre niveaux différents : au niveau national, être un membre efficace

dans une équipe, c'est détenir des compétences et des capacités à mettre en commun et il tient à cœur au DoD de veiller à l'efficacité de ses membres au sein d'une équipe élargie ; au niveau des agences gouvernementales, un effort a été fait pour mettre en place différentes équipes fédérales de cybersécurité impliquant d'autres ministères (Affaires étrangères, commerce, Trésor) ; au niveau industriel, les entreprises détiennent et gèrent la plus grande partie du cyberespace, sur lequel les institutions gouvernementales s'appuient, y compris l'armée, pour mener à bien leurs opérations.

Cette action collective sur le plan national, français ou américain, demande un investissement conséquent dans l'organisation et l'équipement. La formation et les divers exercices d'entraînement permettent à la cyberdéfense d'un pays de gagner en maturité. Les programmes de formation sont destinés aux personnels des équipes de cyberdéfense du réseau national et, outre Atlantique, des équipes de « missions de combat » qui intègrent le cyber à la planification opérationnelle. L'objectif est d'anticiper la menace mais également d'être capable de défendre la nation contre une attaque touchant la sécurité nationale ou l'économie et de s'assurer de la capacité de riposte en tant que force militaire.

La cyberdéfense est un domaine qui, depuis quelques années, gagne en maturité notamment grâce aux divers exercices d'entraînement menés par les cellules de crise. L'armée de l'Air et la Marine françaises sont actuellement en pointe dans cette intégration des réseaux dans la conduite de leurs opérations ; l'armée de Terre et les unités spécifiques agissant dans le cyberespace ont également pleinement intégré cette particularité dans leur mode d'actions et les procédés d'exécution.

III- Des partenariats internationaux pour lutter contre une menace globale

Aucune organisation, publique ou privée, ne dispose de toutes les compétences et ressources ni de l'autorité pour, seule, faire face efficacement à la cybercriminalité. Une approche collective doit être développée au plan international afin de « croiser les signaux » pour combattre ces menaces avec force.

En effet, l'armée repose sur des infrastructures permettant d'honorer ses obligations au regard des alliances internationales. Pour ce qui est des États-Unis, ces infrastructures ne sont pas contrôlées directement par l'armée américaine ou l'industrie américaine mais contrôlées, gérées et sécurisées par les partenaires internationaux. Un pays comme l'Estonie apporte actuellement le socle d'entraînement virtuel OTAN (Cyber-range) qui va permettre aux pays membres de concevoir des scenarii sur le volet défensif.

Partager le sens de l'ennemi commun est un élément-clé de toute approche collective. Elle implique le recueil du renseignement, le partage d'informations et la diffusion des alertes. Cette dernière mesure, proactive, aurait pu empêcher certains incidents de se produire. Pour accroître l'efficacité de leur partenariat, les États-Unis et la France envisagent de se réunir dès le 22 janvier 2015 pour revoir en détails les modalités de leur partenariat.

Par ailleurs, les Américains sont désireux de créer ou de renforcer la coopération cyber avec les pays du Moyen-Orient et d'Asie dans lesquels les infrastructures ne sont pas aussi développées qu'en Occident. Le but est de les aider à identifier les failles de leurs systèmes, à développer des stratégies et à se former pour élever le niveau de cybersécurité et l'efficience des personnels impliqués. Il est important, pour chaque pays, d'évaluer son propre système et ses responsabilités, d'identifier les failles, de développer des stratégies, d'organiser la réussite des opérations et d'investir le fruit de son travail dans des partenariats multilatéraux.

La transparence entre alliés s'agissant des attaques subies et

des mesures prises pour y faire face participe aussi à l'efficacité globale du dispositif.
Enfin, pour limiter les risques que peuvent impliquer certains partenariats internationaux, l'OTAN a mis en place un accord sur les normes de comportement responsable afin de mettre en exergue ce qui est acceptable et ce qui ne l'est pas en matière de cyber actions.

Glossaire :

EMA : Etat-Major des Armées (France)
ANSSI : Autorité Nationale de Sécurité des Systèmes d'Information, rattachée au secrétaire général de la défense et de la sécurité nationale. http://www.ssi.gouv.fr/agence/missions
USCYBERCOM (États-Unis): unité qui planifie, coordonne, intègre, synchronise et conduit des activités pour diriger les opérations et la défense de certains réseaux d'information du Département de la Défense, et prépare et, au besoin, conduit, tout le spectre d'opérations militaires du cyberespace dans le but de permettre des actions dans tous les domaines, assurer la liberté d'action des États-Unis et de leurs alliés dans le cyberespace, et le dénier à nos adversaires ».http://www.arcyber.army.mil/org-uscc.html

K01

Incident Response, The Future of Security
La réponse à incident, avenir de la sécurité

Intervenants :
- Bruce Schneier

I want to talk about a variety of security topics. I want to talk about incident response, but I'm gonna get there in a meandering way.
I'm going to start by talking about some trends in information security and talk about some pieces of science, the economics and psychology of security. I'm gonna talk a bit about incident response and then sum it all up with some systems theory from a U.S. Air Force Colonel.

TRENDS
As I walked around the show floor late this morning, I saw a lot of companies doing things about some of these (trends). They're not new, but I think they're important. The first one is that we're losing control of our IT infrastructure. Those of us who have been in computing for awhile have noticed that. We no longer have the same control that we used to. And this is the result of two different things that are happening. The first is the rise of cloud computing. It means we no longer have control of our data. Our email, our photos, calendar, address book, messages, documents. They're all now on servers belonging to Google and Microsoft and Apple and Facebook and other companies. As organizations, we outsource our communications, our CRM, our applications and sometimes our desktops; our entire IT infrastructure. My new company outsources its entire email to Google. We do not have an email server. That's relatively new. And the thing about the security here is that we can't affect the security of the systems. I can't call up Google and say "I want better security of my corporate email."
I can't even really ask what security I have. I just have to accept it. It's

the same with Facebook. I don't even know what operating system Facebook uses.

So that's the first half of that. The second half is that we're increasingly accessing our data on devices we have a lot less control over. It's stuff like this (shows his phone). iPhones, iPads, Android phones, Kindles, Chromebooks. These are not really the same as computers. I can't run arbitrary software on this. I have much less control over this system. I can't build a firewall for this device. I can't even build a file erasure program because I don't have direct access to the memory. With these new devices, there's much more vendor control of how they work and what goes on them. Even if you look at the new computer operating systems. Look at Windows 8. Look at Apple Yosemite. They're looking more and more like phone operating systems where the vendor of the OS has much more control over the eco system. Right now, organizations are embracing both of these changes for really good reasons. A lot of good financial reasons why we outsource everything and we give all our employees Ipads and interface everything through a browser. It makes a lot of sense, but it's hard for security and I think this is a really important trend. There are companies out there that are trying to solve this very problem.

On trend two, attacks are getting more sophisticated. I could spend an entire hour on this point. If you've been following security, you can see that we're seeing a lot of very sophisticated attacks out there. There are a variety of attackers, from nation states to non-nation states, from the NSA to random criminals to the government of North Korea to cyber terrorists. There is this whole gamut of attackers doing all sorts of things. And this is causing a lot of consternation. The term you'll often hear is cyber war. I don't think that's right. It's not that we're fighting a cyber war. The real point is we are increasingly seeing warlike tactics of broader cyber conflicts. This is important. Technology is spreading capability. It used to be that you could determine the attacker by the weaponry. If you walked outside this building and you saw a tank, you would know that the French government was involved because only governments can afford tanks. That mnemonic trick doesn't work on the internet. Everybody does the same things. Same attacks, same tactics. This is why we can't tell the difference between the government of North Korea and two hackers in a basement somewhere. This is the lesson of all the Snowden documents. A reporter asked me earlier today, "What was the most surprising thing about the Snowden documents?" The most surprising thing is the lack of surprising things. The stuff they're doing is the same stuff hackers are doing. They just have a bigger budget. They just have a fancier interface. They just have more bandwidth, better access. It's really no different. Attackers are becoming as sophisticated as governments. This is an important trend.

A lot of this is APT, advanced persistent threat. The way to think of that is this. Normally in security we worry about low focus attacks, opportunistic attacks. If you've been following the hacking in corporate America last year, the two big things were about Target Corporation and Home Depot. Those were criminal attacks of criminals wanting big blocks of credit card numbers. And the companies that were hacked didn't have to be those particular companies. They were just easy targets. If they had had better security, the hackers would've gone elsewhere. This is very different from the Sony attack where, for whatever reason, the attackers wanted Sony. And the difference is relative security versus absolute security. Against an opportunist, you have to be more secure than your neighbors. Against a dedicated attacker, you have to be more secure than they are skil-

led. If anyone does penetration testing for a living, you know that a sufficiently motivated, skilled and funded hacker will always get in. Right now on the internet, attack is easier than defense. We are all more vulnerable than we are secure. A lot of this is politically motivated attacking and politics is very broad here. It's against governments, corporations, nationalistic, ethical, religious. Sony is a company that hackers love to hate and have for over a decade. So is Google. It used to be Microsoft, but now no one cares. There's a lot of this. We will see political hacking, for example U.S. versus China, Israel versus the Arab states, India versus Pakistan, U.K. versus Northern Ireland, Russia versus Estonia. A lot of it, I think, is kids playing politics. And if you remember a couple of weeks ago, the United States military, U.S. Central Command, had their Twitter feed hacked by someone associated with ISIS. The press reported that the U.S. military got hacked. That wasn't actually true. The U.S. military's Twitter feed got hacked. They didn't have any magical, secure Twitter. They had regular, ordinary Twitter. But this is an example of politically motivated hacking. There is a lot of IP theft. The United States is very concerned about IP theft from China. And it's not just against governments, it's also against corporations. Last year, the U.S. Attorney General indicted five Chinese nationals in absentia for hacking not U.S. government networks, but U.S. corporate networks, companies like U.S. Steel. There's a lot of this going on. Cyber crime is also more sophisticated. Cyber criminals are getting better. They're getting better at basically the whole supply chain...from stealing credentials, to turning it into accounts, to monetizing it, to laundering the money and getting it offshore.

The third trend is increasing government involvement in cyber space. More and more governments are taking a very strong interest in cyber space. There are lots of regulations. This is true in countries like China where there's an enormous amount of censorship and surveillance and control. And it's true in Western democracies where there's less censorship and control, but there's still a lot of government involvement. There are a lot of government regulations, a lot of privacy regulations, much stronger in Europe than in the U.S., but there are a lot of them everywhere. We are seeing a lot more nation state espionage and attack. If you followed the latest Snowden documents, there were two great stories in Spiegel, one at the end of December and one last week talking about the NSAs and at GCHQ their activities in espionage and in attack. And you have to assume that those countries are not unique. These are the same things being done by all other countries...Russia, China, France, Germany, Israel, India, Argentina...any country with a big military.

We're seeing a lot of talk about critical infrastructure, how to secure it, and whether that's best left in private hands or if the government needs to step in. I suspect this will become more important in the coming years. Some of it is coming from terrorism fears. We're going to see more government involvement in things like communications infrastructure and national power grids. There's big talk about that in the U.S. And we're in the early years of a cyber war arms race. Countries are gearing up for cyber war...NATO countries, Russia, China...the usual suspects. There's a huge market for vulnerabilities, for cyber weapons. Countries that can't build their own cyber weapons can buy them. There are companies that sell espionage and attack weapons to countries like Uzbekistan, Ethiopia, Pakistan, Saudi Arabia, Bahrain...countries that you might not want to have these capabilities, but they're out there. So those are the three trends.

Now I quickly want to talk

about IT security economics. I want to explain some things about the way the market works and I have to look at economics. I have four pieces of economics to talk about. The first one is the network effect. You've all heard of Moore's law. There's a lesser known law called Metcalfe's law. It says that the value of a network equals a square of the number of users. Basically the value of a network is the number of connections and you kind of know this. I mean one fax machine is useless, two are kind of boring...a million fax machines and suddenly you have something. The more people that have a fax machine, the more your fax machine becomes valuable. This is true for phones, for email, for SMS, for Facebook, for Skype. The more people on the network, the more valuable the network is to everybody already on it. This is also for virtual networks. Think of Windows versus Mac users or IOS versus Android. The more people using a platform, the more cool stuff happens on the platform. And what this means is that you tend to get a marketplace with a single dominant player. The big get bigger because there's value in being big. There's value in us going with the big player. That is really important in IT.

The second is the notion of high fixed costs and low marginal costs. Whenever you build a product, there are two types of costs. There's the cost of the design and development and the cost of making the product. So, for example, for that chair over there, most of the cost of that chair is the cost of making it. It's the marginal cost. So, eight chairs will cost eight times one chair because the cost is in the actual chair. Software is different. The first copy of Microsoft Windows cost, let's say 20 million dollars, the next copy is free. In software, all the costs are in development. Making the individual objects costs almost nothing. It's not just for software, there's also music, movies, pharmaceuticals. The development costs dominate in those markets. And this is why stealing the results of this development is such a powerful attack in all of those areas. This is why you see so much effort going into anti-market solutions to allow companies to recover their fixed costs. Software suffers from that.

The third piece of IT economics is the notion of switching costs. The switching cost is the cost for you to switch to the competitor's product. So, for example, with my lunch I had a Coke. If I didn't like it, I could have a Pepsi tomorrow. The cost to switch from Coke to Pepsi is zero. On the other hand, I'm using AT&T as my cellphone provider. I use them because they have good international service. If I'm here in France and I don't like the way they're working, I'm probably going to use them tomorrow because the cost of switching cellphone providers is much higher than for switching soft drinks. In IT the cost can be very high. It can mean retraining staff, rewriting applications, converting data. And here's the thing of it, the higher the switching costs, the more a company can annoy you before you'll switch. AT&T has to have really lousy service before I'm gonna switch because it's hard. And this is why companies do everything they can to keep switching costs high. Think of proprietary file formats, think of non-compatible accessories, think of not being able to take your data with you. You want to leave Facebook? You can't take your data. You want to leave Itunes? You can't take your music. You want to leave Kindle? You can't take your books. All of that serves to keep switching costs high. And that's really important to software companies because they can provide less good service. They don't have to be as responsive in the same way a restaurant does where it's trivial to go across the street instead.

The fourth piece of IT economics is the notion of a lemon's

market. This is work done by an economist by the name of George Akerlof and he won a Nobel prize for this work. He looked at markets with asymmetric information between buyer and seller, basically markets where the sellers know more about the products than the buyers. His example was a used car market. In English, the term for a lousy used car is a "lemon". That's why Citroën never sold in the U.S. because it had bad connotations. So, in Akerlof's thought experiment, imagine a used car market in a town with one hundred cars for sale. Fifty good cars at $2000 and fifty lemons at $1000. In this market, the equilibrium price for cars is $1500 and at that price, none of the good cars sell and all of the lemons sell. What Akerlof showed, and he showed this experimentally, observationally, theoretically, that when sellers know more about products than the buyers, bad products drive good products out of the market. This is very much the IT security market. Buyers tend not to be able to tell good products from bad products because quality in security is non-functional. It's hidden. I could hold up two VPNs. They can use the same protocol, same algorithms, make the same claims. One is good and one isn't. You can't tell the difference. You're going to buy the cheaper one, probably not the best one. This is what happened to the VPN market. Before that, it's what happened to the firewall market and the IDS market and the encryption market. The stuff that wins isn't the best stuff. It's the easiest to use stuff. It's the more popular stuff. It's the cheaper stuff.

Now I want to do one piece of psychology. A little bit of security psychology. I want to explain to you Prospect Theory. This is actually another theory for which the authors won a Nobel prize. They won a Nobel prize in economics and these were the first non-economists to win it. They were psychologists. They did something that was really believed to be impossible by economists. This is called loss aversion or the framing effect. I'll give you the basic experiment in prospect theory. You take a room, much like this one, and you divide it in half up the middle and you ask each half of the room similar questions. You ask this half of the room to choose between winning 1000€ right now or a coin-flipped chance of winning 2000€. The expected return is the same. The basic question is "Are you a gambler or not?". When you ask real people these questions, about three quarters will take the sure gain. In English, the phrase is "A bird in the hand is worth two in the bush". It's better to take the smaller, sure gain than the riskier larger gain. Then you ask the other half of the room a similar question, "Will you take a loss of 1000€ (I'll hit you over the head and take your money) or a coin-flipped chance at losing 2000€?". Again, the expected return is the same and the question is "Are you a gambler or not?". And when you ask real people these questions, about eighty percent of you will take the risk. You'll prefer the coin-flipped chance of losing 2000€ or nothing versus the guaranteed loss of 1000€. So what these experiments show is that we are risk averse when it comes to gains and risk seeking when it comes to losses. It's actually extraordinary. It seems obvious in hindsight, but economists believed this was totally not true. And if you think about it, security is this choice. It's a choice between a sure, small loss (buy my stuff), or a risky, larger loss (you might get hacked). And in that case, most people prefer to take the chance. It's not that they never buy security. It's that it's a harder sell. And you see this in IT security. You see it in insurance, in burglar alarms. You'll go to your boss and you'll say, "We need this security thing to keep us safe." Your boss will look at you and say, "We didn't have that last month and we were ok. Why don't we take the chance next month?". That's prospect theory.

That's preferring to take the chance. It sort of dovetails for what the position is for a middle-manager in a company. If he saves five percent in his budget, he's going to get promoted. If he's unlucky and gets attacked, he quits and gets a different job. It's actually in his best interest to take the chance.

So I said I'd talk about incident response. I'll talk about it now. So we all know that security is a combination of prevention, detection and response. And we need response because prevention and detection aren't perfect. The attackers have the advantage on the internet. Today we need it more than ever before for a bunch of reasons. We've lost control of our computing environment, attacks are getting more sophisticated. Government involvement means that we're often buffeted around by what they're doing and companies will underinvest in prevention and detection because of prospect theory. So, way back in the 90s I used to say that security is a product, not a process. And by that I meant something very strategic. It meant that you couldn't just buy some security and then be done with it. It's a continual process of evaluating what you're doing and your security posture and then refiguring out what you need to do. Tactically, really, security is a product and a process. Actually, security is really people, process and technology. They used to say that a lot in the 2000s. What's changing are the ratios. So conventional wisdom is that people generally don't help with security. People are the weakest link, the worst security problem. And the more you remove them, the better. That's what we're always saying. I have a quote from Lorrie Faith Cranor. She does security usability at Carnegie Mellon. She wrote this in 2008. "Whenever possible, secure system designers should find ways of keeping humans out of the loop." Right? That's just common sense. And if you think about it, we've been doing this pretty well. Anti-virus works because people are out of the loop. Update works because it's automatic. We have lots of automated prevention systems. We have lots of automated and semi-automated detection systems. But here's the thing about response. You can't automate it. As you move from protection to detection to response, the people:technology ratio goes up. You need more people and less technology.

Incident response is hard to automate for a bunch of reasons. All attacks are different. All networks are different. All security environments are different. All organizations are different. Regulations are different and the political and economic considerations are much more important than the attack. Another lesson from Sony. The real problems Sony had were not technical. They were political. They were social. They were managerial. They were public relations. They were legal. That's where their big problems were. So this truism affects the economics of security. Incident response products end up being different. There's less network effect. There are higher marginal costs. There are lower switching costs. There's less of a lemon's market. In response, better products and better companies will do better. I think this is a really good thing.

So, people, process and technology...the key here is to scale. That's what we want. We want scaling. And this is the follow on sentence from Lorrie Cranor, "However, there are some tasks for which feasible or cost effective alternatives to humans are not available. In these cases, system designers should engineer their systems to support the humans in the loop and maximize their chances of performing their security critical function successfully." If you can't remove the humans, make them as effective as possible.

Think of any emergency response. Think of police. Think of fire. Think of medical. Think of

military. They all use technology, but the people are in charge. I'm going to give you an example. Yesterday, I flew to France and I went through airport security in Minneapolis. Airport security is a system where technology is in charge. Yes, there are people, in the U.S. they are called TSA agents, and they do a bunch of stuff, but the technology is completely in charge. The technology tells them what line I go through, what machine I walk through, what kind of search happens after – what's detected and what's not. The only reason people are used is that we can't figure out how to replace them with machines. And as soon as we can, we will. And it will be a better system because the people will be removed. Now, imagine as I was walking through security yesterday evening, I had made a bomb joke. They would have called the police and completely ruined my day. But as soon as the police had arrived, the people:technology ratio would flip. Suddenly the people would be in charge. There would be lots of technology. They'd look me up in databases. They'd take apart my luggage and scan it. They'd do all sorts of annoying things. They would use technology, but the people would be in charge using the technology. That's what response tends to look like. Technology that aids people instead of people that aid technology.

So the goal here is resilience. Resilience in all its factors...mitigation, survivability, recoverability, adaptability. What we learn again and again from the incidents we see is that they're different. They're unique. In order to survive them, you have to do things you might not realize you had to do. You get resilience through things like adaptability, mitigation, survivability and recoverability. You get resilience against attacks. Sony could not have prevented the attackers, whoever they were. Whether they were a couple of guys or the North Korean government. But there are ways they could have been much more resilient in the face of attacks. This is true in the real world as well. We've seen over the course of the last decade and a half lots of examples of countries and societies being more or less resilient to terrorist attacks. And when we are resilient, the attacks are much less effective, no matter whether they're successful. When we are not resilient, and the U.S. is a great example, the attacks are very effective even if they're not successful. Resilience is really a key part of security. It's what I think we should talk a lot more about, especially in this technological world. How do we recover? How do we survive? How do we mitigate? How do we deal with the plethora of threats? This is not gonna be through prevention. A lot of this is the feedback loops.

So I want to end by talking about some systems theory. I'm gonna talk about OODA loops . Now I saw some military people around. Who here has heard the term OODA loops? This is really interesting and worth looking up after this talk. OODA stands for Observe, Orient, Decide, and Act and it's a loop that reflects a real time adversarial conflict. This was developed by the U.S. Air Force, by a military strategist whose name is Colonel John Boyd and he developed this for fighter pilots, for Top Gun people. This is a continual process of collecting, evaluating and acting on information. It was developed for dog fights, but it's widely applicable in all sorts of real time adversarial situations. It has been talked about in strategic military planning, for business competition, for martial arts combat and also IT security. It's an iterative process; it's a loop you do again and again. And what Boyd says is that people in these situations are constantly going through the loops in their head. They're doing this OODA loop again and again and again. And what he did is he took this theory and looked at a fighter aircraft. He looked at everything on the fighter aircraft and asked

"How does this improve the speed of the pilot's OODA loop?". And if it didn't, then he asked "Why is this on the aircraft?" because in the theory of OODA loops, speed is critical. If you can do your OODA loop faster than the other guy. The phrase is "to get inside your opponent's OODA loop", then you have an enormous advantage. And in incident response, we need faster OODA loops than the attacker. There's a bunch of stuff written on applying this to cybersecurity; there's a book, there are some papers, and really, I encourage you to Google this because I think it's really interesting.

So, what I think we need for incident response are tools to help us speed up our OODA loops. We need tools for observation; knowing what's happening on networks in real time. We have some of that. Think of real time threat detection from IDSs, think of log monitoring and analysis, think of network and performance data, think of network management tools. All of that stuff provides information about the networks and the faster we get that information, the more usable it is by turning it into charts, into reports where we can see what's going on, makes us faster. It makes us quicker to observe what's going on.

Step two is to orient, to understand what it means in context. This is in the context of the organization, in the context of the greater internet community. Think of some of the threat feeds out there that tell us what's happening on the internet, what malware is being used, which IP addresses the attacks are coming from. It's also about the orientation of your organization. Is your company rolling out new software or is it engaging in layoffs? Has it been attacked before? In the case of Sony, I think they missed a lot because Sony has been attacked again and again over the decades. They're a company hackers love to hate. In this latest attack, they were not able to orient themselves, to understand how this reflected what happened years before. Orientation requires lots of information from all sorts of areas inside and outside the organization.

The third step is to decide. There's not a lot of stuff here to figure out what to do and to do it. So we need decision support software. Here is where you see a lot of companies fall down. Who has the power to decide? How do they decide? Do the executives have input? Does marketing have input? Do the lawyers have input? How is the decision justified, approved, audited. In the U.S., most of these high-profile hacks are followed by major lawsuits where the companies have to justify what they did. With good decision software, they'll be able to justify it. This is hard because attackers are fundamentally more agile here. They have no bureaucracy. They're not following the law. We really need defense to be more agile.

Finally, the last step is acting. How do we give IR people the power to make changes they need to do? And this is really hard because normally in security we work in permissions. You can't do something unless you have permission. In response, that often doesn't work because you never know what you'll have to do. A better model is to give response people the permission to do anything they want and just audit it later. It's faster and more effective to require them to justify what they did rather than requiring approvals. So we need tools for all these things. We need tools that are powerful, flexible, and intuitive. We need tools that aid people. Instant response is getting more important for a whole bunch of reasons including the ones we talked about...attacks are getting more sophisticated, the regulatory environment is more sophisticated, litigations are more common, geopolitical factors are spilling over. The Sony case really should give you

pause. The fact that we can't tell the difference between North Korea and a couple of guys. I remember a couple of weeks ago some people from Anonymous said that they were going to take out ISIS. That's a little freaky. Or in 2010 when Anonymous threatened NATO. That's really weird. Hacker groups shouldn't be able to threaten large, international, military organizations. It just shouldn't happen, but this is the geopolitics of the internet. It makes response more important. Lastly, organizations are underspending. I believe that IR isn't going to be like the rest of security, "the better stuff will do better", because it supports experts instead of replacing experts. That is a critical difference. There are more people and less technology. Remember the goal. The goal is to bring people, process and technology together. If you think about it, the 1990s was a decade of prevention...anti virus, firewalls. The 2000s was the decade of detection...IDSs, manager security monitoring. This decade is the decade of response. This is the decade that response will mature into a service category like the other two. I think it's long overdue. I think it's really important. And I really think this is the way we're going to defend against the threats. This is what's gonna work. Thank you very much.

K02

La souveraineté numérique

Bonjour à tous,
Merci de cette invitation et de l'honneur qui m'est donné d'intervenir devant votre assemblée. Nous sommes à la moitié des années 10 du vingt-et-unième siècle. Comment les historiens du futur verront-ils cette époque ? Quelle dynamique marquante définira notre temps ?
Les réseaux numériques. Les réseaux numériques sont la clef.
Voilà ce que sera le sens et le résumé de notre époque : l'âge où ces réseaux sont devenus des États et où les États sont devenus des réseaux. Quelle puissance donc émerge ainsi soudain pour rivaliser avec les États ? Cette puissance vient de la rencontre entre les progrès de l'informatique et l'effet de réseau. L'effet de réseau. C'est la loi de Metcalfe. La valeur - ou l'utilité - d'une machine est égale au carré du nombre de machines auxquelles, elle est connectée. 10 machines en réseau, cela fait 10 au carré, soit 100, comme valeur de chaque machine.
Rajoutez une onzième machine, la valeur de chaque machine passe de 10 au carré à 11 au carré, soit 121. Vingt et un pour cent de croissance de valeur de chaque machine avec une seule machine ajoutée. On doublant le nombre de machine, on multiplie la valeur de chacune par quatre. Cette loi est une machine exponentielle à créer de la valeur. Elle est tellement puissante qu'elle met les ordinateurs en réseau, qu'elle met les réseaux d'ordinateurs en réseau, c'est Internet.
Le nombre de machines et d'appareils connectés au réseau est passé de 200 millions en 2000 à 15 milliards en 2015 et sera de 40 milliards en 2020. C'est vertigineux. L'effet de réseau entre les documents, c'est le Web. Entre les gens, c'est les réseaux sociaux.
À cela s'ajoute l'accroissement, à prix constant, de la capacité de calcul des machines : multipliée par

Intervenants :
- M. Pierre BELLANGER, président directeur général de Skyrock

mille en quinze ans. Enfin, moins connue, la progression de l'efficacité des logiciels : quarante-trois fois plus rapide que l'évolution des machines. Quand le matériel progresse de 1 000 fois, le logiciel progresse de 43 000 fois.

Ainsi, en quinze ans, la puissance informatique d'une machine moyenne - qui multiplie les progrès des matériels et des logiciels - s'est accru 43 millions de fois ! Et ce chiffre sera doublé dans dix-huit mois. Et n'oublions pas qu'avec une exponentielle, mille en quinze ans, c'est un million en vingt ans. L'exponentielle de l'effet de réseau multiplie l'exponentielle du progrès informatique. Le résultat dépasse l'imagination. Nous avons du mal avec les exponentielles. Une feuille de papier pliée en deux puis en quatre, cinquante fois de suite. Quelle est l'épaisseur finale du pliage ? 114 millions de kilomètres, soit les ¾ de la distance de la Terre au Soleil.

Oui, nous avons du mal avec les exponentielles. Et nous n'imaginons même pas notre incapacité absolue à estimer la puissance d'une exponentielle d'exponentielle. Le réseau est un tel moteur de croissance, de valeur, de rendement et de productivité qu'il est entré dans une logique de substitution des activités et des systèmes traditionnels. Il transfert et concentre la valeur avec une violence qui n'a d'équivalent que l'exceptionnelle utilité et facilité des services qu'il nous rend.

Notre vie migre sur le réseau. Notre passé, par nos souvenirs numérisés, est sur le réseau. Notre présent transite de plus en plus par le réseau qui, sans cesse, oriente nos décisions. Notre futur dépend du réseau car les informations collectées sur nous, aujourd'hui, déterminent les choix qui nous seront proposés demain. Nos amis, notre univers relationnel, passe également par le réseau, jusqu'à être désormais inaccessible sans cette intermédiation numérique.

L'économie, quant à elle, est confrontée à une force de productivité qui la désarticule, à la manière de l'effet gravitationnel du trou noir. Le réseau détruit quatre emplois quand il en créé un. Près de la moitié des emplois du tertiaire seront remplacés par les machines en réseau dans les vingt ans.

Ce choc immense serait déjà rude à vivre s'il intervenait au sein de notre société, à la manière d'une révolution industrielle traditionnelle. Mais, ce n'est pas le cas, le centre de gravité du réseau et de ses principales entreprises est étranger, le siphonage est brutal et unilatéral.

Alors que le réseau est notre meilleure chance de progrès et de changement positif, nous n'avons pas de pouvoir sur le processus en cours. Nous perdons le contrôle des infrastructures, des services, des données, du droit, de la vie privée, de la propriété intellectuelle et c'est notre société entière qui se dévitalise alors que le réseau est sa chance de régénération.

La souveraineté numérique est justement cette volonté de maîtriser ce nouveau destin, afin qu'il réponde des lois de la République et que cette mutation renforce tout autant nos libertés, nos choix que notre prospérité. Car le réseau est notre chance. Chance en tant qu'individu. Jamais autant de possibilités concrètes, de choix, d'informations, d'échange. C'est une révolution positive absolue. Jamais autant de puissance informatique à disposition de chacun. L'effet de réseau joue à plein. Mon émancipation est égale au carré de toutes les émancipations auxquelles je me connecte. Et comme l'humain est un devenir constant, l'amélioration de chaque être humain auquel je suis connecté accroît ma propre valeur. La spirale positive dans laquelle nous sommes entrés est incalculable et sans prix. Chance en tant que société car c'est la seule solution magique à nos problèmes.

Le XXème siècle a résolu la question de l'incertitude par le gaspillage. Je ne sais pas combien d'exemplaires de tel journal seront vendus demain, je le distri-

bue partout et récupère ensuite les invendus. C'est un modèle fou. La moitié de la nourriture est gaspillée, notamment par le manque d'informations permettant le réajustement rapide des circuits de distribution. Un tiers de l'essence consommée est perdue en recherche de place pour se garer et donc par l'absence d'information à jour sur les emplacements disponibles. Et plus gravement, selon certaines études, l'emploi des données permettrait de réduire la mortalité des patients hospitalisés de 20 pour cent. À chaque fois, on gaspille les ressources et les gens pour pallier le manque d'informations.

En ce siècle, on change de modèle. On résout l'incertitude non plus par le gaspillage mais par l'information. Le gain de productivité à tous niveaux est immense. Chaque État, chaque collectivité, chaque entreprise, chaque individu peut faire mieux avec moins grâce à plus de données.

Pour la France, sur près de 3 000 milliards d'euros de PIB, c'est probablement un enjeu de plus de 10 % d'économies lorsqu'on remplace le gaspillage par l'information : 300 milliards d'euros, une estimation basse de la valeur annuelle de nos données.

Maintenant pourquoi cela nous échappe-t-il ? Pourquoi, sommes-nous atteint du complexe du hérisson : émerveillés par les phares mais immobiles ? C'est parce que l'évidence nous a collectivement échappé. Nous sommes à l'âge où les réseaux deviennent des États et où les États deviennent des réseaux.

Comment un réseau devient-il un État ?

Les réseaux numériques et le premier d'entre eux Internet capte la valeur de la société car il la remplace par une meilleure productivité, un meilleur rendement, un meilleur service. Ce transfert et cette concentration par le réseau est transférée et concentrée par une nouvelle catégorie d'entreprise : l'alliance de services en réseau ou résogiciel.

Le résogiciel concentre à son profit l'exponentielle d'exponentielle et voilà comment il procède. Il commence par un service à succès, puis en associe d'autres parfois, ces alliances dépassent la centaine. La loi de Metcalfe s'applique aux services. Un service associé à 100 vaut 100 au carré soit 10 000. Un service isolé, même meilleur, est broyé. Un service de carte associé à votre agenda, votre carnet d'adresse, une messagerie, votre géolocalisation, un service de trafic dynamique et un réseau d'utilisateurs n'a bientôt plus de rivaux.

L'alliance de service en résonnance développe ensuite ses infrastructures pour être plus rapide et rapidement investit les réseaux de télécommunications pour être plus près et plus rapide. Bientôt le résogiciel développera son système d'exploitation et les terminaux qui vont avec. Rien ne doit empêcher ou altérer, l'intégration de la chaîne, l'accès au client et la collecte des informations. Le résogiciel est le nouveau type de société dominante. Exemple : Google qui propose plus de 120 services en ligne coordonnés entre eux : moteur de recherche, carte, courrier, agenda, traducteur, carnet d'adresses, réseau social, plateforme vidéo, etc. et investit dans les câbles et fibres de télécommunications, les robots, les drones, jusqu'aux thermostats connectés d'appartement. L'effet réseau s'applique aux services. L'effet de réseau s'applique aussi aux données. La valeur d'une donnée est proportionnelle au nombre de données auxquelles elle est reliée et donc la contextualise.

L'information selon laquelle j'achète une poussette à une valeur certaine pour les fournisseurs de la petite enfance. Sa valeur est différente, si une seconde information indique que je l'offre à ma voisine.

Ainsi plus un acteur dispose de données plus les nouvelles données ont plus de valeur pour lui que pour les autres, la aussi la logique conduit à un monopole par le seul effet de réseau. Cette mutation est en accélération

constante. Un terrain capital devient le temps. Plus on a de données et de capacité à analyser les données plus on va vite et plus on ralentit le temps. L'œil d'une mouche gère 200 images par seconde, huit fois plus vite qu'un humain. Lorsqu'il pleut les gouttes descendent huit fois moins vite relativement pour une mouche que pour humain. La mouche se faufile entre les gouttes. L'acquisition et la vitesse de traitement des données ralentissent le monde. Seule cette capacité de ralentir le monde par le traitement sera en mesure de compenser l'accélération du changement.

Tout le monde sera dans le brouillard des données sauf les résogiciels.

Les réseaux financiers qui agissent sur les marchés à ultra-haute fréquences sont plus rapides que les États. On en a vu les conséquences.

Le résogiciel en saura plus que quiconque sur chacun. Une étude récente sur 17 000 utilisateurs de Facebook à comparer la machine et leur proche quant à la connaissance de leur personnalité. La machine est meilleure pour prédire la psychologie et le caractère que les collègues, les amis, les membres de la famille et du conjoint. La machine bat le collègue de bureau à partir du traitement de 10 likes, il lui en faut 70 pour battre un ami, 150 pour un membre de la famille et 300 pour le conjoint. En moyenne, un utilisateur laisse 227 like.

Quant au système d'exploitation, il ne se cantonne pas à la machine de bureau où au terminal mobile. Il se retrouve partout dans le thermostat d'appartement, la voiture, la montre, tous l'électroménager et l'audiovisuel jusque dans les équipements urbains. L'effet de réseau s'applique aux systèmes d'exploitation.

La valeur d'un système d'exploitation est proportionnelle au nombre de système d'exploitation de même famille auquel il est connecté. Là aussi, la dynamique est sans rivale. Et il ne faut pas se tromper. L'effet réseau sur les systèmes d'exploitation a pour conséquence la fin de l'Internet libre et ouvert. Et le fameux Web, libre de publication et d'accès, sera marginalisé par les logiques croisées de ces systèmes de gestion d'appareils qui deviendront la porte d'entrée majoritaire du réseau. Le trafic Internet d'ailleurs quitte peu à peu le Web traditionnel et fixe pour rejoindre l'accès mobile, plus pratique, et donc en croissance record.

Jadis, on créait un site sans entrave, ni contrainte ; aujourd'hui, on soumet une application à une plateforme de gestion de sources et de services (iTunes, Google Play), émanation de ces nouveaux systèmes.

Ce distributeur virtuel développe ses propres applications éventuellement en concurrence avec les vôtres, maîtrise votre accès à son système d'exploitation, accède à vos données, contrôle tout, pour finalement décider de votre présence et donc de votre existence. Une telle situation de subordination est inouïe.

Cette tutelle sera répliquée sur tous les métiers. Demain, un médecin qui n'aura pas la licence de tel ou tel équivalent d'Android n'aura pas accès à votre dossier de santé et aux données collectées par le système. Votre garagiste, sans licence, ne pourra réparer votre véhicule, faute d'accès au système et l'architecte, démuni de ce Sésame, ne saura traiter l'informatique des bâtiments. La valeur de chaque activité, tant son bénéfice que son savoir-faire et ses données collectées, seront transférées à ce tiers numérique dont l'hégémonie ne cessera de croître.

Imaginez la situation d'un État dont la relation même à ses citoyens passe par cette intermédiation informatique généralisée qui, à tout moment, peut devenir rivale ? Nous sommes à genoux.

La valeur passe de la société au réseau et du réseau aux résogiciels.

La société traditionnelle explose car rien ne résiste aux résogiciels. Les taxis sont au début de la liste,

le reste suit avec les banques concurrencées par des prêts sélectifs et informés des données des emprunteurs, l'assurance dépassée, les assurances sélectives pour des assurés triés par leurs données de santé. L'automobile devient la carcasse d'une licence de système d'exploitation. C'est ce que Microsoft à fait à l'industrie du PC, c'est ce que le résogiciel fait à toutes les industries et services.

Lorsque les premières sociétés par action sont apparues à l'aube du XVII ième, peu imaginaient vraiment la portée de ce nouveau type d'entreprise. Aujourd'hui, sur les 100 premières entités économiques mondiales 70 sont des sociétés et 30 des États. C'était 51/49 en 2000.

Le résogiciel a cette puissance accrue de l'effet de réseau.

Le résogiciel contrôle l'identité. Il garantit mieux l'identité qu'un document public. Certains loueurs de voitures américains vérifient les papiers d'identité en les validant par le profil sur un réseau social. Il peut battre monnaie, plusieurs d'entre eux expérimentent ou utilisent des monnaies virtuelles. Il prélève un impôt puisqu'il marge sur les transactions. Il édicte des propres règles sur la liberté d'expression. Il autorise par exemple les décapitations mais pas les tétons et dispose de la peine de mort puisque la radiation d'un réseau social peut pour un utilisateur moyen signifier la perte de toute existence en ligne. Avec 65 milliards de dollars de chiffre d'affaires, un résogiciel comme Amazon a un chiffre d'affaires supérieur au PNB de la moitié des pays du monde.

Ce sont en fait des États.

Et d'ailleurs nos dirigeants ne s'y trompent pas et les reçoivent ainsi. Et négocient avec eux comme ils peuvent. Les plus hautes autorités parfois se déplacent pour les sensibiliser, le mot est magnifique, à nos règles de droit. Quant à ces résogiciels, soucieux de leur extraterritorialité et de leur optimisation fiscale, en terre étrangère y ouvrent des centres culturels et bientôt viendront en aide à l'artisanat local et aux groupes folkloriques.

La souveraineté numérique s'exprime donc par le droit et par l'activité économique qui s'incarne de façon déterminante par le résogiciel. On peut ainsi dessiner les contours, toujours approximatif et toujours en mouvement, de trois grands sous-ensembles.

Et voir ainsi comment les États se transforment en réseau :

Le premier Internet a réalisé l'alliance entre le réseau et l'État pour former une symbiose ouverte sur le monde, démocratique, expansionniste et compétitive. Le fondement en est le mercantilisme et la puissance impériale : des résogiciels d'envergure désormais mondiale en assurent la croissance. L'intérêt commercial prime notamment sur le droit des données et ses résogiciels ne cessent d'accroître leur emprise et leur influence sur le système politique. Il s'agit bien entendu des États-Unis avec des entreprises comme Google, Apple, Amazon ou Microsoft mais aussi de la Corée du Sud avec Samsung.

Le second Internet a également constitué un partenariat organique entre l'État et le réseau. Il s'est affirmé par la constitution d'une membrane l'isolant partiellement de l'Internet mondial, par la privation de liberté des citoyens et par la culture en serre - sur un marché intérieur considérable - de géants des services numériques, potentiels résogiciels mondiaux pour certains. Il s'agit de la Chine avec des entreprises comme Tencent ou Alibaba. Mais aussi de la Russie avec Yandex et Vkontakte.

Le troisième Internet n'a pas pris conscience dans les faits de la puissance du réseau. L'État et le réseau ont des destins séparés. La préoccupation ministérielle, ici où là, se concentre, tel un rémanence issu du siècle passé, sur la création de jeunes entreprises du secteur qui sont autant de fonctionnalités futures ou de services à adjoindre à un résogiciel désespérément absent.

La législation ouverte, et le plus souvent démocratique, livre les

citoyens de ces nations au pillage légal de leur vie privée et de leur activité économique. Il s'agit de l'Europe, du Japon, du Canada, du Mexique, de l'Australie, du Moyen-Orient, de la plupart des pays d'Afrique, d'Amérique centrale et du Sud. Ce Tiers-Internet est le buffet gratuit et le backyard de nos amis américains et désormais chinois.

La situation de ce Tiers-Internet ne sera pas tenable. La révolution numérique est en effet extrêmement brutale, après une phase lente et discrète, comme le sont les exponentielles. Un emploi sur deux du tertiaire sera remplacé par les machines en réseau d'ici vingt ans. Ce que la mondialisation a fait aux classes populaires, l'Internet va le faire aux classes moyennes. Nos sociétés matures seront menacées, les économies des pays émergents seront coupées dans leur élan. Il est impératif d'imaginer notre futur avant qu'il nous arrive !

Comment faire ? La réponse ne réside ni dans le premier Internet qui privatise les données personnelles et corrode ainsi les libertés individuelles et les droits civiques, ni dans le second, directement privatif de libertés politiques et attentatoire aux droits fondamentaux.

La réponse est dans notre tradition de liberté et de démocratie. Il faut faire de nos libertés, l'arme de notre compétitivité.

Deux chantiers immédiats :

Tout d'abord, le droit des données.

Comment faire dans l'urgence ? Un des premiers pas décisifs vient du droit. C'est le droit des informations collectées par le réseau. Les informations sont sur le réseau, ce que l'argent est à l'économie. Il n'y a pas de politique économique sans souveraineté monétaire, il n'y a pas de politique numérique sans statut des données.

Les données personnelles : le sac de bille et la pelote de laine. Aujourd'hui, les données personnelles ne sont plus isolées, elles sont en réseau. Elles forment un réseau de données, certes chacune demeure personnelle, mais elles sont désormais organisées en une totalité indissociable. Et cela pour plusieurs raisons :

les données personnelles ne sont pas isolables en pratique : donner accès à sa liste de contacts, à ses photos, à son agenda, à son courrier, à sa position, engage mécaniquement, de fait, les données personnelles d'autrui sur lesquelles on ne dispose d'aucun droit ;

les données personnelles renseignent sur d'autres personnes : les algorithmes de corrélation, ces programmes informatiques qui permettent de déduire, par probabilité, des informations par le traitement prédictif de masse de données sans rapport direct avec l'information inférée, font que chaque donnée personnelle renseigne indirectement sur autrui. Par exemple : les données personnelles de clients bancaires croisées avec leur défaut de paiement vont servir à déterminer le risque d'impayé de nouveaux clients par la comparaison de leurs comportements. Par exemple encore : les données corrélées entre cancer du côlon et consommation en supermarché d'un groupe d'individus vont permettre de prédire le risque cancérogène d'une personne, sans relation avec le groupe témoin, et cela à partir de ses seuls tickets de caisse ;

les données personnelles sont une extension de la personne : à la manière du sang, c'est un soi hors de soi. Engager le transfert ou la cession de données personnelles d'autrui, indissociables ou déductibles des siennes, en échange de l'accès « gratuit » à un service s'apparente par conséquent au trafic d'organes ;

le contrôle individuel par accord de gré à gré devient impossible : les collecteurs de données personnelles sont destinés à se multiplier sous forme de capteurs disséminés partout et intégrés dans la plupart des objets ; tandis, qu'à son tour, chaque individu devient collecteur de données sur lui-même et sur autrui. L'autorisation individuelle réfléchie à chaque captation, déjà aléatoire, n'est plus possible dans les faits. Le monde qui vient est un monde où tout incorpore de

l'intelligence informatique, captatrice et communicante, par laquelle tout se traite et transite, afin de transmettre un flux permanent de données. La brosse à dent, la cafetière, l'automobile, le réfrigérateur, la montre, les lunettes, les vêtements, les chaussures captent et se connectent. L'objet muet deviendra l'exception, l'environnement aveugle disparaît ;

Ainsi la vision des données comme indépendantes et fondamentalement séparées les unes des autres est une abstraction qui n'est plus pertinente. Les données personnelles se déterminent mutuellement et forment un réseau organique.

De plus, ce réseau est dynamique. Le volume de données collectées double tous les 18 à 24 mois. Les données, jadis discrètes et donc isolables, deviennent des flux continus d'informations captées et quantifiées à chaque instant, liant en temps réel les données de sources individuelles multiples. Enfin les liens logiques reliant les données entre elles se multiplient de manière exponentielle. Le réseau de données forme désormais une totalité animée en croissance permanente.

Quelle est la nature juridique de ce réseau de données ? Il s'agit d'un objet sur lequel toutes les personnes, dont les données sont maillées, disposent de droits mais qui ne peut être matériellement divisé entre eux. Il est ni dissociable, ni individualisable par nature car chaque donnée personnelle renseigne sur les autres. C'est donc une forme d'indivision qui concerne toute la population.

Par ailleurs, les informations provenant du réseau de données sont d'un intérêt général majeur pour la collectivité, notamment, en matière de santé, de transports, de consommation, d'environnement ou encore de compétitivité économique.

Par son origine multi-personnelle, son impossibilité à le séparer, et son utilité collective, le réseau des données est donc un bien commun - res communis - : un bien qui appartient à tous mais ne peut appartenir à personne en particulier. Son statut est défini en droit français par l'article 714 du Code civil. C'est aussi un bien où chacun dispose de droits spécifiques (retrait, opposition, oubli) sur son propre apport et ce, dès lors qu'il n'engage pas les droits d'autrui.

Le réseau de données répond donc de droits collectifs et de droits individuels. La gestion et l'exercice de ces droits doit revenir à un organisme public, garant du contrôle démocratique et souverain et seul à même d'en permettre l'accès et l'usage.

Une agence des données pourrait ainsi être établie. La meilleure base ne serait-elle pas l'actuelle Commission nationale de l'informatique et des libertés (CNIL) ?

La reconnaissance de la nature en réseau des données personnelles fait qu'un individu n'a plus la faculté de consentir seul à la cession ou à l'accès à ses données personnelles. Toute captation ou traitement de données personnelles doit passer par un agrément de l'Agence de données, préalable à tout accord individuel.

Le transfert de données personnelles vers un service non agréé sera constitutif d'une infraction y compris à l'égard des personnes dont les données personnelles seraient impliquées.

C'est donc cette Agence qui agréera toute captation de données sur le territoire national. Son statut public fonde une relation symétrique avec les grandes entreprises du réseau, plus équilibrée que les contrats d'adhésion souscrits d'un clic de souris par des particuliers pressés.

Le reconnaissance de l'indivision en réseau des données personnelles et de leur statut de bien commun, la reconnaissance des droits individuels et collectifs sur cette ressource ; la création d'une Agence des données pour les gérer, la mise en pratique de ce dispositif légal par un chiffrement des données personnelles associé à des métadonnées de traitement, un contrôle judiciaire et un contrôle contributif

de la société civile sur les méthodes et procédures, voilà qui apportent les garanties civiques nécessaires tout en accélérant le progrès et l'innovation par la mutualisation maîtrisée des données.

Ces principes et pratiques des données en réseau sont applicables d'abord en France mais ont pour objectif la dimension européenne puis mondiale.

Le grand aspirateur prenait grain par grain nos données. Et chacun, de fait ou de droit, de se laisser dépouiller, à l'unité, sans se rendre compte, qu'au final, chacune de ces petites concessions indolores nous livraient, tous, tels les confettis de la fête d'autrui. La reconnaissance juridique des données en réseau bloque la machine. On n'avale pas un pays comme on gobe un carnet d'adresses. C'est la première étape.

Le second objectif est la création d'un Système d'Exploitation SOuverain, le SESO.

Le SESO est le coup d'après des logiques privatives actuelles. Il est un service public ouvert et collaboratif, neutre à l'égard des services qui l'utilisent qui mutualisent leurs données.

Ce système d'exploitation est qualifié de souverain en ce qu'il est sur le réseau la continuation de la République, de ses valeurs, de ses droits et de ses devoirs. Ici la loi et le code informatique ne font qu'un.

Le système d'exploitation du réseau est une nouvelle expression de notre Constitution. Par sa conception, il garantit la sécurité des informations, le respect des données et ne capte pas à son profit la valeur qu'il contribue à créer. Chaque nouveau partenaire bénéficie de la dynamique du résogiciel et vient l'enrichir. Les utilisateurs disposent d'une offre de services compétitive sans risque pour la vie privée et la confidentialité des informations. Autour du SE souverain se constitue le résogiciel souverain. Ce réseau est le moteur de la reconquête de notre souveraineté numérique et le partenaire de nos services, de notre industrie et de l'administration dans la maîtrise de leur mutation numérique.

Le SESO est le pivot de l'Internet européen libre et ouvert. Cette aspiration démocratique lui apportera le concours des meilleurs talents. Il faut coordonner les compétences des ingénieurs système et réseaux, des spécialistes de la sécurité informatique, des juristes et bien entendu des développeurs informatiques. Par le droit des données et ce résogiciel libre fondé sur l'OS souverain, nous rentrons dans le jeu. Non pas en tentant de reproduire une concurrence indépassable mais en imaginant le coup d'après, forcément ouvert et collaboratif.

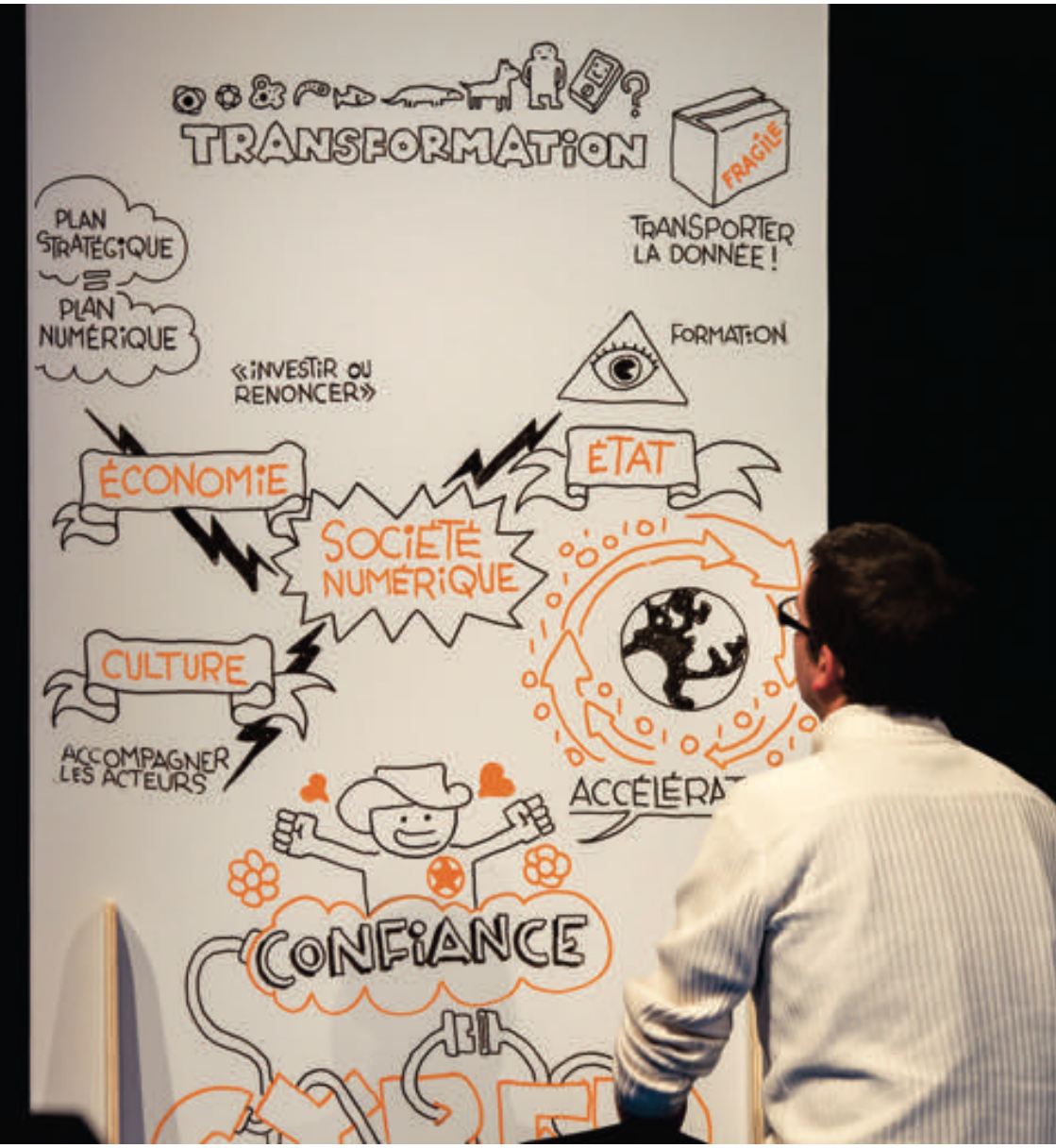
Le système d'exploitation souverain est la réponse. Il est le coup d'après de ces grandes combinaisons de services logiciels en réseau, ces résogiciels privés qui avec talent et détermination maillent notre quotidien. Il est le coup d'après parce qu'il inscrit le droit dans son code informatique, mutualise les données protégées et, finalement, est l'équivalent sur le réseau, de la Constitution pour un État.

L'économie mondiale devrait doubler de taille entre 2015 et 2030. La moitié de l'économie de demain n'existe donc pas encore et elle se fera autour et avec les réseaux. Nous avons le choix de piloter cette formidable chance ou de nous laisser dévorés.

Enfin, le drame que nous venons de vivre démontre tragiquement que nous sommes incapables de faire respecter la loi de la République sur les réseaux et services numériques. Une nation souveraine comme la nôtre doit quémander des retraits de vidéos d'appel à la violence où d'assassinats. C'est une honte collective.

Nous n'avons pas le choix. Nous serons souverains sur les réseaux ou nous serons balayés.

Il faut donner l'effet de réseau à notre belle République. C'est désormais notre mission. Je vous remercie.


TRANSFORMATION
FRAGILE
TRANSPORTER LA DONNÉE !
PLAN STRATÉGIQUE = PLAN NUMÉRIQUE
«INVESTIR OU RENONCER»
FORMATION
ÉCONOMIE
ÉTAT
SOCIÉTÉ NUMÉRIQUE
CULTURE
ACCOMPAGNER LES ACTEURS
CONFIANCE


FIC
2016