LES ACTES DU FORUM

6E FORUM INTERNATIONAL DE LA CYBERSÉCURITÉ

IDENTITÉ NUMÉRIQUE ET CONFIANCE

FIC 2014

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

Sommaire

FIC 2014

RÉGION Nord-Pas de Calais

euratechnologies EXCELLENCE & INNOVATION

ceis

Couverture :
MAJ C. GILLOT
Maquette PAO :
BRI J. OBERLINGER
Crédit photo :
MAJ F. BALSAMO

Discours au Forum International de la Cybersécurité

À Lille, mardi 21 janvier 2014

M. Pierre de SAINTIGNON
Premier vice-président de la région Nord-Pas-de-Calais

Mesdames et Messieurs, général Favier, directeur général de la gendarmerie nationale, et général Watin-Augouard, que je salue puisque c'est finalement vous le père fondateur, ou en tous les cas l'inventeur, et le promoteur du FIC; Cher Rémy Pautrat, préfet historique de notre région Nord-Pas-de-Calais, qui a probablement le plus poussé la Région Nord-Pas-de-Calais à s'intéresser à l'intelligence économique et aux questions qui nous réunissent aujourd'hui. C'est peut-être pour cela que nous sommes maintenant, un peu mon Général, la tête de pont du FIC.

Bienvenue à Lille, dans cette capitale des Flandres, dans cette capitale régionale du Nord-Pas-de-Calais ! Bienvenue surtout aux participants des 58 pays représentés. Nous sommes très fiers, car nous serons pendant ces deux jours à l'évidence, grâce à ce forum, une capitale internationale de la cybersécurité et de la confiance numérique.

Je vous remercie très chaleureusement de votre présence. Durant ces deux jours, se succéderont 250 intervenants, tous de très haut niveau. Ce forum se composera de séances plénières, de conférences et multiples ateliers et sont aussi présentes 80 entreprises partenaires .

J'ai pu constater que l'organisation était très bien structurée, au niveau pédagogique, mais aussi au niveau scientifique. Nous aurons l'occasion d'accueillir au cours de cette journée 4 ministres qui évidemment nous appuient sur ces questions.

Dans un instant la parole sera donnée à monsieur Manuel VALLS, ministre de l'Intérieur. Cet après-midi, nous accueillerons monsieur Jean-Yves Le DRIAN, ministre

de la Défense, puis madame Hessa AL JABER, ministre des Technologies de l'information et de la Communication du Qatar, et madame Milena HARITO, ministre de l'Innovation et de la Fonction Publique de la République d'Albanie. Nous les accueillerons évidemment très chaleureusement avec une volonté de dialogue.

Pourquoi le FIC à LILLE ? Parce que le FIC est né à LILLE, de l'action de la gendarmerie initiatrice du projet, et rejointe immédiatement par le Conseil Régional du Nord-Pas-de-Calais. J'ai voulu que nous soyons présents dès sa création avec tout ce que cela implique en termes d'organisation. Je crois, mon général, que le FIC est bien ancré maintenant. Vous vous exprimerez d'ailleurs sur ce sujet. On est passé par toute une série d'aventures. Si tout cela est bien en place c'est grâce à un solide partenariat entre la Gendarmerie, le Conseil régional de la région Nord-Pas-de-Calais, CEIS, Eura Technologies et la Mission Lille-Europe Défense / Sécurité qui a été créée par le général Thomann en fonction à cette époque dans notre région. Il a su, non sans une certaine fierté pour notre territoire, allier la pédagogie, la formation et la recherche sur toutes les questions de Défense. On ne peut pas parler, c'est l'acteur économique de la Région qui le dit, de développement économique sans parler de protection des entreprises, d'intelligence économique et donc de cybersécurité et de confiance numérique.

On ne peut pas parler non plus de développement des technologies sans parler de protection des données stratégiques si essentielles à notre compétitivité et à notre intelligence collective. Les cybermenaces qui nous entourent nous obligent sans cesse à une capacité d'anticipation des moyens de riposte.

Comme toutes les technologies, celles de l'information et de la communication sont ambivalentes. Elles offrent à la fois des possibilités inouïes, presque sans limite en termes d'échanges d'information, d'échanges de savoir, de développement économique et culturel. Elles posent aussi un grand nombre de problèmes politiques, juridiques, éthiques, sociaux et sociétaux parmi lesquels la sûreté des applications et la protection des supports et logiciels utilisés mais aussi le respect de la vie privée. Ces données ont un impact technologique sur la compétence des salariés et l'organisation du travail, éléments majeurs dans une période qui va très vite, où les mutations sont très importantes, notamment les mutations de la santé, le retraitement de fin de vie des composantes électroniques, ce qui en reste ou les informations qu'ils contiennent, l'accès des moins favorisés aux usages technologiques.
C'est la culture de la confiance numérique que nous voulons diffuser et l'organisation de ce sixième forum cybersécurité à LILLE en est une illustration majeure. C'est d'ailleurs la raison pour laquelle le Conseil régional a décidé de confier à Eura

Technologie, parc d'excellence sur le plan technologique et d'ambition mondiale, la création d'un cluster "cybersécurité et confiance numérique" dont l'ambition est de fédérer tous les acteurs régionaux et euro-régionaux autour de questions communes, de comprendre les enjeux de la cybersécurité et de trouver les leviers de la croissance économique grâce à cette thématique.

Il s'appuie sur un pôle d'excellence, le pôle ubiquitaire installé à Eura Technologies et qui fédère l'énergie de tous les acteurs régionaux du numérique, l'association RDSSI, Eura-Technologie, ainsi que les universités et les centres de recherche. Au fur et à mesure de son développement, ce pôle mettra ses compétences au service des entreprises et des collectivités. Il diffusera nos savoir-faire bien au-delà des frontières du Nord-Pas-de-Calais.

Il me reste à vous souhaiter un bon FIC 2014. J'espère que vous prendrez autant de plaisir à le vivre pendant deux jours que nous avons pris de plaisir à l'organiser. Je remercie toutes celles et tous ceux que se sont engagés depuis un an pour vous accueillir. Je déclare donc le FIC 2014 ouvert et cède la parole au général Denis Favier.

Discours au Forum International de la Cybersécurité

À Lille, mardi 21 janvier 2014

Général d'armée Denis FAVIER
Directeur général de la gendarmerie nationale

Merci Monsieur le président des paroles chaleureuses que vous venez de tenir en particulier pour la Gendarmerie. Merci également pour le soutien fort que vous apportez à la conduite de ce projet, qui est un projet très important pour notre pays et au-delà de notre pays. Je suis très honoré d'ouvrir solennellement cette édition du 6e forum international de la cybersécurité de LILLE. Comme cela a été évoqué par Monsieur Pierre de Saintignon, ce sont 3 000 personnes, décideurs, experts, représentants de plus de 50 pays qui vont se réunir dans cette ville de LILLE pour échanger sur ces questions essentielles qui sont au cœur des préoccupations de nos sociétés contemporaines.

Depuis 2007 vous l'évoquiez Monsieur le président, la Gendarmerie Nationale partage avec la Région Nord-Pas-de-Calais l'ambition d'un rendez-vous annuel permettant de décloisonner les réflexions sur un sujet particulièrement complexe, celui de la cybersécurité. Je veux saluer cet investissement et remercier la Région en la personne de Pierre de Saintignon pour sa pleine implication dans l'organisation de cette manifestation, faisant de LILLE une capitale de la cybersécurité. Je veux à ce stade vous rassurer : nous sommes dans un partenariat qui s'inscrit dans la durée. Nous sommes dans un partenariat fort et nous voyons bien, à l'aune du public qui est présent dans cette salle, à quel point le FIC est désormais présent dans le paysage de la cybersécurité. Nous sommes ainsi appelés à poursuivre notre collaboration et notre coopération dans un sens de grande efficacité et d'intérêt général.

La Compagnie européenne d'intelligence stratégique (CEIS) nous a rejoints comme co-organisateur en 2012. Elle nous a permis de faire franchir un nouveau cap à cet événement majeur qu'est devenu le FIC. Que soient donc aussi remerciés son président, Olivier Darasson et l'ensemble de ses collaborateurs.

Industriels, universitaires, chercheurs, étudiants, institutionnels, nous partageons ici une conviction : les cybermenaces auxquelles sont confrontées nos sociétés modernes appellent une réponse pluridisciplinaire qui fait tour à tour ou simultanément intervenir chacune de nos expertises. Je salue particulièrement l'ensemble des participants étrangers. Leur présence nous rappelle que face à une problématique aussi complexe qui ignore toute frontière, une coopération internationale coordonnée s'impose. Durant ces deux jours, trois séances plénières et une quarantaine d'ateliers vont nous offrir des opportunités de rencontre, d'échange et de réflexion. Je souhaite que ces travaux permettent d'imaginer véritablement les actions de demain. Nous connaissons tous les enjeux, nous les partageons tous ensemble. Sachons être tous des acteurs engagés pour un cyberespace sûr, générant de la confiance, propice au développement des activités économiques et de loisir.

Dans quelques minutes, le ministre de l'Intérieur s'exprimera à cette tribune et vous confirmera à quel point les questions de cybercriminalité, de cybersécurité sont au cœur de ses préoccupations. Face aux cybermenaces, la protection de nos concitoyens et de nos entreprises en un mot la protection de la Nation, est un défi que nous avons ensemble collectivement choisi de relever.

À mon niveau, en qualité de directeur général de la gendarmerie nationale, je m'engage fortement pour que notre réponse ministérielle par rapport aux problématiques de cybersécurité soit vraiment structurée et que nous ayons une entité forte qui permette de prendre en compte ce sujet de manière solide et ambitieuse.

Les enjeux sont considérables ; la réponse que nous comptons apporter sera bien sûr résolue et particulièrement ambitieuse. Je souhaite, comme vous l'avez fait Monsieur le président au nom des organisateurs, un excellent FIC 2014 à tous nos invités. Je souhaite que ce FIC nous permette ensemble d'innover pour faire progresser la cybersécurité.


Général Denis Favi
Directeur Général

Discours au Forum International de la Cybersécurité

À Lille, mardi 21 janvier 2014

M. Manuel Valls, ministre de l'Intérieur

Mesdames, messieurs,
A la même époque, l'année dernière, j'avais le plaisir de clore les travaux de la 5e édition du Forum International de la Cybersécurité. C'est avec un plaisir renouvelé que je viens, aujourd'hui, ouvrir cette 6e édition.

Je tiens, tout d'abord, à féliciter le conseil régional du Nord Pas-de-Calais, et son premier vice-président Pierre de SAINTIGNON, pour l'organisation de cette manifestation, conduite en partenariat avec la gendarmerie nationale et CEIS.
La qualité des invités, la présence de membres de gouvernements étrangers, que je salue chaleureusement, témoignent de la réputation désormais établie de cet espace de réflexion et d'échanges, lancé en 2007. Le caractère précurseur de cette initiative montre combien la gendarmerie, au même titre que la police nationale, sont des institutions en phase avec leur temps.

Nous tous sommes – et chaque jour davantage – immergés dans un monde de données. Nous les créons, les exploitons, les transmettons, faisons en sorte de les protéger. Ces données sont intellectuelles, commerciales, juridiques, ou encore financières et fiscales. Elles sont, aussi et surtout, des données d'identification, constitutives de notre identité numérique. Elles disent ce que nous sommes, ce que nous faisons. Et même ce que nous pensons.
Cette identité est, par définition, précieuse. Elle peut cependant être attaquée, détournée, usurpée. Ces atteintes nuisent alors profondément à la confiance, pourtant indispensable pour l'essor du cyberespace.

Face à cela, chaque acteur a une responsabilité et un rôle à jouer. L'État joue pleinement le sien. Il doit assurer dans la sphère virtuelle – autant que dans la sphère réelle – la sécurité de nos concitoyens, mais aussi celle de nos entreprises et plus largement des intérêts de la Nation. Cette action intervient dans un cadre indépassable, celui du respect des libertés fondamentales : respect de la vie privée et de la liberté d'expression.
Lutter contre les cybermenaces demande d'intégrer une triple exigence :
tout d'abord, en avoir une bonne connaissance, sans se limiter à la cybercriminalité ;
ensuite, adapter les réponses opérationnelles, en portant, notamment, une attention particulière à la politique de prévention ;
enfin, mieux piloter et coordonner les moyens engagés et les différents services impliqués.

Ce sont ces trois exigences que je veux détailler devant vous.

1. Face à une sphère virtuelle en mutation permanente, une connaissance des usages et des menaces potentielles est indispensable.

Nous sommes, en effet, devant un phénomène en pleine expansion ; un phénomène complexe et global, mal appréhendé par un droit qui est soit peu adapté, soit en construction, et en tout cas sans réelle cohérence.
La cybercriminalité nous renseigne de façon parcellaire sur l'état réel de la menace : que sont les 1 100 faits d'atteintes aux systèmes d'information dénoncés aux services de police et aux unités de gendarmerie, en 2011, par rapport à la réalité vécue par les entreprises et les administrations ? Un simple aperçu !
La plateforme PHAROS de signalement de contenus illicites de l'Internet, opérée par l'OCLCTIC, donne un éclairage complémentaire. Avec près de 124 000 signalements en 2013, elle atteint un nouveau record, signe de la vigilance des internautes.
Nous devons être en mesure d'appréhender des menaces toujours plus diverses : risques de déstabilisation de l'activité économique, atteintes à l'e-réputation, menaces pesant sur l'ordre public et la sécurité du territoire mais aussi diffusions de messages de haine (racistes, antisémites, antireligieux, homophobes, …), radicalisation, embrigadement, recrutement par des filières terroristes.
Le réseau mondial est aussi celui où se rencontrent, se fédèrent, se préparent, souvent dans l'obscurité, les pires intentions. Internet est un lieu de liberté certes, mais cela ne doit pas être une zone de non droit où l'on pourrait tout se permettre.
Les menaces de l'Internet concernent tout le monde, ne serait-ce que du fait de la progression de la fraude sur les moyens de paiement à distance. Mais elles ciblent, en particulier, les plus jeunes. Une étude récente a ainsi souligné que 40% des élèves disent avoir été victimes d'une agression en ligne.
Nous devons donc mettre en œuvre des politiques publiques à la hauteur de ces enjeux.

Des enjeux qui sont éclairés par un travail qui va au-delà de nos frontières. Le monde virtuel n'en connaît pas. À ce titre, je veux saluer la contribution du centre de lutte contre la cybercriminalité EC3 d'Europol. En un an, il contribuait à la résolution de plusieurs dossiers d'enquête complexes et permis de compléter la vision des risques cyber auxquels nous, pays européens, sommes confrontés.

Seule une démarche globale peut nous permettre de prendre la mesure d'une menace elle-même globale.

Ceci passe par une approche décloisonnée ; décloisonnée entre services, entre matières. Travaux de recherches, observatoires thématiques, veille des réseaux numériques, surveillance des activités des groupes criminels et terroristes, alertes sur la sécurité des systèmes d'information : c'est l'ensemble de ces démarches qui permettent d'appréhender les risques et de piloter au mieux la réponse opérationnelle.

2. De nombreuses actions sont mises en œuvre, chaque jour, pour contrer ces nouvelles formes de menaces qui ont chacune leur spécificité.

Je connais la mobilisation des acteurs européens, étatiques, industriels. Je vais visiter, dans quelques instants, les stands des partenaires institutionnels, des industriels, des PME-PMI, des écoles et des universités. Je sais que leur objectif commun est d'améliorer la confiance dans l'espace numérique, de proposer un cyberespace plus sûr et protecteur de nos libertés fondamentales.

Je sais que les attentes les plus grandes à l'égard de l'action de l'État viennent des entreprises, qui demandent une protection efficace contre les atteintes aux systèmes d'information, les fraudes, l'espionnage industriel.

Et il y a urgence ! Par exemple, en décembre, dans deux régions françaises, deux PME ont été victimes d'escroqueries aux faux ordres de virement pour des montants respectifs de 480 000 € et 450 000€. Pour l'une d'entre elle, les escrocs ont pris la main sur le système d'information de la société pour finaliser la transaction. Depuis 2011, ce type d'escroquerie représente un préjudice estimé à plus de 200 millions d'euros pour les entreprises françaises. Ce chiffre prend un relief tout particulier alors que les entreprises françaises doivent s'adapter à une concurrence internationale de plus en plus forte.

La loi de programmation militaire, récemment adoptée, renforce le dispositif de protection des entreprises les plus sensibles. Elle conforte et amplifie le rôle de l'Agence nationale de la sécurité des systèmes d'information – dont je salue le directeur présent aujourd'hui – dans le contrôle de nos opérateurs d'importance vitale. Cette mesure était prioritaire. Au-delà, les entreprises qui forment notre tissu économique, bénéficient au quotidien

de l'action des services de la police et des unités de la gendarmerie qui les sensibilisent aux cyber-risques dans le cadre de leurs missions d'intelligence économique. Cette action territoriale, s'adressant tant aux grandes entreprises qu'aux PME-PMI participe de la réponse globale de l'État.

Une réponse qui doit concerner l'ensemble de nos concitoyens. J'ai d'ailleurs la conviction que le niveau de sensibilisation à la cybersécurité est encore insuffisant et que nous avons, dans ce domaine, de grandes marges de progression.

Aussi, je me félicite des initiatives de la police et de la gendarmerie à destination des plus jeunes, à l'image de l'opération « Permis Internet » mise en place par la gendarmerie nationale, en partenariat avec AXA Prévention. Je viens d'ailleurs de remettre des « Permis Internet » aux élèves de CM2 de l'école Roger Salengro d'Hallennes-lez-Haubourdin. Au sein de leur établissement scolaire, depuis quelques semaines, ils apprennent à utiliser en sécurité l'Internet, à mieux identifier les dangers auxquels ils peuvent être confrontés. Ils deviennent donc des Internautes avertis.

L'année dernière, je m'exprimais devant vous à l'issue de longs débats sur la loi antiterroriste. Je vous avais alors fait part de ma volonté et de celle du gouvernement de lutter plus efficacement encore contre le cyber terrorisme.

Plus largement, renforcer notre efficacité en matière de cybercriminalité nécessite de prendre un certain nombre de mesures : adapter notre arsenal juridique, coordonner l'action de tous les services de l'État, sécuriser les titres d'identité et leur exploitation ou encore améliorer la formation des personnels de tous les ministères concernés.

C'est pourquoi, j'ai souhaité la constitution d'un groupe de travail interministériel, réunissant, sous la présidence d'un haut magistrat, des représentants des ministères de l'Économie et des Finances, de la Justice, de l'Intérieur et de l'Économie numérique. Les travaux menés, depuis l'été 2013, sous la présidence du procureur général Marc ROBERT, sont achevés. Les conclusions seront remises aux quatre ministres dans les prochains jours.

J'attends des propositions ambitieuses, notamment en termes de techniques d'enquête ou de recueil et de traitement des plaintes. J'attends, également, des propositions permettant d'améliorer l'organisation de nos services et d'offrir aux citoyens un dispositif plus lisible et plus proche de leurs préoccupations. Il s'agira naturellement, à court terme, et en parallèle des évolutions de l'organisation du ministère de la Justice, de renforcer les capacités d'investigation pour les infractions spécifiques liées au monde cyber en s'appuyant sur les enquêteurs spécialisés en technologies numériques de la gendarmerie et de la police.

3. Je souhaite également qu'au sein du ministère de l'Intérieur soit menée une réflexion de fond pour développer une capacité fine de pilotage et de coordination dans la lutte contre les cybermenaces.

Nous devons fédérer les actions des différents services, faire le lien entre les capacités d'anticipation, la politique de prévention, les efforts de recherche et développement et les dispositifs de répression.

L'attention que je porte aux moyens consacrés, au sein du ministère de l'Intérieur, à la lutte contre les cybermenaces s'étend bien évidemment à ceux dédiés à la sécurité et la défense de ses propres systèmes d'information.

Les systèmes d'information mis en œuvre pour la sécurité intérieure et pour la conduite de l'action territoriale de l'État ne peuvent souffrir d'aucun manquement à leur propre sécurité. Ces outils permettent, au quotidien, l'action de notre administration, de nos forces. Le ministère de l'Intérieur est ainsi engagé au premier chef dans les démarches entreprises par les services du Premier ministre, afin de renforcer et garantir la sécurité de nos systèmes d'information.
J'ai donc demandé aux directeurs de la gendarmerie et de la police nationales de me proposer une stratégie de lutte contre les cybermenaces, sous 3 mois, et de définir un véritable plan d'action. Cette réflexion s'appuiera sur les compétences développées au sein du ministère mais devra également, le cas échéant, définir ce qui nous manque. Elle pourra déboucher sur des évolutions structurelles.
En outre, dans le cadre de la réforme des statistiques, j'avais demandé que l'on améliore la mesure des phénomènes de cyber-délinquance, et ce dans le cadre rigoureux des principes de la statistique publique. Les travaux de conception sont désormais bien avancés et je demanderai au chef du nouveau service statistique ministériel (SSM), dès sa prise de fonction fin février, de se prononcer sur le nouvel indicateur composite. Celui-ci devra clairement distinguer les atteintes directes aux systèmes d'information, les infractions liées aux contenus, les fraudes et escroqueries réalisées par l'internet, etc. Il est grand temps d'améliorer la qualité, la disponibilité et la régularité des données publiques sur ces enjeux fondamentaux de sécurité.

Enfin, si la sécurité du cyberespace relève en premier lieu de l'État, elle passe, aussi, nécessairement, par une mobilisation autour de partenariats avec le monde académique et les acteurs privés, fournisseurs de services et industriels de la sécurité des systèmes d'information.

Aussi, je salue la création cet après-midi, dans cette même enceinte, du « centre expert contre la cybercriminalité français (CECyF) », qui associera dans un premier temps la gen-

darmerie et la police nationales, les douanes, des écoles d'ingénieurs et universités – l'EPITA, l'Université de Technologie de Troyes – et des industriels – Orange, Thales, Microsoft France et CEIS.
Ce centre permettra l'émergence d'une communauté d'intérêts autour de la lutte contre la cybercriminalité. Les objectifs sont clairs : contribuer à la réflexion stratégique dans ce domaine, développer des actions de formation et encourager la mise au point d'outils d'investigation numérique et de travaux de recherche.

Mesdames, messieurs,
Chaque époque connaît des mutations techniques, technologiques. Elles sont porteuses de progrès pour nos sociétés tout en générant des contraintes, des menaces nouvelles qu'il faut savoir intégrer. Comme vous le voyez, les pouvoirs publics se sont pleinement saisis des enjeux liés au monde cyber.

Chaque phénomène, chaque menace doit pourvoir trouver une réponse adaptée. Mais l'essor du réseau mondial nous oblige à agir en réseau, à mobiliser l'ensemble des acteurs pour assurer la cybersécurité, c'est-à-dire simplement la sécurité de tous.

Discours au Forum International de la Cybersécurité

À Lille, mardi 21 janvier 2014

M. Jean-Yves Le Drian, Ministre de la défense

Madame et Messieurs les ministres,
Monsieur le Vice-Président du Conseil régional,
Mesdames et Messieurs les élus,
Messieurs les officiers généraux,
Mesdames et Messieurs,

Je suis très heureux d'être avec vous pour cette nouvelle édition du forum international de la cybersécurité, et de pouvoir m'exprimer devant vous au terme de cette première journée.

Je comprends que les débats ont été riches et animés depuis ce matin. J'y vois la preuve que nous devons plus que jamais, sur les questions de cybersécurité et de cyberdéfense, rapprocher les domaines techniques et non-techniques, experts et non experts. C'est bien ce décloisonnement qui fait le succès du FIC depuis sa création en 2007. Je saisis cette occasion pour remercier les fondateurs de ce forum, la Gendarmerie nationale et la région Nord pas de Calais, que je salue particulièrement en la personne de Philippe de Saintignon, son premier vice-président. Je les remercie d'organiser une nouvelle fois, avec CEIS, un salon au succès toujours grandissant.

Je remettrai tout à l'heure le Prix du livre cyber. En m'y préparant, j'ai constaté que les ouvrages en compétition illustrent la complexité des enjeux de la cybersécurité, dans ses différents domaines (technique, économique, juridique, stratégique, RH), mais aussi la diversité de ses acteurs (autorités gouvernementales, forces armées, forces de sécurité, grandes, moyennes et petites entreprises, chercheurs et acteurs de la formation, et simples citoyens). Je me réjouis de cette ouverture. Dans ce domaine en particulier, nous avons le devoir d'élargir autant que possible notre champ d'analyse.

Le ministère dont j'ai la charge est directement

intéressé par la menace cyber et j'ai décidé d'en faire l'une de ses priorités.
Il revient en effet à la Défense de mettre en œuvre les moyens correspondant aux différentes postures de protection du territoire et de la population, y compris pour la sauvegarde maritime et aérienne, de dissuasion nucléaire, ainsi que de conduite des interventions militaires. À ce titre, elle développe et opère des systèmes d'information et de communication particulièrement complexes, qui sont des supports essentiels pour toutes nos opérations militaires, tant en France qu'à l'extérieur du territoire national.

Le ministère de la défense est responsable des systèmes les plus stratégiques, ceux qui sont liés à la dissuasion nucléaire, mais également les systèmes d'attaque et de défense les plus sophistiqués comme ceux des sous-marins, avions de combats, missiles, frégates ou véhicules de combat terrestres.

Les responsabilités qu'il me revient d'exercer s'étendent, au-delà du territoire national, partout où nos forces sont stationnées chez des pays alliés. Je me félicite d'ailleurs de la présence, aujourd'hui, de nombreuses délégations étrangères, et en premier lieu de Mme la ministre de l'informatique et des télécommunications du Qatar, avait qui j'ai eu l'occasion d'échanger quelques mots tout à l'heure. Son intervention a montré que nous avons les mêmes préoccupations.

Nos forces font en outre face à des menaces cyber spécifiques. Je pense à la zone du Golfe arabo-persique. Je pense aussi, bien sûr, aux opérations militaires décidées par le Président de la République, comme c'est actuellement le cas au Mali et en Centrafrique. S'ajoutant à celles que nous connaissons sur le territoire national, force est de constater que le risque n'a cessé, ces dernières années, de s'accroître. Le nombre d'attaques sur les seuls sites du ministère de la défense a ainsi été multiplié par 4 en deux ans. Pour l'instant nous les contenons : elles visent la compromission d'informations, voire la paralysie de nos systèmes, mais leur effet est faible aujourd'hui.

Mais au-delà de ces cyberattaques qui relèvent de la cybercriminalité et de l'espionnage, l'hypothèse d'attaques informatiques majeures s'est renforcée depuis la parution du Livre blanc en 2008. C'est l'analyse que porte le nouveau livre blanc. Ce qui est désormais en jeu, c'est la capacité de contrôle, de paralysie à distance, ou bien de destruction d'infrastructures vitales pour notre pays. Se présente, désormais, le risque d'atteinte grave aux intérêts stratégiques de l'État, à notre autonomie d'appréciation, de décision et d'action, par la menace cyber.

Devant des menaces majeures, qui peuvent aller jusqu'à de véritables actes de guerre, militaires ou non directement militaires, il y a un enjeu de premier ordre pour la défense, la souveraineté, la sécurité de notre Nation.

Cet enjeu représente un champ stratégique à part entière, entièrement nouveau, que nous commençons seulement à appréhender et dont les règles, les techniques, les rapports de forces, doivent encore largement être explorés ou inventés.

Le ministère de la défense l'a perçu depuis quelques années. Pour y répondre, il a développé et renforcé des compétences de pointe. Il possède aujourd'hui une expertise, tant opérationnelle que technique, qui est reconnue dans le domaine de la cyberdéfense. Ses capacités uniques sont au service de la posture nationale de cyberdéfense.
Il appuie ainsi l'ANSSI dans sa mission interministérielle de sécurité des systèmes d'information. Il travaille étroitement avec l'ensemble de ses partenaires étatiques.

Mais nous ne pouvons pas nous arrêter là, face à la menace grandissante dont j'ai parlé. Il faut changer d'échelle. Face à un nombre d'attaques qui double chaque année, nous devons recruter des experts, aptes à protéger, détecter, réparer, répliquer. Nous devons former tous nos personnels, depuis les simples utilisateurs jusqu'aux experts chevronnés, à qui il faudra offrir des perspectives de carrière. Nous devons aussi aider à structurer une base industrielle encore beaucoup trop fragile. Nous devons enfin nouer des partenariats avec le monde civil comme avec nos alliés dans le monde.
Fort de cette ambition pour la cyberdéfense, je lancerai dans quelques semaines un « Plan Défense Cyber ». Ce plan, sur le modèle de ce que j'ai mis en place pour les PME avec le « Pacte défense PME », formalisera les objectifs que je souhaite fixer et les actions à mener, tant au sein du ministère qu'avec ses partenaires, publics et privés.

L'enjeu est que l'excellence du ministère en matière de cyberdéfense soit encore renforcée, et de progresser à la mesure des défis qui nous font face.

Ce Plan embrassera tous les aspects de la cyberdéfense. Outre les mesures propres à l'organisation et aux moyens du ministère, il comportera des dispositions destinées à créer ou soutenir des dynamiques extérieures. À cette fin, il apportera un socle sur lequel des initiatives venant des collectivités locales, des grands groupes ou des opérateurs de formation, pourront trouver un appui décisif. Il contribuera à mobiliser les énergies de toute la Défense.
Dans le même esprit de mobilisation collective, le Plan Défense Cyber permettra à chaque acteur de la communauté nationale de cyberdéfense, qu'il soit militaire ou civil, public ou privé, d'identifier les meilleures voies de coopération avec mon ministère, ou un soutien pour ses projets.

Je souhaite que ce Plan Cyber concrétise ainsi une avancée majeure, au service de la posture nationale de cyberdéfense, et toujours en appui de l'ANSSI dans sa mission interministérielle de sécurité des systèmes d'information.

Permettez-moi donc de vous en dire quelques mots plus en détail.

Mon souci est bien sûr de répondre en premier lieu aux besoins de la défense, et en particulier à ceux de nos forces en opérations. Pour cela, nous leur apporterons de nouvelles capacités défensives et offensives, appuyées par un renseignement d'intérêt cyber que j'entends voir développer de façon volontariste. Mais nos efforts ont également vocation à servir les intérêts de la Nation dans son ensemble, conjointement avec l'ANSSI et le ministère de l'Intérieur, au sein d'une communauté nationale de cyberdéfense, fondée sur la confiance, portée par des objectifs communs, à savoir améliorer la protection de nos administrations et de nos entreprises face aux nouvelles menaces informatiques.

Le centre de cyberdéfense du ministère, le CALID, continuera à voir ses effectifs renforcés. Ils étaient 20 en 2011, ils seront 6 fois plus nombreux à la fin de la LPM. Le CALID travaillera étroitement avec le centre opérationnel de l'ANSSI, le COSSI – avec lequel il est d'ailleurs co-localisé depuis quelques semaines –, ainsi qu'avec ses homologues des pays alliés. Son action dépasse d'ailleurs le ministère, car le CALID peut intervenir en prévention ou en réaction à des incidents ou des attaques informatiques au sein de groupes d'action rapides.

De leur côté, les effectifs cyber du centre « Maîtrise de l'information », de la Direction Générale de l'Armement, vont presque doubler, pour passer de 250 à 450 dans les années qui viennent. Ils contribuent, entre autres, à développer des équipements assurant un haut niveau de protection pour les forces armées, mais aussi pour l'interministériel, toujours en étroite collaboration avec l'ANSSI.

J'attacherai également une grande importance à la base industrielle et technologique. Vous savez que c'est l'une de mes préoccupations constantes, dans tous les domaines de la défense.

Je me félicite de la création par le premier ministre du comité de filière des industries de sécurité (le COFIS), et je sais qu'Hervé Guillou, ici présent, que je salue, vous le décrira dans le détail ce soir.

Je salue également le plan cybersécurité annoncé par Arnaud Montebourg, l'un des 34 plans de son programme « la France Industrielle ». Nous contribuerons fortement à ces initiatives.

Sur notre propre périmètre, nous allons déjà tripler le volume des études amont consacrées à la cyber. Nous poursuivrons aussi la montée en puissance du dispositif de soutien à l'innovation RAPID, pour aider les PME à développer en peu de temps des projets concrets et innovants dans le domaine de la cybersécurité et de la cyberdéfense.
J'en viens maintenant aux capacités en relation avec la Nation, en particulier à la réserve. En

2012, le ministère a pris l'initiative de créer une réserve citoyenne spécialisée en cyberdéfense. Mise en place en 2012, cette réserve cyber est animée par l'amiral de Coustillière et M. Luc François Salvador, que je remercie pour leur implication. Elle comprend déjà plus de quatre-vingts réservistes actifs. L'élargissement de son réseau est en cours, notamment en province. Ainsi, nous toucherons un plus grand nombre d'acteurs de la société civile. Je pense notamment aux petites et moyennes entreprises, ainsi qu'aux petites et moyennes industries. De nombreux représentants de cette réserve sont présents au FIC. Ils ont contribué au succès du Challenge, et certains sont d'ailleurs les auteurs des ouvrages en compétition pour le Prix du Livre Cyber. Je tiens à les saluer.

J'entends que nous développions également une réserve opérationnelle cyber. L'enjeu est ici de pouvoir mobiliser des effectifs toujours plus importants de personnes de compétences et de confiance, pour appuyer l'État dans la gestion d'une crise cyber. Si le Livre blanc a identifié le besoin d'une telle composante au service de la résilience de la Nation, il reste à présent à en définir les contours, ainsi qu'à trouver les moyens et modalités de son véritable essor.

Je finirai cette brève présentation par deux sujets qui me tiennent à cœur. Le premier est juridique. Pour la première fois, le cadre juridique de la cyberdéfense a été défini par le législateur, sur des bases claires et novatrices, qu'il s'agisse de la définition des pouvoirs réglementaires du Premier ministre, des obligations imposées aux opérateurs d'importance vitales, ou bien de la capacité à se défendre et à riposter dans le cyberespace. Grâce à la loi de programmation qui vient d'être votée, nous avons ainsi comblé un vide.

Le deuxième, et dernier sujet, est la création du pôle d'excellence Cyber en Bretagne, que j'avais évoquée en juin dernier à Rennes, et que le Premier ministre a inscrit dans le Pacte d'avenir pour la Bretagne. J'ai donné mandat à l'Ingénieur en chef de l'armement Paul-André PINCEMIN de mener à bien ce projet. Vous connaissez mon attachement à la région Bretagne, mais c'est d'abord parce que le ministère de la défense y dispose d'implantations uniques dans ce domaine que j'ai décidé d'y installer ce pôle. Je pense à l'école des transmissions de Rennes, au centre DGA « Maîtrise de l'information » à Bruz, à l'école de Saint-Cyr Coëtquidan, et je pourrais également évoquer l'École Navale à Brest ou l'ENSTA Bretagne, entre autres. Dédié à la formation, à l'entraînement ainsi qu'à la R&D, ce pôle s'appuiera sur cette expertise unique en France, et bénéficiera d'un tissu académique et industriel dense, particulièrement propice à son développement et à son rayonnement.

L'ensemble de ces actions sont présentées sur le stand du ministère de la Défense, que je vous invite à aller visiter, si vous ne l'avez

pas déjà fait. Tous les personnels des forces, du CALID, de la DGA et de la réserve citoyenne cyber, vous expliqueront, avec la passion qui les anime, les actions qu'ils mènent au quotidien.

Mesdames et Messieurs,
En l'espace de quelques années seulement, le sujet de la cybersécurité, qui semblait jusqu'ici réservé à une petite communauté d'initiés, s'est élevé en France au rang de priorité nationale. Ce sujet très technique, qui a pu paraître obscur, est aujourd'hui omniprésent. Il touche à des questions aussi fondamentales que notre sécurité, notre autonomie d'appréciation, de décision et d'action – en un mot, à l'essence de notre souveraineté.

Cette prise de conscience fut brutale ; elle a pu être déstabilisante. Pour sa part, le ministère de la Défense est au rendez-vous du défi immense qui se pose à chacun d'entre nous. À travers ses capacités et son expertise, il assume plus que jamais le rôle qui doit être le sien, en lien avec tous les autres acteurs de la communauté nationale de cybersécurité. Les menaces cyber nous concernent tous. C'est collectivement que nous parviendrons à y répondre.

Je vous remercie.

Allocution de Monsieur Toomas Hendrik ILVES, président de la République d'Estonie.

À Lille, mercredi 22 janvier 2014

Bonjour. Pouvez-vous imaginer ce que serait la vie si vous n'aviez pas de tablette, de téléphone portable, d'ordinateur ?… Quand j'étais enfant, je me demandais comment mes parents vivaient sans télévision. De la même manière, mes enfants me demandent aujourd'hui « comment c'était avant les ordinateurs ». C'est une illustration très concrète de l'importance prise dans nos sociétés, en 20 ans, par les technologies digitales. Dans mon pays, l'Estonie, nous avons fait un gros chemin en matière d'utilisation des technologies de la communication. Nous avons fait ce chemin aussi en 20 ans, le temps d'une génération.

La base d'une société digitale qui réussit, c'est la confiance. Vous devez avoir confiance pour créer une économie digitale qui fonctionne. Cela suppose, et c'est crucial, de disposer d'une identité en ligne sécurisée. Dans le monde cyber, vous devez savoir qui sont ceux qui accèdent à vos données, qui sont ceux à qui vous vous adressez. Pour reprendre l'image d'un dessin animé d'il y a vingt ans, sur Internet, personne ne sait que vous êtes un chien. Cela peut prêter à rire mais en fait le sujet de l'identité est essentiel pour tout ce que vous entreprenez dans le monde digital.

En Estonie, nos services en ligne fonctionnent extrêmement bien parce que nous avons prêté la plus grande attention à la question de l'identité, aux questions techniques. Nous avons un système d'identification à deux facteurs qui permet à nos citoyens de donner avec confiance leurs identités lorsqu'ils en ont besoin. Notre gouvernement a progressé dans un domaine où l'offre commerciale est un échec. Le secteur privé n'a pas été en mesure d'offrir jusqu'à présent une identification sécurisée à grande échelle. Le gouvernement, qui souhaite favoriser l l'économie digitale, l'offre aux citoyens comme un service. Nous garantissons la

sécurité là où le secteur privé ne le fait pas. Les gouvernements, partout, garantissent la sécurité, la police pour leurs concitoyens. En Estonie, le gouvernement garantit la sécurité des communications en ligne, si vous souhaitez les utiliser. En Europe, aujourd'hui, une crainte de Big Brother se diffuse. Cela ne nous concerne pas en Estonie. Cette peur est le principal obstacle à un développement des e-services en Europe. Big Brother, ce n'est pas forcément le gouvernement. Ce peut être des sociétés privées, qui traquent tous vos faits et gestes, qui savent tout de vous et peuvent le dire à des tiers. Nous avons à prendre en compte ce problème. Nous avons une réglementation qui protège la vie privée mais nous devons travailler davantage dans cette voie.

Nous ne devons pas balkaniser notre vie digitale. Nous ne comprenons pas la véritable nature d'une identité en ligne sécurisée, nous n'avons pas de standards clairs sur la manière dont les données peuvent, doivent ou devraient être utilisées. Dans mon pays, le citoyen possède ses données et sait comment elles sont utilisées. C'est une condition sine qua non pour avoir une société digitale humaine. Un autre point sur lequel nous devons adapter notre législation au monde réel est la liberté de circulation des services. Nous savons tous que la liberté de circulation des services est une liberté fondamentale affirmée dès 1956 dans les documents fondateurs de l'Union européenne. Cette liberté fondamentale a mis du temps à s'établir dans le monde physique. Dans le monde cyber, elle est encore plus pertinente. Nous voyons bien comment l'Europe est à la traîne de pays comme les Etats-Unis, où la liberté de circulation des services digitaux a permis de nous surpasser dans bien des domaines.

Cette liberté fondamentale doit être mise en place. Si on ne l'étend pas au domaine digital, nous serons encore plus à la traîne, je le crains. Nous devons travailler à un cadre légal, nous devons permettre le développement des e-services au sein de l'UE dans son ensemble. Cela donnera un coup de fouet à notre économie, nous le comprenons tous. Bien sûr, les effets du développement digital de la société vont au-delà du simple domaine économique. Selon ma propre expérience, c'est un bénéfice pour le développement de tout le pays. Cela a permis à mon petit pays, plutôt pauvre initialement, d'évoluer en 20 ans et de faire des choses qui n'auraient pas été possibles à un territoire aussi petit que le nôtre. Pour reprendre la métaphore, je pense que l'Europe serait bien plus grande si on permettait aux services digitaux et au monde cyber d'atteindre leurs pleines possibilités.

Dans ce monde digital, la taille d'un pays n'a plus d'importance. La technologie nous permet d'être plus grands que nous ne le sommes physiquement. Nous encourageons tous nos partenaires et amis européens à travailler à leur propre version d'une question fondamentale, celle de l'identité sécurisée en ligne, qui permettra à l'Europe, j'en suis persuadé, de s'épanouir.

Discours de Monsieur Francis Delon secrétaire général de la défense et de la sécurité nationale

À Lille, mercredi 22 janvier 2014

Madame la ministre, Monsieur le Président, Messieurs les officiers généraux, Mesdames, Messieurs,

Chacun a pu le constater, ce sixième « forum international de la cybersécurité » est un succès. Succès bien sûr par la qualité de ses intervenants, la qualité des conférences plénières et des ateliers, succès également par l'affluence croissante des participants année après année, succès enfin par l'internationalisation du forum puisque des représentants de quarante-deux pays y ont pris part.

Ce succès n'est évidemment pas un hasard. Il est le fruit de l'initiative du Général Watin-Augouard du soutien fidèle de la région Nord-Pas-de-Calais et de l'engagement sans faille de la gendarmerie nationale dont je salue ici les représentants, Pierre de Saintignon, premier vice-président de la région et premier adjoint au maire de Lille et le général de corps d'armée Richard Lizurey, major général de la gendarmerie nationale.Le succès de ce forum est également issu d'un partenariat public privé efficace, puisqu'à côté des acteurs publics que je viens de citer et de quelques autres, se trouvent CEIS – la compagnie européenne d'intelligence stratégique – et son dynamique président Olivier Darrason qui a œuvré depuis plusieurs mois à l'organisation de ce forum ainsi que de nombreuses entreprises de toutes tailles, qui, par leur soutien, ont permis à ce forum de se tenir dans d'excellentes conditions et de donner lieu à des échanges particulièrement féconds. Cette collaboration public-privé me semble d'ailleurs le modèle qui pourrait nous permettre, demain, de vivre dans une société numérique plus sûre.

Je développerai ce point, si vous le voulez bien, en évoquant les rôles qu'ont, selon moi, l'État, les opérateurs et les collectivités territoriales en matière de cybersécurité.

Mais avant tout, je voudrais revenir aux fon-

dements de notre présence ici : pourquoi la sécurité des systèmes d'information est-elle un sujet qui nous mobilise ? Pourquoi agit-on ? Pourquoi les efforts humains et financiers de l'État et de certaines entreprises dans ce domaine sont nécessaires ? Et pourquoi une telle attention est-elle portée au sujet par une collectivité territoriale ?

Réellement engagée depuis une quinzaine d'années, la numérisation du monde est déjà à un stade avancé. Une jeunesse née dans un monde connecté fait émerger une société nativement numérique. Cette société est celle du partage universel des connaissances et de la communication interpersonnelle. Elle bénéficie des atouts du numérique et du confort de vie qu'il apporte. Elle cherche la valeur ajoutée des services numériques, pilier de la croissance des économies modernes.

Source d'enthousiasme, cette numérisation du monde est simultanément porteuse de menaces préoccupantes :

menaces économiques et sociales. Certains acteurs du numérique, virtuellement installés dans des pays qui sont presque devenus des plates-formes d'évasion juridique offshore, se comportent en prédateurs. Ces mêmes acteurs utilisent toutes les possibilités offertes par les technologies pour collecter et exploiter toute information personnelle susceptible d'être monnayée, au mépris de la vie privée ;

menaces criminelles. Ce sujet vous a été largement exposé au cours de ce forum. Le retour financier pour les auteurs de crimes ou de délits via le cyberespace dépasse désormais le retour financier issu du trafic de drogue, avec un risque bien moindre d'être inquiété par la justice. Or nous n'en sommes qu'au début de la créativité criminelle dans ce domaine…

menaces stratégiques. Elles sont désormais largement médiatisées. Certains acteurs privés ou publics utilisent le cyberespace pour mener des opérations d'espionnage massives, systématiques et organisées. Ces opérations minent la confiance entre les peuples, entre les États, entre le peuple et son État.

Elles déstabilisent des entreprises et ruinent leurs efforts en matière de compétitivité. On peut d'ailleurs craindre que les révélations égrenées au cours de l'année 2013 en ce domaine entraînent une prolifération de ces pratiques, tant par l'attitude transgressive qu'elles favorisent que par les techniques et méthodes qu'elles divulguent et qui risquent désormais de proliférer.

Les menaces stratégiques et les menaces criminelles issues du cyberespace ont un point commun : elles sont rendues possibles par la faiblesse du niveau de sécurité de nos systèmes d'information. Chaque administration, chaque entreprise, chaque collectivité territoriale qui n'assure pas la sécurité des systèmes d'information dont elle a la charge a une part de responsabilité dans la concrétisation de ces menaces.

Face à ces menaces, quel peut être le rôle de l'État, des entreprises et des collectivités territoriales ?

Pour l'État, il s'agit de se défendre contre une menace de niveau stratégique, susceptible de le déstabiliser. Le général de Gaulle, qui n'a pourtant pas connu l'explosion du numérique, en a donné le sens, le 14 juin 1952 à Bayeux, en disant : « *La défense est la première raison d'être de l'État. Il n'y peut manquer sans se détruire lui-même.* ».

S'agissant du cyberespace, la première mission de l'État est de sécuriser et de défendre les systèmes d'information les plus critiques de notre pays, ceux qui participent à notre potentiel de guerre ou économique, à la sécurité ou à la capacité de survie de la Nation. Cette priorité a été rappelée par le Livre blanc de la défense et la sécurité nationale de 2013, qui a classé la menace liée aux attaques informatiques parmi les menaces les plus graves pouvant atteindre notre pays.

Comme vous le savez, la sécurité et la défense des systèmes d'information sont une responsabilité du Premier ministre. L'agence nationale de la sécurité des systèmes d'information, qui m'est rattachée, est son bras armé dans l'exercice de sa compétence et de son autorité. Dans son article 21, la loi de programmation militaire votée par le Parlement en décembre dernier précise les responsabilités du Premier ministre dans la définition de la politique nationale et la coordination gouvernementale en matière de sécurité et de défense des systèmes d'information.

La loi de programmation militaire traduit les mesures annoncées par le Livre blanc pour renforcer la sécurité des systèmes d'information des opérateurs d'importance vitale. L'année 2014 sera donc particulièrement active pour l'ANSSI puisque, outre ses missions habituelles et notamment le traitement d'attaques informatiques qui touchent les opérateurs d'importance vitale ou le déploiement de moyens de communication sécurisé pour les hautes autorités de l'État, l'agence va piloter un travail de fond avec les opérateurs concernés par la loi, afin de les aider à mettre au niveau de sécurité nécessaire leurs systèmes d'information les plus critiques.

La révolution numérique nous expose donc à des menaces inouïes. Elle n'en ouvre pas moins de formidables opportunités. L'industrie et les services du numérique relèvent, pour certains de ces services, d'activités stratégiques. La France doit être capable d'indépendance technologique dans ces activités afin de garantir son autonomie. C'est une exigence pour un pays comme le nôtre. Et c'est aussi une opportunité car ces secteurs d'activité sont une source extrêmement prometteuse de croissance économique et représentent un gisement d'emplois qualifiés.

La volonté du Gouvernement de soutenir une politique de défense et de sécurité des systèmes d'information s'incarne donc également dans le développement d'une politique industrielle cohérente. Je veux citer le plan cybersécurité, qui est l'un des 34 plans de la nouvelle France industrielle présentée par le président de la République, porté par le ministre du redressement productif et confié au directeur général de l'ANSSI. Je veux également citer les appels à projets

lancés dans le cadre des investissements d'avenir qui visent notamment au développement d'équipements de sécurité de confiance, ou encore le volet cybersécurité de la filière sécurité piloté par le SGDSN.
Un effort particulier est également mené en matière de recherche et va l'être en matière de formation, à la fois dans l'enseignement supérieur et à destination des plus jeunes.

J'en viens maintenant au rôle que doivent jouer les entreprises en matière de cybersécurité.
Le rôle des entreprises est notamment de créer de la richesse. Or, désormais, la chaîne de la valeur de l'entreprise est tout entière dépendante de systèmes d'information. Dès lors, une défaillance de ces systèmes, – que ce soit en raison d'une simple panne, d'une malveillance ou d'une attaque informatique –, peut ruiner l'entreprise, et donc priver l'entrepreneur de son projet, priver l'actionnaire de son investissement, priver le salarié de son emploi et porter atteinte au dynamisme économique de la Nation.
Sous cet angle, la sécurité du système d'information d'une entreprise fait partie de sa responsabilité citoyenne et de sa responsabilité sociale.
Les entreprises créatrices des objets connectés de demain ont une part déterminante de ces responsabilités.
Il est devenu primordial de prendre en compte le risque liés à la cybersécurité lorsque l'on met sur le marché des produits dépendant pour leur fonctionnement de systèmes d'information. Compte tenu de l'ampleur que peuvent prendre aujourd'hui les conséquences des attaques informatiques, des catastrophes écologiques voire de pertes de vies humaines qu'elles peuvent déclencher, chaque fournisseur doit avoir conscience que sa responsabilité, y compris pénale, peut être engagée du fait de négligences dans la sécurité de son offre et de son système.
Les entreprises du domaine de l'informatique doivent quant à elles avoir, pour leur propre sécurité, le même haut niveau d'exigence que celui qu'elles accordent aux produits et aux services qu'elles offrent à leurs clients. Les systèmes d'information qu'elles utilisent au quotidien doivent donc être au niveau de sécurité correspondant à leur activité car une entreprise du numérique qui ne protégerait pas son propre système d'information mettrait en danger ses clients et ses partenaires.
J'en viens aux systèmes d'information eux-mêmes. Les compétences humaines permettant le développement de systèmes d'information de qualité existent, comme les méthodes pour atteindre cet objectif. Dans ce domaine, la France a plutôt une situation enviable. Par la compétence de ses ingénieurs, la rigueur des méthodes de développement appliquées chez ses éditeurs, la France est capable de produire des logiciels et des systèmes robustes, documentés et certifiables. Il est essentiel de préserver cette capacité. Il est tout aussi essentiel de continuer à progresser dans le domaine de la sécurité pour la placer à un niveau adapté à la sophistication de la menace.

Cette exigence est évidemment décuplée pour les entreprises du domaine spécifique de la cybersécurité.
L'autonomie et la sécurité de la France dépendent en effet de sa capacité à disposer d'entreprises de confiance capables de lui fournir les systèmes d'information et les outils de sécurité dont elle a besoin.
J'ai la conviction que l'ensemble des entreprises qui soutiennent le FIC et qui sont ici présentes développent et utilisent des systèmes d'information sécurisés et proposent des produits et services de qualité. Certaines de ces entreprises soutiennent par ailleurs la réflexion et la recherche dans de multiples domaines. C'est un point qu'il faut souligner et une démarche qu'il faut saluer.
Notre sécurité passe par des fournisseurs de qualité et des acheteurs raisonnables qui s'adressent en priorité à ces fournisseurs.
Le rôle de l'État, c'est de veiller à la qualité de ce qui est produit : par des labels, par de l'assistance, par le soutien à la recherche et au développement, par une incitation amicale lorsque l'on constate que le compte n'y est pas en matière de sécurité…
Mais c'est aussi le rôle de l'État d'inciter les entreprises à recourir à des solutions de qualité : par l'éducation, la sensibilisation, la publication de recommandations et parfois par la régulation comme le prévoit la loi de programmation militaire. C'est tout le rôle de l'ANSSI que de piloter ces actions.

Quel rôle enfin peuvent jouer les collectivités territoriales ?
Les collectivités territoriales peuvent avoir un rôle capital dans l'augmentation du niveau général de la sécurité informatique de notre pays, de sa résilience, sous réserve qu'elles soient conscientes de l'enjeu et qu'elles prennent les bonnes décisions.
Le premier levier d'action des collectivités territoriales correspond à leurs propres exigences en matière de cybersécurité.
Quelques exemples pour préciser ma pensée :
s'il est mal sécurisé, le site internet d'une petite commune, comme celui d'un particulier, peut servir de relais à une attaque informatique ou participer à l'hébergement de fichiers piratés ;
une attaque informatique contre une installation d'épuration d'eau pourrait entraîner une intoxication des populations si l'attaquant décidait de modifier certains paramètres ;
dans un autre champ de compétence, les collectivités locales sont aussi des donneurs d'ordres et peuvent donner l'exemple elles aussi en ayant recours à des prestataires et des fournisseurs de confiance ;
enfin, ajouter systématiquement une clause concernant la sécurité des systèmes d'information dans les marchés publics que la collectivité passe peut, en quelques années, transmettre cette préoccupation à tout un tissu économique.
Un autre levier à disposition des collectivités est l'action en matière de développement économique. Si demain, l'ensemble des gui-

chets chargés du développement économique, ouverts aux entreprises, participent à l'effort national de sensibilisation au risque informatique, nous assisterons mécaniquement à une élévation du niveau général de la sécurité des systèmes d'information des entreprises. Des guides compréhensibles, des recommandations concrètes sont proposés sur le site de l'ANSSI et sont directement utilisables. J'ai également demandé à l'ANSSI de se tenir prête à soutenir toute action en ce sens.
Beaucoup d'autres leviers d'action sont à la disposition des collectivités territoriales et pourraient être utilisés à des fins de sensibilisation : la communication vers le grand public, les projets des établissements scolaires ou la formation professionnelle…

Pour conclure, je voudrais tenter de montrer la cohérence entre les rôles des différents acteurs que je viens d'évoquer.
Car chacun de nous, particulier, citoyen, industriel, agent de l'État, responsable local, porte une responsabilité dans le niveau global de sécurité de nos infrastructures.
En tant que client d'abord, capable de discernement entre la technologie éprouvée, labellisée, et le gadget qui ouvre plus de surface d'attaque qu'il n'apporte de fonctionnalités,
En tant qu'utilisateur responsable, qui respecte les règles qui s'imposent,
En tant que prescripteur, qui conduit une étude de risque argumentée et émet des exigences de sécurité,
En tant que fournisseur dans le domaine du numérique, qui comprend que la sécurité est porteuse de valeur et que le marché ne restera pas sourd à la sécurité.
Depuis trois ans, nous avons eu la démonstration de la réalité de la menace informatique sur des infrastructures critiques. Depuis le mois de juin dernier, les techniques de renseignement dévoilées dans les documents de la collection Snowden donnent un aperçu de la puissance du glaive dans le monde numérique. Le terrain est mûr aujourd'hui pour faire éclore un écosystème de la sécurité, reposant sur des prescripteurs avisés, des fournisseurs compétents et des citoyens responsables.
Cette société numérique plus sûre sera le fruit d'une démarche commune entre le public et le privé, dont l'un des éléments est le comité de la filière de cybersécurité installé récemment par le Premier ministre et qui réunit les différents acteurs du domaine.
Je vous propose de nous quitter sur cet objectif commun et qui ouvre le débat de la prochaine session du forum, consacré au dialogue public-privé.

Je vous remercie.

P1 – La cybersécurité est-elle un échec ?

Participants

Modérateur : Michel PICOT, Journaliste, BFM Business

Patrick PAILLOUX, Directeur Général de l'ANSSI.
Jean-Michel OROZCO, Chef executive office, CASSIDIAN.
Bernard BARBIER, Sogeti.
David LACEY, Consultant and Strategicadviser, IOActive
Jérémie ZIMMERMAN, la Quadrature du net
Marc WATIN-AUGOUARD, Fondateur du FIC

Clip d'ouverture :

Notre identité n'est plus ce qu'elle était, elle n'est plus simplement la garantie régalienne de notre unicité au moyen de titres sécurisés. Les technologies numériques bouleversent en effet les rapports entre les personnes physiques ou morales et leur identité. L'identité numérique est aujourd'hui un faisceau de traces relatives à un individu, une entreprise, une administration : traces techniques, traces liées à la navigation, au comportement sur la toile, aux contenus édités, aux objets possédés ou utilisés. Notre identité est désormais multiple. Elle peut être ciblée, profilée, exploitée, manipulée, usurpée. Elle est en outre dispersée dans le Cloud. La confiance, notre confiance, est donc mise à dure épreuve. Or, le cyberespace ne sera pas un vecteur de croissance sans confiance et la confiance exige une identité numérique veillée et maîtrisée, protégée, authentifiée. Cela implique des arbitrages difficiles et exige des investissements.

Notre souveraineté et notre croissance économique sont en jeu. Les services liés à la confiance de l'identité numérique représenteront 8 % du PNB européen en 2020. Jamais sécurité et développement économique n'ont été aussi liés.

Michel PICOT

6e FIC avec une question centrale qui va nous intéresser ce matin : « La cybersécurité est-elle un échec ? Permettez-moi tout d'abord de me présenter, je suis Michel Picot, journaliste à BFM Business. Ce poste

de journaliste est un poste d'observation très intéressant qui m'a permis de voir effectivement ces dernières semaines que l'actualité était riche et de poser ainsi la question : la cybersécurité est-elle un échec ?

Je pense notamment à la chaîne de magasin américaine Target. En décembre dernier, ce groupe a annoncé effectivement être victime d'un piratage extrêmement important. En effet, 40 millions de numéros de cartes bancaires ainsi que leur date d'expiration et les cryptogrammes au dos sont partis dans la nature, ainsi que les 70 millions de noms, d'adresses mails et d'adresses postales qui ont été dérobées.

Il y a une autre étude que j'ai trouvée intéressante, celle d'H-line qui a été publiée jeudi dernier. Cette étude indique que 70% des City-commerces se montreraient imprudents en autorisant par exemple leurs clients à avoir des mots de passe aussi basiques que 123456. Il faut savoir qu'en 2013 le mot de passe le plus utilisé par les Français était 123456 et certains ont ajouté le chiffre 7 derrière pensant être mieux protégé.

Je me pose la question parce que les technologies sont là, vous avez pu le voir peut-être très rapidement au niveau des stands et vous aurez l'occasion de le découvrir. Ces technologies extrêmement efficaces amènent finalement la question : l'utilisateur a-t-il pris conscience qu'il avait une identité ou des identités numériques, qu'il devrait prendre un peu plus attention à ces dernières et regarder ce qu'il s'y passe.

Alors, la cybersécurité est-elle un échec ? Pour en parler j'ai le plaisir d'accueillir le Général Marc WATIN-AUGOUARD, Patrick PAILLOUX, Directeur Général de l'ANSSI, Jean-Michel OROZCO, le Président de CASSIDIAN, Bernard BARBIER, conseiller spécial pour la cybersécurité et la cyberdéfense chez Sogeti, David LAYCE futurologue et consultant en sécurité et Jérémie ZIMMERMANN de la Quadrature du Net. Vous avez pu constater que nous avons procédé à un petit sondage juste avant le début de cette plénière. La question était : pensez-vous que la cybersécurité est un échec ? Si vous souhaitez voter pendant cette conférence, un petit badge a été remis à chacun. Ce dernier a un QR Code et vous pouvez le flasher et ensuite intervenir. Vous avez également la possibilité de réagir en envoyant vos Tweets et n'oubliez pas les H tags, les H tags P1 et FIC 2014, cela nous permettra effectivement de prendre votre température tout au long de cette matinée.

Alors la Cybersécurité est-elle un échec ? Lorsqu'on parle d'échec en cybersécurité, on sous-entend plus ou moins un domaine extrêmement complexe qui évolue en permanence, est-ce qu'on peut réellement parler d'échec ?

Général Marc WATIN-AUGOUARD

Je ne vais pas vous faire un cours de philosophie. L'échec est toujours relatif, c'est par rapport à un standard, un temps, un objectif que l'on s'est fixé. Mais nous sommes 3100 / 3200. Cela fait 10 ans que le FIC existe, vit-on un échec ?

Nous venons de parler de construction de l'avenir qui s'inscrit dans une configuration globalement positive. Les Chinois nous disent bien que l'échec est la mère du succès et finalement les personnes qui ont lancé l'aéronautique se sont-elles arrêtées parce qu'il y a eu des échecs au début ? Aujourd'hui les avions volent avec une grande sécurité alors qu'au commencement ils ont connu l'échec.

L'échec peut être salvateur et constituer un électrochoc. Alors je crois que pour la cybersécurité, l'échec est la mère de tous les succès. Les difficultés successives rencontrées, les attaques qu'on a pu voir se développer et susciter la création de la cybersécurité sont la fille de l'échec. Ne soyons pas naïfs, nous aurons des échecs, toujours des échecs, encore des échecs, mais à chaque fois nous devrons surmonter l'échec pour créer une cybersécurité qui soit fiable.

Deuxième élément que je voulais évoquer, la cybersécurité doit tenir en échec deux pôles extrêmes :

Le premier, c'est le pôle libertaire : aucune régulation, tout ira bien, ce sera la loi du plus fort, le « Faustrecht ». Nous n'en voulons pas.

Deuxième tentation, c'est la cybersécurité absolue. On sait très bien aujourd'hui que ces atteintes à la cybersécurité sont porteuses de risques politiques, économiques et sociaux. En conséquence, il faut que nous créions les conditions du non-échec par une action unitaire. Nous n'assurerons la cybersécurité si nous ne le faisons pas ensemble. Nous devons faire une analyse systémique et conjuguer tous nos talents car personne n'a la clé de la réponse à la question.

Nous devons investir dans la formation, la recherche et le développement. Nous devons aussi regarder l'avenir car finalement nous bâtissons quoi ? Soit une tour de Babel, soit une cathédrale, mais personne n'a fait les plans. L'avenir, c'est l'anticipation et nous devons savoir ce qui se passera dans 15/20 ans. Personne n'a la réponse, mais tout le monde a la réponse collective. Construire les plans du futur d'un cyberespace qui sera de plus en plus en nous, autour de nous, avec nous, c'est à cette condition-là que nous pourrons maîtriser cette cybersécurité qui ne sera qu'un ordre public d'équilibre entre les contraintes et les libertés. Nous devons préserver les libertés et aussi construire cette unité et c'est l'objectif du FIC depuis son origine.

Qu'on soit civil, militaire, policier, ou gendarme; qu'on soit Français ou étranger, civil, administrateur ou industriel, quelle que soit notre fonction, nos responsabilités, nous avons tous quelque chose à apporter. Je suis sûr que le sondage va s'inverser et vous verrez que la cybersécurité sortira renforcée de notre discours. Parce que nous aurons un discours qui ne sera pas de nous plaindre, de pleurer. Simplement un discours où nous disons : attention si nous ne faisons pas ensemble le parcours, alors oui ce sera non seulement l'échec de la cybersécurité mais ce sera l'échec de notre société.

Michel PICOT

Merci Mon Général, c'était pour l'introduction, cela va être difficile après pour vous car je vais poser à peu près la même question. J'espère que le sondage va s'inverser, pour l'instant cela n'a pas l'air de le faire, mais c'était effectivement ce que je voulais, mon Général, c'est que vous plantiez le décor et qu'on parle des fondamentaux.

On va faire un tour de table rapide pour parler de votre actualité et de cette question centrale : la cybersécurité est-elle un échec ? Et ensuite au-delà du constat, je souhaite que nous partions avec des débuts de réflexion, voire des pistes, des solutions. Ensuite, il y a les 40 ateliers qui permettront d'aller beaucoup plus loin bien entendu.

Patrick Pailloux, merci d'être avec nous, d'abord peut-être un petit mot sur l'actualité de l'ANSSI ?

Patrick PAILLOUX

Pour revenir sur le discours du Général, j'aurais envie de dire au lieu de poser la question « La cybersécurité est-elle un échec ? » j'aurais tendance à dire par rapport à ce que l'on voit, bienvenue dans le monde réel et c'est plutôt ça la réalité.

Vous savez que l'ANSSI aime la comparaison avec le monde médical. C'est un peu comme si on avait posé la question à l'équipe de Louis Pasteur à la fin du XIXe siècle : « la médecine est-elle un échec ? » Mais non la médecine n'était pas un échec à la fin du XIXe siècle, pour autant au XXIe siècle on continue à progresser, à faire des cœurs artificiels, *etc.* On est exactement dans la même situation.

Le gouvernement français a déjà intégré depuis quelques années cette dimension. Il fait évoluer petit à petit son dispositif en le faisant croître. C'est vrai pour l'ANSSI avec ses fonctions de cybersécurité et d'autorité de Défense. Mais c'est vrai pour l'ensemble du dispositif gouvernemental, du ministère de l'Intérieur, on a parlé de la gendarmerie. Il y aura le ministère de la Défense tout à l'heure qui en parlera. Pour ce qui est de l'adaptation, on vient de modifier légèrement notre organisation ou plus précisément mettre en cohérence nos pratiques avec la réalité de ce qu'on affiche. On vient de renommer de CERT gouvernemental, le CERTA, en CERT-FR, pour deux raisons :

- d'abord, on a intégré, comme c'est aujourd'hui le cas dans notre centre opérationnel, l'ensemble des fonctions, pas seulement la fonction détection / notification d'alerte, mais aussi détection d'incident, la surveillance H24, les audits, la reconstruction sur les attaques informatiques, etc.
- ensuite, il s'agit de donner de la visibilité en international, puisque CERTA ce n'était pas très lisible. CERT-FR permet de mieux comprendre concrètement quelles sont les fonctions. Tout le monde s'adapte en permanence.

Michel PICOT

Pour vous, ce n'est pas un échec. Jean-michel Orozco, pour vous, ce n'est pas un échec ? pour avancer c'est l'innovation permanente, c'est le cœur de votre défi si j'ose dire ?

Jean-Michel OROZCO

Oui tout à fait, je crois que pour nous la cybersécurité c'est avant tout un défi. Un défi que l'on doit relever tous ensemble, ici présents et au-delà des gens qui sont présents dans cette salle l'ensemble des organisations

étatiques, gouvernementales et industrielles. C'est un défi que nous devons relever. Si l'on regarde les 10 ans passés, on voit bien que nos sociétés occidentales, nos sociétés d'une façon générale, ont bénéficié d'un apport de productivité en matière de facilité de vie. Cet apport est dû aux technologies du numérique. La numérisation a créé un gain de productivité colossal, que ce soit dans nos vies personnelles, industrielles ou étatiques. Si on fait un constat de tout cela, il n'y a pas de chemin en arrière, nous n'avons pas le choix. La cybersécurité, c'est un défi qu'on doit relever, un vrai challenge, une vraie opportunité également pour l'Europe, pour la France, de créer une filière industrielle dans un domaine extrêmement novateur, extrêmement pointu technologiquement. Je crois que, tous ensemble, on doit relever ce challenge.
Pour revenir sur la thématique de l'échec, je crois que l'on est au tout début d'une histoire. Pour mesurer déjà les progrès que l'on a faits dans ce contexte-là, le mieux est de regarder où nous étions deux ans avant. Quand je rencontrais un certain nombre de décideurs, je voyais des gens qui n'étaient peu ou pas au fait de la cybermenace. Maintenant, quand vous rencontrez des décideurs que ce soit étatiques ou industriels, il est relativement rare de voir des gens qui ne sont pas au fait de la situation. Cela veut dire que la prise de conscience est là et qu'elle se traduira par la mise en place de programmes budgétaires qui sont la prochaine étape.

Michel PICOT

Il va falloir apprendre à réagir vite. Pouvez-vous nous expliquer le changement de nom de CASSIDIAN ?

Jean-Michel OROZCO

Nous rejoignons, sans changer de périmètre, la division Airbus Defence and Space.

Michel PICOT

Bernard BARBIER, votre point de vue sur cette question ?

Bernard BARBIER

Personnellement j'ai décidé de quitter l'administration pour rentrer dans le domaine de la cybersécurité car c'est un sujet auquel je crois beaucoup. Ce n'est pas un échec, c'est un défi.
J'ai une carrière de scientifique. Il faut aborder ce sujet-là de façon scientifique et technique, enjeu essentiel pour notre société. Nous ne reviendrons jamais en arrière. Il y a des échecs en permanence, car les sociétés subissent des attaques informatiques réussies. J'ai passé presque 8 ans comme directeur technique de la DGSE. Je pense que c'est un véritable enjeu pour notre pays. Au début de ma carrière professionnelle, j'ai travaillé dans la dissuasion nucléaire française. Je pense qu'on est au même niveau. Pour un pays comme la France, c'est un enjeu d'indépendance nationale. La France doit créer sa propre industrie technologique, ses entreprises. Pas uniquement la France, mais aussi l'Europe. Le discours récent d'OBAMA est très clair, les Américains n'arrêteront pas. La France sera toujours face à des enjeux techniques et d'indépendance énormes et je pense que c'est essentiel. J'ai franchi le pas en choisissant la société SOGETI; c'est un enjeu technique et même personnel. Je n'ai pas choisi un domaine qui serait un échec sinon je serais allé dans un autre domaine.

Michel PICOT
Je vais donner maintenant la parole à David LACEY qui est prospectiviste et futurologue, consultant en sécurité informatique. Pour vous la cybersécurité est-elle un échec ?

David LACEY
Oui, la cybersécurité est un échec à tous les niveaux, tant sur le plan réglementaire, les méthodes, les compétences, que sur les normes, la direction et la technologie.
Le problème sous-jacent est que les directeurs des systèmes de sécurité d'information ne mettent pas en œuvre une réelle sécurité. Ils se mettent en conformité avec les normes. La norme est indispensable, car les directeurs d'affaires n'accepteront pas de bon gré le prix de la sécurité et les contraintes qui les lient. Mais la norme n'est pas la meilleure approche. La norme incite au moins cher et à la réponse la plus simple. Elle favorise la bureaucratie au détriment de la technique d'excellence et des idées prodigieuses. Les réglements n'incitent pas à l'innovation, ils reconnaissent les vieilles méthodes enracinées. Certaines d'entre elles ont été élaborées il y a déjà plus de 20 ans. Aujourd'hui, les directions de systèmes de sécurité sont dépassées. Elles s'appuient sur un modèle de gestion d'âge industriel, élaboré par Deming : planifier, développer, contrôler, ajuster. Ceci prend trop de temps pour identifier de manière convenable les points faibles. L'attaquant a donc l'avantage, car il peut changer son attaque à l'instant même, mais le défenseur, lui, aura à développer une analyse de rentabilisation, obtenir un budget et aller au travers d'un processus de passation de marché avant de pouvoir mettre en œuvre une solution technique. Nous devrions remplacer la roue de Deming par son équivalent militaire connu sous le cycle de Boyd ou OODA (observe, orient, decide and act) observer, s'orienter, décider et agir. Ce principe est utilisé par les pilotes de combat et les forces spéciales. Il met l'accent sur le temps de réaction et de la vitesse. Le résultat de toutes ces exigences est : nouvelles compétences, nouvelles attitudes et nouvelles technologies. Il nécessite d'importants changements de réglementation, des instituts, des organismes de normalisation mais aussi de formation. Mais ces organisations sont très lentes à changer. Rien à mon point de vue ne changera à moins qu'il y ait un incident majeur, type "11 septembre", alors je pourrais être au côté d'une entreprise voire même d'une grande entreprise ou dans la société et il y aurait alors une grosse réaction.

Michel PICOT
Je pense qu'il y aura de la réaction. Jérémie Zimmermann de la Quadrature du Net, quel est votre avis ?

Jérémie ZIMMERMAN
Je pense jusqu'à présent que la cybersécurité est un échec. On s'est engagé dans la mauvaise direction en oubliant de mettre le citoyen au cœur de la cybersécurité. Nous voyons aujourd'hui que la confiance est rompue. Edouard Snowden, au courage incroyable, a peut-être plus fait pour la cybersécurité que tous autant que nous sommes ici dans cette salle. Ses révélations montrent que ces entreprises auxquelles la majorité des gens font confiance ne méritent plus notre confiance. Je vais me livrer à un rapide sondage dans cette salle.
S'il vous plaît, levez la main et gardez-la levée si vous utilisez un ou plusieurs produits ou services des compagnies suivantes : Apple,

Facebook, Microsoft, Google. Voyez environ qu'il y a près de 100 % de la salle ici qui a levé la main, alors qu'on sait aujourd'hui que la confiance avec ces entreprises est rompue. On a laissé les clés de la maison à quelqu'un qui avait l'air très sympathique, très souriant, et aujourd'hui non seulement il tape dans le frigo, il couche avec le conjoint ou la conjointe mais en plus il a changé les serrures. Nous nous sommes fait exproprier de nos données et de nos communications. Exproprier aussi de la technologie par des boîtes noires et des puces qui sont des boîtes noires à l'intérieur de nos téléphones : les puces baseband, des systèmes d'information fermés aux architectures centralisées. Or, les pouvoirs publics n'ont eu qu'une idée en tête, une doctrine : la cyberguerre. On a investi massivement dans des capacités de surveillance et offensives. La commande publique a acheté tous les joujoux des partenaires Platinium et Gold du FIC, des Eagle de MI6, Bull et des choses comme ça, mais jamais on n'a pensé à mettre le citoyen dans l'équation. Il est grand temps, au lieu de cette doctrine guerrière, au lieu de la cyberguerre, de construire la cyberpaix avec les citoyens et de promouvoir non pas les technologies du contrôle des individus et de leurs communications mais les technologies qui libèrent et rendent plus libres.

Michel PICOT

Merci beaucoup pour cette franchise, vous voyez que nous sommes directs et transparents. J'imagine que dans ce qui a été dit vous avez une réaction. Mon Général une réaction ?

Général Marc WATIN-AUGOUARD

Je voulais répondre à M. Zimmermann : il a à juste titre placé le citoyen au cœur de la cybersécurité. Dans ce domaine, nous avons un grand travail d'information à faire pour que les gens aient confiance, de reconstruction d'un certain nombre de paramètres que vous avez évoqués.

S'agissant de la cyberguerre, vous savez que tout espace conquis par l'homme, (dans ce cas de figure il se trouve que le cyberespace n'est pas conquis mais créé par l'homme) voit arriver à un moment donné les prédateurs : l'espace terrestre, maritime, aérien ont vu arriver les prédateurs. À un moment donné, agissent les criminels, les terroristes et les guerriers. Entre nous aujourd'hui quand on parle de cyberguerre, il n'y a plus d'actions de guerre sans actions cyber.

Peut-on reprocher à l'État de prendre un certain nombre de mesures, je ne le crois pas. Je fais un sondage :

Qui parmi vous est terroriste, membre d'une organisation criminelle, a reconstitué une ligue dissoute, porte atteinte massivement au potentiel scientifique et économique de la France ?

Personne, donc vous n'avez rien à craindre du dispositif de la loi de programmation militaire.

En revanche, qui a déjà eu sur internet des spams, des publicités montrant qu'il était profilé ? Tous ! ne me dites pas le contraire. Finalement, quand on parle de cyberguerre, ce n'est pas forcément ceux que l'on vise qui sont les plus coupables. Et vous avez raison d'indiquer que le citoyen a perdu confiance mais pas parce que c'était l'État,

il a perdu confiance car il y avait d'autres opérateurs qui n'ont pas joué le jeu.

Michel PICOT

J'ai évoqué dans cette introduction que cet être humain finalement n'utilise pas ces outils à sa disposition. Il a presque perdu l'idée qu'on a une identité numérique ne serait-ce que lorsqu'on fait un achat. On a beau essayer de mettre l'humain au centre, si celui-ci ne fait rien, on n'avance pas plus. Les risques sont là, le fait que l'être humain soit de plus en plus connecté ouvre la porte de plus en plus à des cyberattaques.

Jérémie ZIMMERMAN

Déjà, il y a une différence entre défendre les infrastructures sensibles contre des attaques et la militarisation d'Internet pour laquelle c'est Internet tout entier qui va devenir un champ de bataille. Il sera soumis non plus au droit commun mais à un régime d'exception qui est celui du droit de la guerre. C'est dans cet endroit-là de la doctrine que je vois déjà un problème.
Ensuite, pour ce qui concerne les cibles de la loi de programmation militaire, je suis sûr que des gens qui n'ont pas levé la main en font peut-être partie ou sont soupçonnées d'en faire partie.
La surveillance de masse des Américains, est à trois niveaux de liens. Exemple : je suis ami avec Julian Assange. Vos GSM sont ici allumés dans le même périmètre que le mien pendant un certain temps, vous êtes dans la base de données. Ce sont des liens très subtils qui sont exploités quand on parle de surveillance de masse. Il faut faire une différence entre la surveillance ciblée, qui est légitime quand il y a un rétrocontrôle démocratique, et la surveillance de masse. Pour répondre à votre question, nous n'arrivons plus à faire la différence entre la surveillance privée et la surveillance publique. Lorsqu'il s'agit des programmes « PRISM» et autres programmes de surveillance de masse, je ne suis pas sûr que l'on puisse faire avancer la sécurité autrement qu'avec une alliance entre le privé et le public.
Quand on parle de cyberpaix, ce sont des technologies qui libèrent plutôt qu'elles contrôlent. Ce sont des technologies qui sont sur la table depuis 10, 20, 30 ans. Il s'agit des logiciels libres, des architectures décentralisées, du chiffrement point à point. Tant qu'on va aller acheter des « joujoux » à Thales ou Bull au lieu d'investir dans les cerveaux de nos universités, dans nos centres de recherche aux quatre coins de la France pour favoriser l'émergence de ces solutions à mettre aux mains des citoyens, je ne vois pas ce qu'on peut dire d'autres aux citoyens qu'aller acheter tel ou tel « joujou » , aller participer à tel ou tel service centralisé. Il faut inventer ces solutions-là et l'État a un rôle à jouer là-dedans.

Michel PICOT

Une réaction à ce qui a été dit éventuellement Messieurs ?
J'aimerais qu'on aborde effectivement le contexte dans lequel on est. David LACEY disait quelque chose de très intéressant : Le hacker a un avantage par rapport à la victime puisqu'il peut s'adapter en permanence. La victime est obligée de prendre du temps,

de définir un budget, peut-être de lancer un appel d'offres, mettre en place une solution, ce qui est quand même assez fou. On ne parlait pas de militarisation, mais de fonctionnement militaire pour aller plus vite, est-ce que cela vous inspire quelque chose ?

Jean-Michel OROZCO
Vis-à-vis de l'intervention de David LACEY, je voudrais revenir sur le point que vous évoquiez qui est effectivement la rapidité, la vitesse de réaction. Ceci est fondamental, car la cybersécurité, nous pouvons la caractériser comme la cyberdéfense par rapport à la cyberattaque. Si nous voulons être efficaces en termes de cyberdéfense, sachant qu'on a affaire à une guerre de mouvement, économique qui pourrait devenir une guerre plus traditionnelle. À l'heure actuelle, c'est une guerre essentiellement économique associée à des opérations d'espionnage. Si vous voulez être efficace par rapport à un enjeu de cette sorte, il faut être rapide et innovant. Je voudrais revenir sur un point : la cybersécurité ne sera pas un échec si nous arrivons à fédérer l'ensemble des énergies innovantes dans ce pays, au-delà de notre pays et en Europe également.

Je crois que l'innovation est une des clés du succès de la cybersécurité. C'est en fédérant ce qui se fait dans les grands groupes, dans les start-up, les PME, qu'on arrivera tous ensemble à offrir des solutions suffisamment rapides et étoffées pour combattre un ennemi qui aura toujours effectivement l'effet de surprise pour lui et l'avantage de cet effet de surprise. La rapidité de la réaction et la capacité d'anticipation sur un type d'attaque seront pour moi fondamentales dans les clés du futur succès de la cybersécurité. Toutes les technologies de type Big Data seront très utiles dans ce domaine-là. Il faut être capable dans le futur, de détecter les signaux faibles et d'anticiper le type d'attaque en cours sur les réseaux.

Michel PICOT
Cela veut dire, et il faut le rappeler que, le chef d'entreprise peut être tenu personnellement responsable en cas d'attaque d'une entreprise mais aussi le maire d'une commune. Quand on sait le temps de prise de décision dans une collectivité ou même une grosse entreprise, il faut peut-être changer.

Jean-Michel OROZCO
David a évoqué la mise en place un peu lourde des mécanismes de « procurement », mécanismes qui ne sont pas adaptés.
Par contre, il y a des solutions pour s'affranchir de tout cela. La cybersécurité, c'est un enjeu que les, organisations étatiques, gouvernementales, industrielles ne peuvent pas traiter par elles-mêmes. Des sociétés comme la mienne vont être spécialisées en cyberdéfense. Ces sociétés seront là comme prestataires de services en vue de servir ces grandes organisations. Ces sociétés spécialisées sauront, pour se montrer réactives, anticiper et réagir H24 en temps réel aux types de menaces.

Michel PICOT
Cela nécessite que l'on revoie la réglementation, certaines décisions en cas de risque. Je voudrais voir avec vous, David LACEY : En 2014, je m'adresse au futurologue, est-ce qu'il y aura plus de risques de cyberattaques selon vous ? Comment vous voyez cette nouvelle année dans ce domaine ?

David LACEY
J'ai développé six contributions le mois dernier sur mon blog Computer Weekly :
- le premier constat est que la technologie échappera enfin à la monoculture qui est très dangereuse. Les nouvelles technologies qui voient le jour fourniront beaucoup plus de choix en matière de défense. Nous devons sortir de notre monoculture de la sécurité où nous utilisons tous des produits identiques, ce qui rend la tâche facile à l'attaquant. Je pense que les produits émergents seront effectivement plus fiables et capables de détecter les logiciels malveillants que les technologies actuelles.
- le deuxième constat est que nous allons effectivement avoir une nouvelle génération d'attaques informatiques. Le ver informatique Stuxnet a été développé il y a de nombreuses années. La prochaine génération d'attaques informatique sera beaucoup plus riche, plus sophistiquée et même furtive. Il y a beaucoup de mobiles d'ordres politiques, commerciaux et pénaux pour les nouvelles attaques. Nous pouvons donc nous attendre à rencontrer des attaques spectaculaires cette année si nous sommes en mesure de les détecter. Certaines d'entre elles sont probablement déjà ici et nous ne les avons tout simplement pas détectées.
- le troisième constat est qu'il y aura un retour de bâton contre les normes de sécurité. Je pense que beaucoup de responsables de la sécurité croient maintenant que la sécurité a échoué. Le problème majeur est la conformité. Les gouvernements et les régulateurs commencent à comprendre ce problème. La conformité ne va pas disparaître, elle sera de plus en plus forte. Mais il y aura une remise en cause des normes dont nous avons besoin pour la sécurité.
- le quatrième constat est que nous allons améliorer notre réponse à la crise. La gestion des crises est une grande faiblesse dans toutes les compagnies, en particulier au niveau stratégique. Il s'agit de protéger les actifs intellectuels, des choses telles que «l image de marque », la responsabilité juridique, la fidélisation de la clientèle, l'habilitation du personnel et l'influence politique. Celles-ci sont très faciles à perdre. Mais le développement des principaux incidents a permis de sensibiliser de nombreuses organisations qui sont en mesure maintenant de planifier une meilleure gestion de crise. Je pense qu'il y aura une grande amélioration cette année.
- le cinquième constat est que le déficit de compétences informatiques va continuer à croître. Il y a une grave pénurie car les très bonnes compétences dont vous avez besoin correspondent à un type particulier de personne. Des cours de formation ne résoudront pas ces problèmes, nombre d'entre eux sont des méthodes d'enseignement de

sécurité obsolètes. Les gens aux compétences particulières ne peuvent pas être «fabriqués», ils doivent être recherchés et il n'y a pas plus difficile comme défi.
Mon constat final est qu'il n'y aura pas de changement à la NSA, la baisse des opérations de veille va se poursuivre comme à la normale. L'espionnage va continuer dans le droit fil des révélations de Snowden. Je pense que le vrai problème est l'absence d'une surveillance visible et une mauvaise présentation de la politique. La réalité est que nous avons besoin de recueillir de très grandes quantités de renseignement pour prévenir les incidents terroristes. La menace n'a pas diminué et ne diminuera pas.

Michel PICOT

En termes de réglementation et de mise à la norme, y a-t-il une prise de conscience aujourd'hui qu'il faut peut-être améliorer, aller plus loin, redéfinir certains champs d'action ?

Patrick PAILLOUX

Oui, si je reviens sur ce qu'a dit David, il y a un point sur lequel on est vraiment 100% d'accord, c'est sur ces questions de « compliance ». On a trop longtemps utilisé cette notion de conformité comme une idée.
On coche des cases dans un questionnaire pour être en conformité avec la réglementation de sécurité. Nous avons dépassé ce stade-là.
Aujourd'hui la sécurité est d'abord une question technique. J'envoie une équipe d'auditeurs, de pen-testers, pour voir s'ils réussissent à pénétrer ou pas dans un système informatique. L'expérience montre que la plupart des entreprises victimes d'espionnage étaient certifiées ISO 27000 et conformes à la réglementation.
Aujourd'hui, si on regarde la menace concrète, il s'agit de s'occuper d'abord de sécurité nationale. Quel est le risque majeur qui vise les Nations ? La France comme n'importe quelle Nation est interconnectée. Nous avons évidemment un risque de sabotage contre nos infrastructures critiques, l'exemple de stuxnet a été évoqué.
Ce risque de sabotage existe et ce n'est pas devant cette assemblée que je vais expliquer pourquoi et comment. C'est une des priorités majeures de tous les gouvernements. Je pense que la France a pour le coup pris une avance avec le vote de la loi de programmation militaire qui nous permet de disposer d'un minimum de réglementation pour savoir si oui ou non nos infrastructures sont critiques, c'est-à-dire ce qui fait que notre Nation survivra ou pas, qu'il y aura des morts ou pas, s'il y a une attaque informatique.
Est-ce que notre Nation est suffisamment préparée ? La LPM a été votée, la France est un des premiers pays du monde à disposer d'une capacité à savoir quel est le niveau de sécurité de ses infrastructures critiques, donc les commandes de contrôle des dispositifs véritablement critiques. Je ne parle pas des intranets, des messageries. Là je suis sur les commandes industrielles, les barrages, centrales, les systèmes d'aiguillages, les contrôles aériens, les hôpitaux, *etc.* sur une régulation qui nous permet de savoir quel est le niveau de sécurité et d'im-

poser un certain nombre de normes qui sont très techniques.
Premier étage de la fusée : Le vote de la LPM.
Le second étage de la fusée : un premier guide référentiel qui va nous permettre avec les industriels et ministères concernés, d'identifier dans leur système d'information ce qui relève du critique. Nous manquons de visibilité de ces systèmes critiques, les industriels aussi. Nous travaillons actuellement avec eux sur ce sujet.
Quels types de mesure doivent prendre ces opérateurs ? C'est le travail de déclinaison de la loi de programmation militaire. Vous trouverez sur notre site Internet une aide à l'identification des systèmes critiques. Ce n'est pas absolu : nous appliquons, regardons et ensuite adaptons en fonction de cette analyse. Ensuite, il y a une série de mesures que nous estimons être en général applicables pour des systèmes de commande contrôle quand ils sont très industriels. Comme je le disais, tout ceci doit être adapté, secteur par secteur, entreprise par entreprise. Nous ne pouvons pas appliquer les mêmes mesures de sécurité à une banque et à une centrale nucléaire, cela n'aurait aucun sens. Nous avons donc lancé la deuxième étape de la fusée. L'année 2014 va être une année de travail avec les opérateurs pour identifier ces systèmes critiques et voir les premières règles qui doivent s'appliquer.

Michel PICOT

Je ne voudrais pas briser le moral mais, ce sera ma dernière question. On parlait des solutions, je voulais poser la question peut-être à vous deux Jean-Marie OROZCO et Bernard BARBIER. Avez-vous constaté de nouveaux types d'attaque, de nouvelles cibles ou manières de faire qui vous ont, en tant qu'industriel, fait travailler sur de l'innovation justement pour arriver à les contrer ? Y a-t-il de nouveaux phénomènes que vous avez pu constater ? ce n'est pas une question piège il y a beaucoup d'innovation en permanence du côté des hackers.

Bernard BARBIER

Les méthodes d'attaque évoluent en permanence, devenant de plus en plus sophistiquées. Les attaques passent par les points faibles. Nous avons une dissymétrie totale entre l'attaquant et le défenseur. Le défenseur doit tout défendre, l'attaquant, lui, a à trouver le point faible. C'est cela l'énorme difficulté. Dans un réseau d'entreprise à 100 000 postes de travail, est-ce qu'il n'y a pas un point faible ? Les attaquants disposent maintenant d'outils extrêmement sophistiqués.
Je pense que la vraie question, c'est le sabotage. Nous avons commencé à voir quelques sabotages d'origines étatiques ou non. Je suis persuadé que nous arriverons à des sabotages terroristes dans les mois, les années qui viennent. Je ne vais pas prendre référence sur les Américains qui sont extrêmement pessimistes. Je crois que des groupes terroristes sont en train de mettre en œuvre des technologies pour réussir des sabotages. Nous serons dans le cyberterrorisme : casser et provoquer des gros

dégâts comme lors du 11 septembre. Nous voyons là le gros problème. D'un côté, effectivement, on peut reprocher aux États de développer certaines technologies que je ne qualifierai pas de militarisées; il n'y a rien de militaire là-dedans même si on appelle cela la cyberguerre. La question est : quel équilibre doit-on réaliser vis-à-vis de la protection contre le terrorisme, ce qui revient à dire que met en place l'État ? Si je devais revenir sur le cas Snowden, selon moi il a trahi son pays.

Patrick PAILLOUX

C'est votre point de vue, je n'apporte pas de commentaire là-dessus. Prenez la parole, après nous abordons le volet solution.

Bernard BARBIER

Pour faire la transition, je ne suis pas d'accord avec Jérémie Zimmerman dans ce qu'il dit sur la façon de se défendre. En effet, je suis sur la position du défenseur, c'est mon métier et celui de mes équipes et du laboratoire. Nous sommes censés développer et concevoir des systèmes qui vont résister aux attaques. Problème, la différence entre l'attaquant et le défenseur. L'attaquant, il lui suffit, c'est bien connu par les gendarmes dans le monde réel, de chercher la vulnérabilité d'un système pour pouvoir y rentrer. De son côté, le défenseur ne sait pas exactement l'évolution quotidienne de la menace. Quand vous concevez un système, c'est un point de vue théorique sur un ensemble de types d'attaque que vous pouvez avoir et pas seulement sur les attaques d'aujourd'hui. C'est extraordinairement complexe, ce n'est pas uniquement en mettant un logiciel libre ou crypté qu'on arrivera à se protéger des attaques informatiques. Si c'était aussi simple que cela, on ne mettrait pas autant de moyens et d'argent à l'ANSSI pour se doter de produits de très haute sécurité. Dieu merci, nous avons en France des entreprises très compétentes dans le domaine de la cybersécurité, capables de nous faire des téléphones et des chiffreurs qui résistent aux attaques car conçus d'une manière scientifique. Cependant, ce n'est pas une ergonomie formidable pouvant être installée sur un PC quelconque.

Jean-Michel OROZCO

Juste un petit commentaire complémentaire. Effectivement dans ce contexte-là, l'avantage est à l'attaquant et l'effet de surprise est pour lui. Si nous voulons bâtir et concevoir une défense efficace, je reviens sur une thématique qui m'est chère, c'est la vitesse de réaction qui compte. Vous ne pourrez pas dans certains cas éviter de subir une attaque et éventuellement une intrusion dans vos systèmes. Ce qui est extrêmement important, c'est de détecter cette attaque dans des délais relativement court et de neutraliser celle-ci dans un délai extrêmement court. Je crois qu'il faut être prêt à ne pas être surpris. Nous arriverons à être efficaces par une réelle défense dans la profondeur.

Michel PICOT

Un twitos intéressant sur la conformité : je me mets à la place d'un directeur des systèmes d'information d'une entreprise qui doit dire à son président qu'il n'est pas protégé. Comment sensibiliser son dirigeant ?

Jean-Michel OROSCO

Il faut parler d'argent. Pour un dirigeant ce qui compte à un moment donné, c'est l'espèce sonnante et trébuchante. La menace

pour un dirigeant d'entreprise c'est combien cela va lui coûter si jamais cela arrive. C'est extrêmement important d'être capable de modéliser pour faire prendre conscience à un dirigeant quelle est réellement son exposition au risque. Dans ce contexte-là, nous avons conclu une alliance avec Axa Matrix Risk Consultants SA pour offrir aux dirigeants d'entreprise une offre globale, faisant à la fois une analyse technique des risques associés et la traduction de ces risques techniques en risques « profit and loss » dans la société. Cela est démonstratif pour un « B.O.M member » (Board of management) ou un dirigeant de société.

Général Marc WATIN-AUGOUARD

La cybersécurité, c'est l'alliance de la lutte contre la cybercriminalité et la cyberdéfense. Nous parlons beaucoup de cyberdéfense, n'oublions pas non plus la cybercriminalité. C'est un enjeu essentiel. Nous allons avoir un glissement du matériel vers l'immatériel. Si nous parlons des entreprises, des secteurs critiques, il faut aussi parler des personnes. Une attaque d'une entreprise est une infraction. Nous avons une cybersécurité versus cyberdéfense très portée par la loi de programmation militaire, très portée sur le Livre Blanc. Il faut impérativement que le pôle cybercriminalité lui aussi émerge. Nous ne pouvons pas faire l'un sans l'autre dans une certaine mesure. La judiciarisation de la lutte contre les atteintes à la sécurité dans le cybersespace est essentielle pour la protection du citoyen. Aujourd'hui, le prédateur n'a jamais été aussi proche de la victime et jamais la victime n'a été aussi loin de son juge. Je crois que c'est quelque chose de très important qu'il faut noter.

En termes de prospective, l'objet sera de plus en plus protégé par l'Internet des objets. Dans 15/20 ans il n'y aura plus de vols, un produit ne sera plus contrefait car traçable. Demain, les personnes seront attaquées dans leur identité, leur intimité ou leur réputation, mais aussi à travers des flux financiers. Cette notion de glissement du matériel vers l'immatériel doit être aussi prise en compte. C'est une des composantes de la cybersécurité à côté des atteintes aux entreprises. Je dis le pour montrer que la militarisation du cyberespace n'intervient que très très loin dans le schéma. Tant qu'un conflit armé n'est pas déclaré, toute attaque d'une entreprise est une infraction prévue et réprimée par la loi Godfrain, mais aussi prévue par la directive du 12 août 2013 de l'Union Européenne.

Michel PICOT

Jérémie Zimmerman vous évoquiez tout à l'heure l'identité de l'être humain qui sera la prochaine victime. Un Tweet qui vient de passer pose la question suivante : si Google était français, serions-nous mieux protégés ?

Jérémie ZIMMERMAN

Heureusement que je n'ai pas dit que la cybersécurité était aussi simple qu'installer un logiciel libre sinon Patrick Pailloux aurait été en désaccord avec moi.

Non ce n'est pas aussi simple que cela. Si nous regardons à la fois les vecteurs d'attaque ciblés de la NSA dans le catalogue publié par Der Spiegel et les moyens qui sont ceux de la surveillance de masse, nous voyons que les technologies les plus communément utilisées ont été sabotées. La NSA dépense 250 millions de dollars par an dans le programme Bullrun pour aller systématiquement affaiblir une par une toutes les nouvelles technologies de communication. Bullrun

introduit des bugs, des portes dérobées à partir des primitifs des clés de chiffrement pour s'assurer un pied dans ces outils-là. C'est véritablement la conception même de la technologie et son rapport que nous avons avec elles qui ont ici concerné. Les vecteurs d'attaque pour la NSA seront les mêmes que ceux utilisés par le crime organisé, par des attaquants chinois, russes etc.... Il faut se poser là ces questions d'architecture. Les technologies qui sont pénétrées de l'intérieur par la NSA ou ses partenaires privés ou publics sont par nature des technologies fermées, des logiciels et des matériels fermés. D'autre part, cette illusion de sécurité apparaît en premier lieu par le petit canal de votre navigateur : ah c'est bon, je suis en sécurité. En réalité, le site que vous consultez fait confiance à une autorité certificatrice, qui elle-même fait confiance à une autre autorité certificatrice, etc...Cette chaîne de confiance tout entière repose sur du sable. De la même façon, les architectures hypercentralisées genre Google et Facebook sont la source de cette surveillance de masse des individus. Il ne s'agit pas de reproduire un modèle Google ou Facebook. À l'inverse, il faut concevoir des technologies de confiance. Au lieu d'un Google à la française, faisons plutôt une espèce de non-Google, d'anti-Google à la française qui reposerait sur les architectures décentralisées d'un logiciel libre.

On avait un projet de logiciel libre qui est français, développé principalement par des Français, un moteur de recherche décentralisé qui s'appelle Seeks. Pas un centime d'investissement n'a été consacré à Seeks depuis les débuts du projet malgré, il y a quatre, ans son atout compétitif pour la France. Il est temps de repenser ces investissements dans la technologie, de mutualiser les ressources entre le public et le privé : par exemple, l'ANSSI devrait fournir des outils pour la sécurité des citoyens, des logiciels libres, des architectures décentralisées, des téléphones chiffrés. Je me pose la question de savoir pourquoi ces téléphones chiffrés ne sont pas des logiciels libres entre les mains de tous les citoyens. Je suis convaincu que nous aurions décelé des failles de sécurité présentes dedans et qui n'auraient pas été trouvées par ailleurs. Il est temps de développer ces technologies faites pour être appropriées par les citoyens, regagner ainsi leur confiance et leur apprendre la cybersécurité.

Patrick PAILLOUX

Je suis d'accord et pas d'accord. Nous nous sommes frottés à cette question plusieurs fois, y compris sur les téléphones mobiles. Ce n'est pas aussi simple. Il ne suffit pas de mettre un logiciel libre sur un téléphone tout public pour d'un seul coup parvenir à sécuriser l'ensemble. Un logiciel par nature est très adhérent à son matériel, matériel que nous ne maîtrisons pas car conçu par des grandes entreprises. Par ailleurs, le logiciel libre repose sur des méthodes de financement légères. L'ANSSI a financé des projets d'évaluation dans le logiciel libre. Il faut prendre conscience que nous ne sommes pas dans un monde de « Bisounours ». Des personnes vivent de

cette activité chère, lourde et très compliquée. Je suis d'accord sur un ensemble de chose, simplement le logiciel libre n'est pas une réponse absolue qui nous amènera sur des systèmes de sécurité totalement fiables. La façon dont le monde fonctionne aujourd'hui, malheureusement ou heureusement je ne sais pas, c'est d'avoir des industriels. Si les Américains sont aussi forts de nos jours, c'est qu'ils ont des industriels puissants et ceci indépendamment du fait qu'ils font du renseignement, piègent ou ne piègent pas. L'intérêt de la France est d'avoir aussi des industries puissantes. C'est une des raisons pour lesquelles nous avons un plan cybersécurité qui figure dans la liste des 34 plans annoncés par M. Arnaud Montebourg dont les objectifs visent à développer ce type d'industrie en France.

Michel PICOT

Je vais demander à David LACEY comment ces sujets sont abordés en Grande-Bretagne et plus généralement dans les pays Anglo-Saxons. Comment se gère la cybersécurité ou la cybercriminalité ? quelles sont les bonnes pratiques ?

David LACEY.

Je ne pense pas qu'il y ait de bonnes pratiques car ces dernières sont une partie du problème. Les meilleures pratiques créent une mono-culture : tout le monde copie tout ce que font les autres. La cybercriminalité est un jeu de jeunes gens. Les données récentes qui ont été la cible de violation en Amérique ont affecté 70 millions de clients signalés. Ces violations se sont basées sur des logiciels malveillants créés par un garçon de dix-sept ans à Saint-Pétersbourg. Les jeunes qui aiment pénétrer les systèmes peuvent choisir soit une carrière dans la criminalité soit dans la sécurité. La société britannique est plus indulgente envers les jeunes qui « hackent » pour le plaisir. Beaucoup de délinquants potentiels deviennent des professionnels de la sécurité.
Au contraire en Amérique, le FBI est plus agressif à poursuivre les jeunes gens et stigmatise certains jeunes hackers. Ainsi, Iceman, un célèbre fraudeur de carte de crédit a choisi une carrière dans le crime au lieu de la sécurité informatique.

Au Royaume-Uni, la Metropolitan Police a proposé des moyens pour les plus de vingt-cinq ans dans le domaine de la délinquance informatique alors qu'initialement elle était sans défense. Les budgets ont maintenant triplé avec plus de 15 millions de livres par an et une équipe de 400 personnes. Ceci est dû à l'augmentation de plus de 60% de la cybercriminalité au cours de l'année au Royaume-Uni, ce qui a coûté à son économie environ 81 milliards de livres Sterling. Il est également important d'avoir des liens très forts avec les autres services de police. La police de Londres travaille étroitement avec le FBI américain, lui permettant ainsi de lutter contre la fraude à la carte de crédit. Nous avons besoin d'une réponse globale pour lutter contre un réseau criminel international. En plus des enquêtes au Royaume-Uni, l'accent est mis sur des conseils aux citoyens et aux petites entreprises. Il n'est pas encore de très bonne qualité mais il y a un très bon

début de partenariat entre la police et les entreprises dans l'ensemble des régions du pays. L'appui aux petites entreprises a une tendance plus affirmée dans une région comme le Pays de Galles, qui cherche à attirer de nouveaux investissements étrangers. Mais le gouvernement se plaît encore à croire qu'au Royaume-Uni, l'industrie financera la police pour la soutenir dans son action. Mais je ne pense pas que cela pourrait arriver. La police a besoin de budgets de plus en plus importants pour lutter contre la cybercriminalité. Je pense que nous devons repenser actuellement dans son intégralité la direction de la sécurité.

Michel PICOT

Merci beaucoup, c'est intéressant de voir ce partenariat qui existe notamment entre la Police et les PME. Mon Général, vous me coupez si je me trompe, il y a déjà un partenariat Public / Privé : la gendarmerie nationale, la région Nord-Pas-de-Calais que je salue au passage, très active dans ce domaine. Il existe un partenariat de sensibilisation, d'audit et même d'explication.

Général Marc WATIN-AUGOUARD

J'ai toujours pensé que, si le cyberespace étant un espace sans frontière, il allait donner une chance nouvelle aux territoires. Le territoire, c'est le lieu ou on va se reconstruire, reconstruire des solidarités, reconstruire la résilience. Cette résilience porte justement sur l'apport des entreprises.
Le FIC est né à Lille. Au début il y avait 50 entreprises de la Région invitées, 50 personnes, deux mois après elles étaient 150. Progressivement on a créé le FIC , pour quoi faire ?
Pour dire aux PME « vous n'êtes pas seules ». En fait, une PME sur un territoire, c'est un élément essentiel de sa compétitivité économique. Si l'État ne protège pas les entreprises, il manque à son devoir. Je suis intimement convaincu que le partenariat Public/Privé est un thème essentiel qui va marquer les années à venir. Nous ne sommes pas dans une évolution, ni une révolution mais dans une mutation. Tout ce que nous connaissons, les paradigmes sur lesquels nous nous reposons sont morts !.
Nos relations doivent changer, nos organisations doivent changer, nos modes de passation des marchés doivent changer, notre réactivité aussi. Si nous ne sommes pas conscients de cela, la cybersécurité sera un échec. C'est un changement et une mutation complète de nos comportements et de nos manières de faire.

Michel PICOT

Le mouvement est en marche mais cela a déjà commencé à changer avec des premiers résultats. Cela aurait pu être pire si rien n'avait été fait.

Général Marc WATIN-AUGOUARD

Cela commence à changer mais ce n'est pas suffisant. Nous avons une organisation très verticale de type « tuyaux d'orgues » et trop fonctionnelle. Aujourd'hui, nous devrions travailler de manière totalement maillée et transversale. Les territoires ont une chance de participer à la reconstruction de la confiance dans la cybersécurité.

Michel PICOT
Pour conclure, avant la venue du Ministre, je voudrais que l'on parle des solutions et que l'on se projette un peu plus avec des pistes de réflexion que nos spectateurs pourront approfondir avec les 40 ateliers. Je souhaite que nous puissions terminer sur une note un peu plus positive. Nous avons dressé un état des lieux et expliqué les solutions. Faisons un tour de table en commençant par Patrick Pailloux.

Patrick PAILLOUX
J'ai l'habitude de dire que la bataille n'est pas perdue, il existe quantité de solutions. La question à se poser est : contre qui voulons-nous sécuriser nos moyens ? Le travail de l'ANSSI est d'essayer de promouvoir l'ensemble de ces choses-là. Pour revenir sur la sensibilité des dirigeants, ces derniers commencent à devenir attentifs.
Le problème c'est qu'ils ne savent pas quoi faire alors que des solutions existent. L'ANSSI et des entreprises sont en mesure de les aider. Le principal travail à mener est d'éduquer les utilisateurs, les dirigeants, les informaticiens et les praticiens de la sécurité sur les bonnes pratiques. La question que l'on se pose est : qu'est-ce que de la bonne sécurité ? Concrètement, l'ANSSI a ainsi élaboré par exemple deux guides, l'un sur l'hygiène informatique et l'autre relatif à la téléphonie sur IP. Toutes les entreprises commencent à mettre en place de l'IP, opération particulière qui augmente la surface de risque.
Pour autant, il n'est pas impossible de sécuriser la téléphonie sur IP. Quand vous installez cette technologie, généralement l'entreprise qui procède à l'installation n'y connaît rien et lance le CD-ROM. Un travail énorme d'éducation reste à faire. Nous publions un guide dans lequel figure un ensemble de recommandations très techniques sur la bonne cybersécurité sur IP. Au final, des solutions existent pour former, éduquer et faire comprendre.

Michel PICOT
Jusqu'à présent quand les gens sont victimes, ils se disent « ah je suis victime ». Lorsqu'ils sont éduqués, « ah, il s'est passé quelque chose ». Le fameux mot de passe reste 123456. Je me souviens d'avoir animé une conférence cybercriminalité à Eura-Technologies voici 2 ou 3 ans. Nous avons fait un sondage sur l'usage du prénom de l'enfant ou 123456 comme code. Les gens ont joué le jeu et ce fut à l'annonce des résultats une véritable prise de conscience, il suffit d'aller sur facebook pour trouver les prénoms de ses enfants.

Jean-Michel OROZCO
Je ne rentrerai pas dans les solutions techniques qui sont disponibles, j'insisterai sur trois axes où nous devrons certainement travailler pour aller encore plus loin :
1er axe : la partie formation, training, prise de conscience des gens de ce pays, y compris les décideurs.

Michel PICOT
Excusez-moi un Tweet vient de passer où il est écrit : dès l'âge de 5 ans on devrait

apprendre aux enfants les menaces qu'il peut y avoir.

Jean-Michel OROZCO
Si on veut aller vite, il ne faut pas oublier de prendre en compte ceux qui sont déjà aux manettes
2e axe : c'est l'innovation, pilier central du FIC d'aujourd'hui, qui nous permettra d'avoir des solutions « up to date », c'est-à-dire des solutions capables de contrer les menaces fortement évolutives sur ce segment d'activité.
3e axe : l'Europe, si la France veut être en mesure d'avoir des solutions, des technologies capables de rivaliser avec les technologies américaines. Il faut être conscient de la différence de marché qui existe entre les États-Unis et la France : on est dans un facteur de 1 à 10. L'une des solutions, c'est d'essayer de fédérer des solutions, des technologies européennes et de les valoriser sur un marché européen plus considérable que le seul marché français.

Michel PICOT
Cette politique cybersécurité existe-t-elle réellement au niveau européen ?

Jean-Michel OROZCO
Oui, c'est fondamental et c'est un besoin intrinsèque à la cybersécurité. Il y a des industries comme la nôtre déjà présente sur le territoire européen. Quand vous voulez sécuriser par exemple un grand « corporate » vous voyez qu'il n'y a plus des sociétés uniquement françaises, allemandes, italiennes. Elles ont des installations réparties au moins en Europe si ce n'est à travers le monde. Il faut une capacité à transcender les frontières. Les attaquants n'ont pas grand-chose à faire avec les frontières.

Bernard BARBIER
Les solutions commencent à exister. Je suis rentré chez SOGETI qui est une société de service. Nous ne développons pas les solutions, nous les intégrons. Cette notion de service est très importante. Les grandes entreprises sous-traitent leurs moyens informatiques. Ces moyens doivent être sécurisés. Les sociétés de services ont beaucoup de travail. Je suis très confiant sur les technologies qui vont arriver. Il y a un vrai problème d'indépendance. On a parlé des États-Unis, parlons aussi de la Chine, le Snowden chinois n'existe pas. Ce pays a une politique dans les télécoms de nature à tuer l'industrie européenne. On peut se poser des questions sur leurs pratiques vis-à-vis des entreprises européennes. Nous sommes confrontés à deux mondes : un monde chinois dans le domaine des télécoms et un monde américain dans les solutions des grands groupes informatiques. L'Europe est au milieu.
Je fais moins confiance aux Chinois pour nous sécuriser qu'aux Américains. Nous devrions parler peut-être du Snowden chinois.

David LACEY
Comme je l'ai mentionné, nous devons être tournés vers l'avenir. Les responsables de la sécurité sont embourbés actuellement dans de vieilles fausses actions. Nous devons regarder plus à l'extérieur de l'entreprise. Trop de responsables de la sécurité regardent à l'intérieur de leur organisation plutôt qu'à l'extérieur de leurs chaînes d'approvisionnement. Je pense que nous avons besoin

de normes plus élevées. Pour faire face à une menace persistante avancée, nous avons besoin de niveaux significatifs d'expertise, de ressources et de technologies.
Nous ne disposons pas de ces normes en place pour le moment. Nous avons besoin de meilleures compétences pour évaluer le renseignement, la gestion des relations, la psychologie, le marketing, l'ingénierie, l'exploration de données et la gestion des crises. Ces dernières ne sont pas généralement aussi bien faites au sein des organisations.
Je pense qu'il faut intégrer plus rapidement les professionnels de la sécurité, ce qui signifie que les conseils d'administration doivent faire confiance et responsabiliser les responsables de sécurité et ainsi passer outre aux objections commerciales.

En fait, si vous avez une mesure de sécurité essentielle qui ne garantit pas un retour sur l'investissement financier, le conseil devrait approuver, soutenir et faire confiance aux agents de sécurité en chef. Je pense que les régulateurs doivent veiller à ce que la norme encourage des solutions imaginatives qui regardent vers l'émergence de la menace. Finalement, je pense que le gouvernement doit investir beaucoup plus d'argent à l'intérieur de la sécurité. Au Royaume-Uni une devise résume le tout par : «il n'y a pas d'alternative».

Michel PICOT

Dans cette salle, je pense à des responsables de sécurité qui sont dépassés ou qui doivent convaincre le grand management. Comment arriver à évoquer ces questions-là avec son dirigeant et à le sensibiliser ? Ce sont les managers qui devraient être éduqués à ces risques-là.

Jérémie ZIMMERMANN

Heureusement, je suis globalement d'accord avec Patrick Pailloux, sur le fait qu'il ne s'agit pas que du logiciel mais aussi du hardware, de l'humain. Les chinois ont sorti leur système d'exploitation pour GSM alors qu'ils contrôlent déjà le matériel et les puces. Mon désaccord porte sur le monde d'aujourd'hui qui est le monde des géants industriels.
Je pense qu'il faut d'abord se poser la question du monde de demain et de ce qu'on pourra faire pour aller plus loin. Les géants industriels sont tous pénétrés dans leurs technologies, vulnérables, potentiellement sabotés par les programmes de la NSA. Pour aller plus loin que sur ces partenariats public / privé, peut-être faudrait-il des partenariats public-public , privé-privé, public-individus où l'ANSSI française travaillerait avec l'ANSSI brésilienne, angolaise, indienne, avec des géants industriels. C'est ça le logiciel libre, la possibilité de faire coopérer des acteurs qui a priori ont des intérêts divergents autour d'un objet commun. C'est ce genre de coopération plus large qu'il nous faut imaginer aujourd'hui au vu des menaces. Des technologies libres, ouvertes, c'est la seule façon pour que les citoyens puissent se les approprier. S'approprier la technologie, cela veut dire la contrôler. C'est pour moi aujourd'hui l'enjeu de la cybersécurité, que les citoyens puissent reprendre le contrôle de la technologie plutôt qu'être contrôlé par elle. C'est bien ça l'enjeu du logiciel libre.

Michel PICOT

Patrick PAILLOUX pour finir, y a-t-il des coopérations internationales entre d'autres ANSSI en Europe ?

Patrick PAILLOUX

l'ANSSI fermerait si elle ne faisait pas de la coopération internationale. Nous n'avons pas de frontières. Notre capacité à agir et à interagir est en très grande partie dépendante de notre capacité à échanger avec nos grands alliés, c'est une pratique qui fonctionne bien. Nous avons une politique de relations internationales à trois niveaux : les très hauts niveaux (grands alliés), des points de contact partout, et puis pour terminer beaucoup de pays où on développe des accords pour les aider. Le Maroc a avec l'ANSSI une coopération forte.

Michel PICOT

Je regardais les chiffres du sondage initial, 71%. Vous avez deux 2 jours Messieurs pour essayer de voir qu'effectivement la cybersécurité a encore beaucoup de chose à faire malgré tout ce qui a déjà été fait... Merci à tous d'avoir participé à cette plénière : Le Général Marc WATIN-AUGOUARD, Patrick PAILLOUX de l'ANSSI, Jean-Michel OROZCO de Cassidian, Bernard BARBIER de Sogeti, David LAYCE et Jérémie ZIMMERMANN de la Quadrature du Net

Nous avons maintenant l'honneur et le plaisir d'accueillir Mr Manuel VALLS, ministre de l'Intérieur.

P2 – Numérique : quelle stratégie industrielle pour l'Europe ?

Participants

Modérateur : Thierry GUERRIER, Journaliste,

Amelia ANDERSDOTTER, Députés européenne, membres du parti pirate suédois.
Clément CAZALOT, cofondateur et CEO Doctrakr.
Catherine MORIN-DESAILLY, Sénatrice de la Seine-Maritime.
Philippe RAMON, Délégation interministérielle à l'intelligence économique.
Mirva SALMINEN, Cyber Security Rescarcher Storesoft.
Michel VAN DEN BERGHE, Directeur, Orange Cyberdéfence.

Thierry GUERRIER

Mesdames et messieurs, nous allons commencer cette table ronde sur la question de la souveraineté. Elle va dépasser la seule question de la sécurité stricto sensu et de la cyberdéfense. Il sera question de souveraineté industrielle bien entendu, de la stratégie à cet égard, de la souveraineté juridique, des outils légaux pour obtenir et défendre cette souveraineté.

Le titre de cette table ronde : l'Europe, colonie du monde numérique ? Quelle stratégie industrielle pour l'Europe ?

Colonie du monde numérique avec un point d'interrogation, nous verrons pourquoi ce titre a été choisi pour cette table ronde.

Je vous présente nos invités. À ma droite, Amélia Andersdotter, députée suédoise au Parlement européen, membre du parti Pirate, grande spécialiste des questions numériques, qui nous dira ici sa vision de la stratégie industrielle et juridique, de la capacité ou non de l'Europe à se défendre, ou si même elle doit se défendre.

À sa droite, Michel Van Den Berghe qui est directeur de la toute nouvelle société Orange Cyberdéfense, entreprise dont il nous présentera la mission.

Mirva Salminen, ingénieur responsable de la recherche chez McAfee, vous êtes Finlandaise. Je vous remercie de votre présence.

Sur votre droite, Philippe Ramon, conseiller à la Délégation interministérielle à l'intelligence économique. Vous avez en

particulier la mission, auprès du Premier Ministre, de défendre les intérêts des entreprises et chercheurs français en matière de cybersécurité.
Clément Cazalot, PDG de la PME française docTrackr. Malgré quelques offres de rachat extérieures à notre territoire hexagonal, vous avez choisi de rester français. Vous êtes spécialisé dans le traçage et le chiffrement des documents numériques.
Pour lancer ce débat, je propose d'écouter les propos d'une personnalité que le FIC avait invitée mais qui n'a pas pu se libérer, retenue à nouveau par une session de sa commission au Sénat. Il s'agit de la sénatrice française centriste UDI de la Seine-Maritime, que vous connaissez sûrement : Catherine Morin-Desailly. C'est à elle que l'on doit ce sous-titre de notre débat « Europe colonie numérique ? ». Mme Morin-Desailly, vous allez l'entendre, considère qu'il y a urgence aujourd'hui. Notre continent, notre nation européenne, si l'on peut parler ainsi, peut devenir très vite un grand marché de consommation du Web, sans opérateurs réels ni acteurs déterminants de la filière, et même être en difficulté pour défendre ses propres données, son « or noir », pour reprendre l'expression de Mme Morin-Desailly.
Consommateur et non plus acteur ou producteur, urgence... Son propos durera un peu moins de 8 minutes et introduira notre débat. Les termes de celui-ci seront bien posés. Cette interview a été réalisée par CEIS et je pense que les aspects clefs de notre discussion y figureront.

Catherine MORIN-DESAILLY

En fait, le titre, volontairement provocateur, a pour but de créer un sursaut européen. Au lendemain de l'affaire Prism, je crois que l'heure du sursaut est réellement arrivée, il faut que nous réagissions ! La vraie question est celle de la souveraineté, qui doit sans doute évoluer avec Internet. Elle s'entend comme étant l'autorité d'un gouvernement sur un territoire, sur une population. C'est une définition assez traditionnelle mais comme on voit que l'Internet bouleverse les frontières, que l'Etat-Nation en tant que tel n'a plus prise sur l'Internet, dont le principe est justement hors frontières, on questionne cette notion de souveraineté. Je crois que la souveraineté numérique européenne est menacée parce que le numérique dévore tout type d'activité. Il bouleverse les modèles économiques en place, il siphonne la fiscalité, il défie également les règles de droit (on le voit par exemple en matière de protection des données personnelles). Bref, c'est l'avenir entier de l'Union et des Européens qui est en jeu. On voit également que l'Europe est prise en étau, ou risque de l'être, entre d'un côté les équipementiers asiatiques qui excellent dans la fabrication des équipements et de l'autre, les fournisseurs de services Internet qui sont extra-européens, notamment américains. L'Europe est en perte de vitesse sur ces sujets si elle ne réagit pas. Elle est également en passe de perdre la maîtrise de ses données. On voit aussi que la diversité culturelle, qui est une des spécificités de notre continent, est mise à

mal. Bref, on voit que l'Union européenne n'est pas du tout en ordre de bataille pour affronter ces grands défis. Je note que l'Union européenne s'est dotée d'un agenda numérique mais que celui-ci ne questionne pas vraiment ce qui est le vrai sujet, à savoir : serons-nous simples consommateurs ou consommateurs et producteurs sur ce marché unique numérique ?

Il revient au Parlement d'alerter l'exécutif français et européen sur cet enjeu. Je note que le Sénat, pardonnez-moi de vanter les mérites de la chambre à laquelle j'appartiens, se distingue par son regard beaucoup plus prospectif sur ces questions que ne le fait actuellement le gouvernement. Je pense qu'il est temps que l'Union prenne sa juste place dans l'univers numérique. Cela passe par trois impératifs que j'évoque dans mon rapport. Premier impératif, faire de la souveraineté numérique une réelle ambition pour l'Union. Deuxième impératif, miser sur l'unité européenne pour peser plus lourd, en tout cas davantage, dans ce qu'il convient d'appeler aujourd'hui le cyberespace. Il est la nouvelle géographie du monde numérique dans lequel désormais nous évoluons et qui n'a rien à voir avec la géographie traditionnelle des Etats-Nations, qu'il s'agisse de gouvernance de l'Internet, de fiscalité numérique ou qu'il s'agisse aussi de la protection des données personnelles dont on parle beaucoup en ce moment. Troisième impératif selon moi, faire de l'Union une opportunité pour la numérisation de notre économie européenne. On voit qu'il y a des industries spécifiques du numérique mais qu'il y a aussi beaucoup d'entreprises et d'industries qui s'équipent de manière numérique et transforment, font évoluer leur activité avec des possibilités de développement et de croissance. Je pense que l'Union a, à cet égard, les moyens de promouvoir ces entreprises numériques. Il faut qu'elle le fasse.

Ces trois impératifs, dans mon rapport, se déclinent autour de trente propositions concrètes qui visent à mettre en œuvre une politique en faveur de la souveraineté numérique.

Cette politique doit garantir la sécurité numérique des réseaux européens et donner les moyens à l'Union de garder la maîtrise de ses données, l'or noir du numérique. Elle doit aussi préserver la diversité culturelle sur l'Internet et défendre le principe de la neutralité du Net. Vous le savez, la neutralité du Net c'est un Internet accessible et ouvert à tous sans discrimination. Enfin, la politique doit promouvoir l'industrie numérique européenne. Aujourd'hui, on a l'impression que l'on est en train de constituer un marché unique numérique au seul bénéfice du consommateur et non pas de la production. Cela signifie que, dès à présent, l'Union devrait explorer de nouveaux outils qui permettent de juguler la domination notamment des géants de l'Internet. On pourrait imaginer d'imposer des obligations d'équité, de non-discrimination à certains acteurs de

l'Internet devenus ce que l'on appelle en termes juridiques des facilités essentielles. Ils ont en effet acquis une position dominante et monopolistique et toute l'activité économique, quelle qu'elle soit, devient impossible sans eux. C'est le problème des moteurs de recherche : 97 % des recherches sont effectuées par Google. Google, très clairement, est devenu une facilité essentielle. C'est en fait une intermédiation obligatoire pour n'importe quel type d'activité que l'on veut exercer. Cet état de fait pose une vraie question. Ce n'est pas, je le note, la voie qu'explore le nouveau Paquet Télécom que propose aujourd'hui Neelie Kroes.

Sans même parler de protection, on peut au moins plaider pour une vision qui ne soit pas exclusivement libérale de cette politique. L'Union est en mesure d'ouvrir des opportunités de marché à sa filière industrielle numérique qu'elle doit soutenir. D'une part, elle peut - elle doit selon moi - négocier une meilleure loyauté de la concurrence mondiale, en tout cas une concurrence qui ne se fasse pas complètement à notre détriment, qu'il s'agisse par exemple d'aides d'État, d'ouverture des marchés publics. D'autre part, elle pourrait utiliser également le levier de l'achat public pour accompagner notamment le développement des start-ups et d'un cloud européen, pour prendre un exemple extrêmement concret et dont on parle beaucoup aujourd'hui. Je crois tout de même que le concept de préférence communautaire a une pertinence quand il s'agit de sécurité. Qui dit sécurité dit souveraineté. D'ailleurs, je note que ce principe est déjà implicitement reconnu par les règles européennes qui concernent notamment les marchés publics de sécurité. Je me demande dans mon rapport si on ne pourrait pas inclure dans le périmètre de ce type de marché l'achat d'équipements numériques hautement stratégiques, par exemple les routeurs de réseau, tout simplement pour se prémunir contre les risques d'espionnage de pays fournisseurs.

Je voudrais rappeler ce moment important, le 7 octobre dernier, qu'a constitué la conférence de Montevideo, en Uruguay, où l'ICANN, qui est l'organisme de gestion de l'Internet (l'adressage, le nommage) et qui est sous dépendance du département du commerce américain a pour la première fois pris ses distances avec ses méthodes jugées scandaleuses pour plaider une gouvernance multi-acteurs de l'Internet. Il faut pouvoir rétablir la confiance des internautes, la sécurité en ligne et l'unicité du réseau. Je pense qu'à cet égard l'Union européenne est bien placée entre le « tout ICANN » américain et des systèmes tels que les systèmes chinois, russe, iranien, qui sont des systèmes plutôt endogames et qui visent à contrôler et priver de liberté les internautes. Il y a une place pour un système européen qui porte les valeurs de la charte des droits fondamentaux et qui soit respectueux des grandes libertés. Ce sont des valeurs démocratiques auxquelles nous sommes attachés, qui n'empêchent pas d'ailleurs une certaine forme de régulation. Un Internet libre et ouvert mais

un Internet régulé. Je crois, profondément, que, si l'Europe est unie, si elle parle d'une seule voix dans ces instances mondiales de gouvernance, elle peut amener une vision juste et équilibrée.

Thierry GUERRIER

Voilà donc cette intervention très claire. L'Europe est-elle unie ? C'est une des questions que nous allons poser. Deux précisions si vous permettez : le Sénat français a confié une nouvelle mission à la sénatrice Morin-Desailly. Elle sera rapporteuse d'une mission d'information sur la nouvelle stratégie européenne dans la gouvernance mondiale de l'Internet. D'autre part, un sondage réalisé il y a peu sur Internet pour savoir si nous n'étions « plus qu'une colonie aujourd'hui » montre que 54 % des internautes sont de cet avis. Vous pouvez intervenir dans notre débat sur Twitter. Les questions seront éventuellement posées tout à l'heure pour associer la blogosphère à notre discussion. Madame Andersdotter, merci, je rappelle que vous arrivez de Bruxelles et que vous êtes député européen. Pouvez-vous nous rappeler quelle est la position du parti Pirate, dont vous défendez la stratégie ?

Amélia ANDERSDOTTER

Bonjour, je suis du parti Pirate, fondé en 2006 en réaction au manque de débat relatif à ce qu'Internet fait pour nous en tant qu'être humain, en tant que citoyen suédois. Comme le parti s'est répandu dans beaucoup de pays en Europe, la question est aussi de savoir ce que fait Internet pour l'Europe et comment nous pouvons nous assurer qu'Internet est utilisé pour le bien de l'Europe. On m'a demandé de réagir à la vidéo de la sénatrice Morin-Desailly. Ses propositions me conviennent dans l'ensemble, je ne peux rien en dire de plus concret sans en connaître les détails.
Je veux commencer mon intervention en commentant ce que notre animateur disait au début, à savoir que nous avons les outils juridiques dont nous avons besoin. Ce n'est simplement pas vrai. Nous allons discuter de politique industrielle après un discours liminaire du Ministre de la Défense. Dans quel monde, après la seconde guerre mondiale, le ministère de la Défense contrôle-t-il la politique industrielle dans un pays civilisé ? Dans absolument aucun pays. C'est pourquoi, s'agissant d'Internet, nous sommes dans une situation abstraite où, pour on ne sait quelle raison, on a « militarisé » la sécurité en tant que notion et dans l'idée même de ce qu'elle devrait être. Nous avons un débat centré sur la nation et l'État autour de ce que l'intégrité du réseau devrait être, sur la manière dont nous devrions utiliser l'encryptage et comment nous déployons une stratégie de défense. En tant que jeune citoyen européen ayant accès à un réseau Internet qui était initialement ouvert et gratuit, j'ai des amis dans beaucoup de pays européens qui travaillent exactement aux mêmes buts que moi, qui ont exactement la même expérience de l'usage d'un réseau global. Je me sens un peu à l'écart de ça, je ne m'identifie pas à un État. Je suis un individu autonome, j'ai grandi en Europe. Je dirai plutôt que nous avons besoin de nos propres règles de marché

autour de la sécurité des réseaux d'information. La Commission européenne a vainement essayé de faire de la sécurité des réseaux et de l'information une affaire économique. C'est une chose à laquelle l'Europe devrait être un peu plus attentive. Elle devrait notamment s'assurer de l'autonomie des industries de sécurité des réseaux et de l'informatique vis-à-vis du complexe militaire. J'espère que c'est quelque chose que la sénatrice Morin-Desailly pourra envisager d'ajouter à son programme, car elle manifeste une foi profonde en la démocratie et les droits de l'homme. Puis-je ajouter quelque chose ? Google ne domine pas partout en Europe le marché des moteurs de recherche. Nous avons plusieurs concurrents européens, Seznam en République tchèque, Ixquick aux Pays-Bas...

Thierry GUERRIER
Je voudrais vous demander précisément de quelle façon vous considérez que la souveraineté européenne est, ou non, menacée. Vous avez déjà évoqué quelques éléments, ces questions de règles quant au chiffrement mais aussi les moteurs de recherche et en particulier Google. De façon générale cependant, qu'est-ce que caractérise selon vous l'existence d'une vraie menace sur la souveraineté européenne, et dans quels domaines ?

Amélia ANDERSDOTTER
L'Union Européenne n'a pas de politique industrielle pour Internet. Nous avons une politique militaire propre à chaque pays, qui s'oppose à celle des autres. Le ministère de la Défense, chez moi en Suède, déclare ouvertement qu'il souhaite faire la guerre aux autres pays sur les outils que j'associe plutôt à la communication avec mes amis.

Thierry GUERRIER
Il déclare cela ?

Amélia ANDERSDOTTER
Oui, il le dit sur Internet, il y a un Blitzkrieg sur les points d'accès et les routeurs. Vous imaginez ? Quelle stupidité. Alors, le problème pour l'Europe est que nous sommes incapables d'identifier nos points forts. Par exemple, l'Union européenne a toujours été bonne pour le peer to peer. Ce n'est pas par accident que Minanova est hollandais, que Oink était britannique, que Demonoid est ukrainien et The Pirate bay suédois. C'est parce qu'un réseau de circulation de données est un endroit où les personnes se regroupent pour coopérer sur un plan d'égalité pour arriver à un objectif commun. Ils n'ont connu de succès que quelques années en Europe et dans le monde car ensuite nous avons criminalisé les innovateurs et les usagers. De même, Skype, exemple de site de peer to peer de voix sur IP. Nous ne faisons pas grand-chose pour encourager le déploiement de ces technologies, par exemple dans le secteur public. Nous avons des téléphones de service cryptés qui pourraient être fournis par des entreprises de taille intermédiaire, je connais au moins un ou deux fournisseurs allemands, mais le parlement européen a choisi d'investir chez Cisco... Souvent, quand des PME européenne font

une innovation majeure qui pourrait amener des services très utiles aux citoyens européens, en les mettant en rapport les uns avec les autres ou en les faisant coopérer sur des petits projets, nous finissons par criminaliser et punir si bien qu'elles finissent par disparaître. Il ne nous reste donc plus que ces services américains centralisés, monolithiques et pas forcément adaptés à ce que nous sommes. En tant que Suédois, je ne peux pas faire confiance à un acteur centralisé et monolithique français. C'est historique, je sais que je devrais être plus tolérante mais je me sens plus à l'aise à coopérer avec les Français sur un plan d'égalité plutôt qu'à dépendre d'un pouvoir français. Heureusement, l'Internet est très décentralisé dans sa conception et adapté à ce développement. La seule chose que nous avons besoin de faire est de regarder ce qu'est exactement Internet et d'apprendre comment l'utiliser pour notre bien commun.

Thierry GUERRIER

Merci madame la députée. M. CAZALOT est impatient d'intervenir pour vous répondre car sa spécialité est le chiffrement. Je voudrais cependant donner d'abord la parole à M. VAN DEN BERGHE. Vous devez être satisfait d'entendre que, finalement, quitte à collaborer avec un « mammouth », autant le faire avec un « mammouth » français, si j'ai bien compris la formule et même si je caricature un peu. Orange n'est pas un « mammouth », même si c'est un acteur considérable. Pouvez-vous nous en dire plus sur cette nouvelle entreprise Orange-CyberDéfense ?

Michel VAN DEN BERGHE

Orange-CyberDéfense n'est pas une entreprise, c'est une offre de service, une bannière regroupant tous les experts d'Orange pour aider les entreprises à bâtir, concevoir et mettre en œuvre la stratégie de cyberdéfense. Orange Cyberdefense fait suite au rachat d'ATHEOS, qui était une PME française et reste française, destinée à aider les entreprises à lutter contre la cybercriminalité. Il s'agit aussi de faire bénéficier toutes les grandes entreprises de notre retour d'expérience en tant qu'opérateur (car nous sommes une cible importante en tant qu'opérateur).

Thierry GUERRIER

Comment réagissez-vous à ce que vous venez d'entendre Mme MORIN-DESAILLY et à la réaction de cette parlementaire européenne ?

Michel VAN DEN BERGHE

Le sursaut, nous voulons bien y participer. On ne va cependant pas définir une stratégie de cyberdéfense en se refermant sur nous-même. On sait bien que, aujourd'hui, dans les équipements de nos amis américains, il y a des portes d'entrée et de sortie... Ce n'est pas nous, acteurs français, qui vont du jour au lendemain lutter contre la NSA. Ils ont des moyens que nous n'avons pas. On peut, en revanche, surveiller ces portes dérobées, que l'on connaît, et s'assurer qu'elles ne sont pas

utilisées à des fins malveillantes. Un groupe comme Orange, aujourd'hui, ne peut pas imposer à ses clients, qui sont des clients internationaux, des technologies franco-françaises ou franco-européennes. À nous de travailler pour connaître les failles mises en œuvre dans ces technologies, les surveiller et éviter qu'elles soient utilisées contre nous.

Thierry GUERRIER
Ce n'est pas exactement le point de vue de Mme MORIN-DESAILLY ou certains de vos concurrents qui considèrent que l'on a une capacité, quand même, à travers les marchés publics et les règles de concurrence, à imposer une capacité technologique dans les nouveaux sauts technologiques dans lesquels on a une forte présence.

Michel VAN DEN BERGHE
Vous parlez là plutôt des grandes administrations. On ne va pas imposer aux grands groupes internationaux français, qui ont déjà mis en œuvre une stratégie de sécurité avec une technologie américaine, de tout changer pour repartir avec une technologie européenne. J'insisterais plutôt sur la formation, si je peux me permettre de donner un conseil. Il faut arrêter de voir partir tous les talents français à l'étranger parce que l'on n'est pas capable de leur offrir un avenir en France. Aujourd'hui, notre pays est intelligent, c'est un pays d'ingénieurs. Il y a eu une grande conférence sur le numérique à Las Vegas où 20 % des sociétés qui ont présenté des nouvelles technologies étaient françaises. Il faut mettre en œuvre des budgets pour aider ces créateurs d'entreprise à rester en France et ne pas les voir partir aux Etats-Unis pour y créer leur entreprise. C'est là-dessus qu'il faut travailler. Une société comme la nôtre est en manque de compétences, de gens pointus dans la cyberdéfense qui vont chez Google et Microsoft, où ils trouvent un avenir et des moyens de travailler. La formation est vraiment importante. On commence à développer ces moyens, comme le montre la création à Maubeuge, d'une licence qui forme les jeunes sur le « Hacking éthique ». C'est en se servant de notre cerveau que nous, Français, pourrons lutter sur le plan international.

Thierry GUERRIER
Ce que vous dites est important. On parlera financements, il y a la notion de salaire, de ce qui est offert aux jeunes ingénieurs et aux jeunes créateurs d'entreprise. Mais en amont, vous considérez que les filières de formation ne sont pas assez pointues et ne permettent pas de fournir au marché et aux entreprises européens les compétences spécifiques en cyber sécurité.

Michel VAN DEN BERGHE
On voit déjà qu'aujourd'hui, dans tous les cursus de formation au développement d'applications numériques il y a très peu de prise en compte du domaine de la cybersécurité. Du coup, les nouvelles

applications mises en place dans les entreprises deviennent des failles car la sécurité n'a pas été envisagée dès la conception. Ce qu'il conviendrait déjà de faire, c'est d'imposer dans les cursus de formation de développement d'applications numériques la prise en compte des enjeux de la cybersécurité afin que les développeurs soient formés et que les applications soient plus pérennes. Les RSI doivent vérifier, chaque fois qu'une nouvelle application est mise en œuvre, si elle ne va pas rajouter une nouvelle vulnérabilité à l'entreprise.

Thierry GUERRIER
Mirva SALMINEN, ingénieur de recherche, responsable de la recherche chez McAfee ; rappelez-nous en un mot votre mission et ce que représente la R&D chez McAfee.

Mirva SALMINEN
Il y a encore un an, je travaillais pour une société finnoise, appelée Stonesoft, spécialisée dans les firewalls de nouvelle génération et la recherche sur les cyberattaques. Au début de cette année, je suis devenue employée de McAfee. Pour moi, ce que signifie la recherche chez McAfee est quelque chose que je découvre encore. Je fais de la recherche en Finlande sur la cybersécurité et les cyber attaques, les techniques d'évaluation... Ce que nous faisions précédemment n'a pas changé mais nous le faisons sur un volume plus important et en coopération, en coordination avec la compagnie mère.

Thierry GUERRIER
Selon vous, qu'est-ce qui est décisif pour que, à l'échelon d'un continent comme l'Europe, on puisse continuer, dans l'univers numérique et digital, à garder et développer des acteurs forts d'un point de vue technologique et industriel ?

Mirva SALMINEN
De mon point de vue, le cyberespace a pénétré toute la société. C'est ainsi que je vois les choses. On l'utilise pour contrôler à distance des infrastructures critiques, pour des services en ligne, pour la production, l'utilisation et le stockage d'information... Nous devons garder ceci à l'esprit. Pour moi, le cyberespace en lui-même n'est pas indépendant du reste de la société. Ce qui est crucial, dans la société, c'est la confiance. La confiance est une valeur dans le cyberespace aussi. Par exemple, si on y réfléchit, une des choses les plus importantes pour une société spécialisée dans le secteur des technologies de l'information et de la communication, c'est la confiance. La confiance est liée à la sécurité, mais les deux sont différentes : l'une n'est pas la réplique de l'autre. Peut-on imaginer la sécurité sans confiance ? La confiance est par ailleurs beaucoup liée à la notion de réputation. Les sociétés et les gouvernements devraient prendre soin de leur réputation lorsqu'ils sont en contact avec le cyberespace.

Thierry GUERRIER
J'aimerais une précision. Qu'est-ce que vous voulez dire en parlant de confiance et

de technologie ? Sont-ce la nationalité, la qualité technologique, la réputation des équipes de chercheurs qui font la confiance ? Quand on voit des clients français qui ont des grands comptes dans le monde entier s'inquiéter de voir certains de leurs matériels installés ailleurs dans le monde, fabriqués en Chine par exemple, posséder éventuellement en leur sein des composants permettant l'espionnage, on comprend que la nationalité est un élément de confiance. À quoi tient donc selon vous la confiance ?

Mirva SALMINEN
Il y a deux dimensions. On peut créer la confiance par la technologie. On crée des certificats européens qui garantissent certains standards ou certaines provenances. La confiance se crée aussi par l'expérience.

Thierry GUERRIER
Comment les institutions européennes peuvent-elles déjà, pour commencer, déclencher un mouvement de confiance ? La sénatrice a fait des suggestions, avec un cloud européen, des achats imposés pour des technologies issues de la préférence communautaire ou encore des règles de concurrences fondamentalement pour les GAFA, dans les grands monopoles de fait qui sont des facilités essentielles aujourd'hui. Puisque la confiance technologique ne suffit pas, que doit décider l'Union européenne en plus ?

Mirva SALMINEN
Certaines choses suggérées par Mme Morin-Desailly sont intéressantes mais ne constituent pas nécessairement une bonne solution pour tous les pays. Les structures économiques et technologiques sont différentes selon les pays. Il doit y avoir une décision nationale qui s'appuie sur un cadre européen, notamment sur le plan législatif. Tout cela demande des discussions nombreuses pour éclairer ce qui nous semble plus ou moins important. C'est l'affaire de la politique.

Thierry GUERRIER
Justement, Monsieur Ramon, ces discussions, le gouvernement français y participe pour essayer de contrer un impérialisme qui est essentiellement américain. Comment la mise en place d'une filière numérique européenne permettrait-elle de lutter contre cet impérialisme ?

Philippe RAMON
Je ne crois pas du tout aux vertus du repli. L'économie est mondiale, mondialisée et toutes les opportunités viendront du fait que, justement, nous sommes dans cette logique mondiale. L'idée d'un repli salutaire qui permettrait, avec une ligne Maginot, d'être certain que plus rien ne nous arrive, je n'y crois pas du tout. La souveraineté, à mon avis, ne peut venir de cette démarche de repli. Du point de vue économique, en revanche, nous avons un véritable intérêt à soutenir une vraie filière, ne serait-ce que pour maintenir des

ressources humaines de très haute qualité et des questions d'emploi. Nous sommes un territoire d'innovation important, avec beaucoup d'argent national et européen pour la soutenir, ce qui implique d'avoir une filière pour faire aboutir cette innovation. Sinon, l'innovation financée par le contribuable européen part vers les Etats-Unis ou le sud-est asiatique. Il est donc nécessaire d'avoir une filière. Ce n'est cependant pas suffisant. La notion de patriotisme en économie me paraît antinomique. Peut-on considérer que Peugeot, qui vient d'être partiellement racheté par des fonds chinois, n'est plus une entreprise française ? Est-ce que, aujourd'hui, les entreprises qui travaillent dans la cybersécurité n'appartiennent à la sphère européenne qu'à la stricte condition qu'aucun centime de leur capital ne vient d'un pays extra-européen ? Ce sont des notions difficiles à manipuler et les solutions doivent venir d'ailleurs.

Thierry GUERRIER

Vous ne croyez pas à la suggestion de la préférence communautaire appliquée à ce secteur, comme dans la politique agricole commune ?

Philippe RAMON

Je pense que c'est nécessaire d'avoir des normes, des concordances entre les attentes des pouvoirs publics et de la société européenne. Le problème de la préférence communautaire, c'est la ligne de partage : comment définit-on aujourd'hui une entreprise européenne ? Est-ce parce que son dirigeant est européen, que son siège est en Europe, que son capital est essentiellement européen ? C'est une notion difficile à définir. Je crois beaucoup plus à la nécessité d'être vigilant contre un certain impérialisme juridique. Il serait bon que l'Europe se prémunisse contre les attaques légales extraterritoriales américaines, mais aussi d'autres pays qui développent des lois extraterritoriales, dont l'application conditionne l'accès à des marchés et expose à des sanctions devant des tribunaux américains ou de pays du Golfe, par exemple. Ces armes juridiques permettent d'obtenir de l'information peut-être plus sûrement que par l'intermédiaire d'une cyberattaque. Il ne sert à rien de garder les portes fermées si, par ailleurs, vous êtes tenu de donner de l'information par une réquisition d'un juge américain ou autre... Il y a un vrai travail qui doit être fait à l'échelon européen pour cadrer ces lois extraterritoriales et vérifier que les demandes et réquisitions soient strictement proportionnées au besoin et ne soient pas utilisées à des fins économiques. Les lois extraterritoriales sont en général légitimées par des besoins de lutte contre le terrorisme, la prolifération des armes, la corruption... Il est important que des instances européennes ou nationales soient en mesure de vérifier que la requête est bien adaptée à la demande. Malheureusement, ce n'est pas le cas aujourd'hui. Ce peut être une réflexion européenne. Si on développe une filière européenne, il est nécessaire de réfléchir

aussi sur un autre volet qui est celui des attaques illégales. La commission a pris une initiative pour lutter contre le vol et l'utilisation des secrets d'affaire. Aujourd'hui, donner une information à la NSA, qui travaille sur la prévention du risque terroriste, cela a une certaine légitimité. Si la NSA donne ensuite cette information à une entreprise américaine qui va l'exploiter contre une entreprise européenne, on est dans un tout autre cadre. Il est nécessaire de développer des lois au niveau européen pour lutter contre l'utilisation de secrets d'affaire et d'informations obtenues dans ce genre de cadre. Je crois qu'il est indécent de donner un certain nombre de droits à des Américains et pas au reste du monde. Ce n'est pas normal, comme il est anormal d'obliger les entreprises requises à ne pas informer sur le fait qu'elles ont été requises. Il n'est pas normal que personne ne le sache. La question, c'est celle de la vérification par des voies judiciaires ou par l'opinion publique de l'adéquation des requêtes aux objets pour lesquelles elles ont été formulées. S'agissant de la directive européenne, la capacité de blocage de l'Union ne fait pas l'objet d'une initiative. Il y a une initiative sur le secret des affaires, le vol et l'utilisation d'informations acquises illégalement. La commission est en train d'aboutir et une proposition devrait être faite au parlement début février. Il faudra attendre le renouvellement du parlement pour voir aboutir cette initiative.

Thierry GUERRIER

Monsieur CAZALOT, quand je vous ai demandé ce que vous faites chez docTrackr, vous m'avez répondu : « *est-ce que vous connaissez Mission impossible ?* ».

Clément CAZALOT

Vous connaissez la série ou les films : au début, le héros reçoit une mission sur un document qui s'autodétruit immédiatement après. C'est ce que nous faisons. Nous faisons de la cryptographie appliquée à de la gestion documentaire. Nous permettons à des documents d'être partagés, en format Pdf ou Office. Après leur partage, on permet leur destruction à distance et on permet de savoir qui a fait quoi avec le document, s'il a été ouvert en Chine, en Australie, à des endroits où il ne faudrait pas... Ensuite, on permet de détruire ces documents à distance. De grandes entreprises internationales sont aujourd'hui nos clientes.

Thierry GUERRIER

L'innovation reste-t-elle encore européenne, comme vous en êtes la démonstration flagrante, ou est-elle américaine ?

Clément CAZALOT

Nous sommes un spin off de Gemalto, société du CAC 40. Nos premiers clients étaient à Paris. La société a levé 2 millions de dollars aux États-Unis, faute de pouvoir le faire en France. Une partie des accords prévoit que j'habite à Boston. Je suis venu en France pour le FIC. Notre plus gros

marché est la France, nous avons des ingénieurs en Roumanie, notre directeur technique est un Franco-Roumain, nous avons des Allemands dans nos équipes... Alors que sommes-nous ? Européens, Français, Américains ? Nous sommes du monde entier et la réalité que je vois, c'est que les propositions de législation sur l'endroit où nous devrions acheter nos technologies sont mignonnes mais sans fondement. Si on doit acheter des routeurs, on ira vers ce qui se fait de mieux sur le marché. Qui, dans l'assistance, utilise une tablette Archos ? J'ai du respect pour les tablettes Archos mais les gens achètent des tablettes Apple, Samsung... On est censé acheter ce qu'il y a de mieux. Si ce qui est le mieux est européen, on achète européen, si c'est américain, on achète américain.

Thierry GUERRIER
Excusez-moi, mais qu'est-ce qui définit ce qui est le mieux ? C'est ce qui est le plus efficace, ce qui est le plus développé sur le marché ou ce qui a été aidé dès le départ pour amorcer une bonne dimension marketing et commerciale qui lui permet d'être présent sur le marché ?

Clément CAZALOT
C'est ce qui répond le mieux aux besoins de l'acteur qui fait la demande de technologie. Pour un opérateur privé, c'est ce qui répond au cahier des charges. Pour un acteur public qui veut acheter européen, ce sera ce qui répond à la définition du mot « européen ».

Thierry GUERRIER
Vous avez déjà, dans la description de votre entreprise, pointé du doigt certaines difficultés. Avant même de parler du financement et de la formation, il y aurait une question de culture, de mentalité. On ne serait pas très bons, en Europe et en particulier en France, en marketing ?

Clément CAZALOT
C'est une réalité : nos ingénieurs sont excellents, nous sommes très bons en technologie. Aller se vendre à l'étranger, être capable d'exposer en trente secondes pourquoi sa solution est la meilleure du marché, cela s'apprend en Allemagne, aux Etats-Unis où la culture de la vente et de l'exportation est complètement différente.

Thierry GUERRIER
Il reste tout de même que 80 % de l'infrastructure du Web est aujourd'hui américaine. Qu'est-ce qui reste aujourd'hui comme capacité européenne, et française notamment, d'engendrer du meilleur, du neuf, du performant ?

Clément CAZALOT
L'UE est-elle une colonie du monde numérique ? Aujourd'hui, oui, nous consommons de l'américain, du chinois, du monde entier et pas tellement d'européen. Après avoir fait ce constat, et cessons de pleurer dessus, il y a une possibilité de construire sur ces infrastructures qui sont déjà déployées, la possibilité d'apporter de

l'innovation, des nouvelles réponses au-dessus de ces solutions déjà déployées, et ce dans tous les domaines. Il y a un mois, une société française, Critéo, a été cotée au Nasdaq pour 1,7 milliard de dollars. C'est une des plus belles start-up de France, et personne n'en a parlé dans notre pays. C'est une des plus grosses croissances. Ils réinventent la publicité, ils construisent sur les données de Google, sur l'ensemble de leur réseau pour créer de la publicité ciblée. Ils construisent sur l'Internet, qui est américain, pour fournir une solution innovante, en étant français et en étant américain également, avec des équipes commerciales dans la Silicon Valley tout en gardant des ingénieurs à Paris dans leur quartier général parisien.
On parle de capital risk. C'est un terme très français. Aux Etats-Unis, on évoque le venture capital, capital entrepreneur. Ecoutez le nombre de fois où, dans une discussion relative à une vente de solution, apparaissent les mots « petit », « problème ». C'est culturel. On parle de long terme, la France a des atouts pour réussir. Cessons de regarder le passé, regardons le futur et investissons sur les PME, l'innovation, la création de croissance. N'essayons pas d'ériger des barrières autour de la France et de l'Europe.

Thierry GUERRIER

En France, nous avons la Banque Publique d'Investissement, le crédit impôt-recherche, sans parler du Pacte de responsabilité. Cette dimension-là existe et tout ceci est censé appuyer le développement de filières industrielles, notamment dans votre domaine.

Clément CAZALOT

Mon point de vue, c'est qu'il faut arrêter avec les lois et les aides à ne plus en pouvoir. Le temps qu'un entrepreneur consacre à remplir une demande de crédit impôt-recherche serait plus profitable à l'entreprise s'il le consacrait à chercher un client. On a créé un système qui met sous perfusion une partie de l'économie. Ce sont des aspirations tout à fait différentes et qui sont louables mais on permet à un tissu économique de survivre alors qu'il n'a plus de réalité économique sur un marché mondial... Je me marie en France ce samedi, ma vision n'est pas celle d'un Français exilé aux États-Unis. Je ne suis pas un expert du Parlement européen. S'agissant de la législation, de la protection des données, de la neutralité du Web, il y a un sujet qui intéresse la commission. Pour la partie économique, j'aurais tendance à suggérer de ne rien faire, de laisser les acteurs émerger, de laisser les États investir dans l'éducation sur le long terme, d'arrêter d'imaginer des lois protectionnistes qui empêchent les étrangers de venir en France. Sur le Net, il n'y a pas de frontières. Aidez les PME à constituer des clubs. Par exemple, Hexatrust est un groupement de PME qui se sont réunies pour pouvoir être sponsor du FIC et être présentes sur la scène devant vous tous. Encourageons ce genre d'initiative et cessons de fournir des

aides, d'imaginer des lois pour aider des entreprises qui n'en ont pas besoin, qui ont juste besoin de compétitivité et de non discrimination à l'égard des PME.

Amélia ANDERSDOTTER

Je suis d'accord avec MM. RAMON et CAZALOT sur le fait que nous avons une économie globale et que notre manière de traiter les questions d'Internet ne peut se faire par le protectionnisme ou l'incitation explicite à acheter européen. La France et l'Allemagne ont soumis Google à une amende, demandant de fortes sommes à titre de rétribution pour les journaux et les éditeurs. Cela contribue à maintenir une concurrence sur le marché. Je voudrais revenir à une idée lancée par McAfee. J'ai eu besoin de huit mois pour réaliser pourquoi cette idée s'est imposée au parlement européen. Il s'agit des labels de confiance. Nous avons beaucoup parlé de confiance. La commission européenne a effectué des recherches sur les labels de confiance. C'est cher et compliqué sur le plan technique. Ce n'est pas très facile à utiliser. Des études viennent confirmer ces conclusions. Pourtant, malgré l'argent investi dans ces études, on revient à cette idée qui est attractive, semble simple mais est compliquée. Alors que McAfee et Symantec font du lobbying à Bruxelles, de nombreux membres du parlement ne lisent pas les rapports de leur propre institution. C'est une honte. Je pense que nous devrions plutôt, en Europe, définir la sécurité des réseaux et de l'information comme un objet intéressant les consommateurs. Il faut introduire une notion de responsabilité, que les entreprises qui font du mauvais travail soient responsables de leurs résultats. Il faut introduire, dans une certaine limite de temps, une obligation de réparation de telle sorte qu'il y ait toujours un responsable pour régler un problème lorsqu'il survient. L'Union européenne serait le premier territoire au monde qui le ferait à une large échelle. Cela permettrait aux gens de savoir qui appeler quand les choses ne marchent pas, que l'on soit une PME utilisant des services informatiques ou un citoyen européen ou seulement quelqu'un sur le territoire européen. Si les choses ne marchaient pas, vous sauriez vers qui vous tourner pour les faire remettre en route. Actuellement, il nous manque la responsabilité en matière de sécurité informatique. Nous essayons de remplir ce manque avec les militaires. Je crois que nous devrions plutôt envisager les choses de manière plus libérale.

Thierry GUERRIER

Sur cette dimension que vous évoquez, sur les essais pour trouver des outils européens en matière de sécurité, je vois défiler les questions de la salle à travers Twitter. Une suggestion, par exemple, consisterait à ce que l'UE pousse à l'émergence d'une major européenne de cyberdéfense, comme l'est Airbus pour l'aéronautique, qui mettrait en commun de grands experts de Suède, d'Allemagne, de Grande-Bretagne ou de France...

Amélia ANDERSDOTTER

Le problème est que les Européens ne se font pas confiance entre eux. Les citoyens, les États européens ne se font pas confiance. Il nous manque, sur le plan politique, la confiance qui a été soulignée par notre amie finnoise qui est si importante pour bâtir la collaboration. De plus, les entreprises de cybersécurité deviennent souvent, pour ne pas dire toujours, des entreprises de cyber insécurité. Des agences gouvernementales de sécurité, en Europe, achètent des chevaux de Troie pour infecter les ordinateurs de personnes privées considérées comme malveillantes. Un cheval de Troie, sur Internet, c'est normalement utilisé par les voleurs. Ce type de programme ne devrait être financé ni par des agences de sécurité, ni par des agences de renseignement. L'Union européenne pourrait vraiment faire beaucoup pour faire cesser ce non-sens. Si l'Union européenne était capable de comprendre qu'Internet est un outil de paix, de camaraderie, d'aventure et d'amitié et non un outil de guerre, ce serait bien. Mais, c'est le problème, nous ne sommes actuellement pas capables d'avoir ce genre de direction politique. Je me demande d'où peut venir cette direction politique et je serais ravie de voir qu'elle vient de la France.

Thierry GUERRIER

Madame SALMINEN, Vous êtes directement interpellée aujourd'hui. Cette capacité à faire coopérer des groupes européens qui se font plus concurrence qu'ils ne se font confiance est aujourd'hui l'objet des critiques principales. M. VAN DEN BERGHE, vous voulez également intervenir.

Michel VAN DEN BERGHE

Nous n'avons pas attendu le Parlement européen. Aujourd'hui, les opérateurs européens travaillent ensemble et ont créé une association qui s'appelle O5. Elle regroupe les Allemands, les Italiens, les Espagnols, les Anglais... Elle travaille sur ces problèmes de cybersécurité et c'est Orange qui porte cette partie cybersécurité. L'objectif est de partager les retours d'expérience pour voir comment on peut, au mieux, se protéger. Au lieu de créer des lois, donnez-nous les moyens de pouvoir lutter. La NSA a des moyens budgétaires énormes. Si les budgets européens se regroupaient, on aurait 30 % du budget de la NSA, on pourrait déjà se défendre un peu. Ce n'est pas le Parlement européen qui va nous aider avec des lois. Nous ne sommes pas dans le gentil pays de Candy, il faut se défendre contre des agressions. Il faut apprendre à se défendre et à lutter contre la cybercriminalité, en collaborant entre les différents acteurs et en n'ayant pas peur de porter plainte. Dans l'affaire du câble sous-marin reliant la France à l'Afrique du nord et à l'Asie, piraté à des fins d'espionnage, Orange a porté plainte contre X. À partir du moment où l'on porte plainte, on commence à mettre en branle des moyens étatiques et juridiques. La collaboration entre acteurs

est encore en développement mais on partage autour de la cybersécurité.

Mirva SALMINEN

Je suis d'accord quand on dit que les gens ne se font pas confiance. C'est pourquoi il est important de se parler. Je n'ai pas les moyens de dire que les choses vont dans le bon sens, c'est le boulot des politiques et des entreprises, qui doivent fournir ce qu'elles ont promis. S'agissant des chevaux de Troie, c'est quelque chose qui nous préoccupe. Il est naturel, dans un sens, que des moyens qui sont utilisés d'une certaine façon se répandent par ailleurs. On en vient à une problématique éthique, qui est plus importante que ce que chacun est capable de traiter seul ou à travers la coopération. C'est aussi une question relative au budget. Au niveau européen, par exemple, cela a déjà été abordé. Certains acteurs de la société devraient réaliser que c'est aussi leur travail que de veiller à la cybersécurité. Les entreprises devraient prêter davantage d'attention à la manière dont leurs employés sont formés à ce sujet, à la manière dont ils se comportent sur internet. Les gouvernements devraient aussi jouer leur rôle dans ce domaine.

Philippe RAMON

Je suis d'accord avec ce que disait M. CAZALOT sur le fait que la réglementation ne constituera pas la solution. C'est une question de culture. Or la culture entrepreneuriale européenne est différente de celle des Etats-Unis. Créer une filière c'est créer les conditions pour que se développe une culture entrepreneuriale dans le domaine cyber. La cyberdéfense est aussi un comportement au quotidien. L'ANSSI a édité un guide de l'hygiène informatique. Cela relève de l'hygiène : quand on sort de chez soi on ferme la porte. Quand on sort de certaines pièces, on se lave les mains... La Délégation est en train de diffuser un recueil de 22 fiches pratiques de sécurité économique au quotidien. C'est s'assurer que les clefs que l'on branche sont propres, notamment les clefs publicitaires, c'est utiliser des mots de passe suffisamment robustes. Cet aspect de culture manque encore terriblement en France

Thierry GUERRIER

Monsieur CAZALOT, je vais vous faire réagir. La salle demande pourquoi ne pas créer un label européen, ne pas recréer un internet européen avec des protocoles spécifiques. On est dans le domaine de la ligne Maginot, mais est-ce crédible ?

Clément CAZALOT

C'est probablement quelque chose sur lequel il est possible de légiférer mais de là à le réaliser... Peut-être à long terme mais aujourd'hui nous sommes dans une réalité. On peut choisir de la nier et continuer à imaginer un internet européen. On peut aussi embrasser la réalité et avancer, en introduisant les innovations, les éléments techniques et culturels nécessaires pour aller de l'avant. Créer un label européen est intéressant, mais l'impact sur le monde des affaires privées est incertain.

Thierry GUERRIER

Alors que Google est devenu quasiment le moteur unique, facilité essentielle pour ne pas dire service public, l'émergence d'un

Google européen vous paraît-elle impossible pour les raisons que vous venez d'énoncer ou est-elle réalisable ?

Clément CAZALOT

On a déjà essayé à plusieurs reprises. Il y a eu de l'argent public et des fonds privés investis dans ce projet. Exalead a fini par être racheté par Dassault pour devenir un moteur d'entreprise. C'est une alternative franco-française à la recherche sur Google. Est-ce un problème que Google indexe le Web et fournisse des résultats ? À titre personnel et d'utilisateur du Web ça ne me pose pas de problème. À titre intellectuel, je peux concevoir que ça pose problème mais la réalité c'est qu'aujourd'hui tout le monde l'utilise. Créons des outils qui construisent sur cet écosystème-là plutôt que d'essayer de créer notre écosystème spécifique. On a essayé de créer un filtrage français de la propriété intellectuelle, on a créé HADOPI. C'est une loi, un ensemble de commissions ont été créées pour un but technique impossible à atteindre, nous le savons tous. Pour cela on a injecté de l'argent public pour quelque chose qui n'avait aucune réalité économique. C'est franco-français... Allons plutôt de l'avant !

Amélia ANDERSDOTTER

Je suis heureuse d'entendre que mon camarade français, de l'autre côté de la table, ne croit pas, lui non plus, qu'il puisse exister une protection juridique de la propriété intellectuelle sans moyen technique de la faire respecter. Si ce moyen existait, je m'y m'opposerais par ailleurs... Je crois que tout le monde n'utilise pas Google. Google a évidemment intérêt à sa plus large propagation, mais ce n'est pas le cas partout. En République tchèque, il existe Seznam, qui est le moteur de recherche le plus utilisé. Il est géré localement, il est entièrement en langue tchèque et il semble que les Tchèques l'apprécient. C'est le parfait exemple d'un moteur de recherche construit par les Européens et qui apporte un service aux citoyens européens. Pour ma part, j'utilise Ixquick, qui est basé et développé aux Pays-Bas. C'est celui que je préfère, j'en aime bien le logo. Quand je choisis des applications, je suis plutôt superficielle... En France, vous avez le projet open source appelé YaCy qui est un moteur de recherche distribué qui, s'il était étendu à toutes les administrations françaises, pourrait avoir un index réellement important et utile. C'est exactement le genre d'innovation que nous encourageons dans notre secteur public. Avec une communauté paneuropéenne et peu américaine. Si la France souhaitait avoir une stratégie digitale nationale, il faudrait déjà regarder ce qui se fait au sein des pays de l'Union et s'intéresser d'abord aux technologies Peer to peer, domaine où les Américains ne sont pas aussi bons que les Européens. Une stratégie industrielle pour l'Europe doit se consacrer aux domaines où sont nos points forts. C'est notre grand défi.

Clément CAZALOT

Pourquoi les Tchèques utilisent-ils un moteur tchèque ? C'est parce qu'il est meilleur que Google et qu'il fournit une meilleure réponse à leurs besoins !

Amélia ANDERSDOTTER
En Allemagne, ils ont fait une loi spéciale juste pour pouvoir taxer les services d'agrégation des journaux. Il s'agit de récolter des taxes qui peuvent être redistribuées ensuite aux éditeurs. En France également, Youtube et Google paient 60 millions aux journaux nationaux. Google peut supporter ces coûts. Google n'est pas pour une réforme du copyright en Europe car elle est la seule compagnie au monde qui peut traiter avec les 28 formats nationaux de protection de la propriété intellectuelle. C'est son intérêt de conserver en face d'elle une Europe fragmentée.

Clément CAZALOT
Quand vous voyez que le Figaro prévoit dans son budget d'avoir la subvention de Google pour exister l'année suivante, pensez-vous décemment que ce journal va vivre dans le futur ? En face, le Washington Post et le New York Times commencent à avoir une stratégie digitale et sont rachetés par des entrepreneurs du numérique qui entrevoient à nouveau la profitabilité...

Thierry GUERRIER
L'idée de la sénatrice Morin-Desailly est cependant de considérer que ceux qui, comme Google, ont un rôle de facilité essentielle auraient des obligations de service public. Cette seule idée n'a pas l'air de vous effleurer.

Clément CAZALOT
Le service public est une chose française, européenne. C'est très bien mais dans une réalité économique globale, dans le numérique, on ne peut pas imposer un service public. C'est techniquement impossible. C'est comme vouloir imposer aux voitures de voler par la seule force de la loi : c'est impossible.

Michel VAN DEN BERGHE
On parlait de label tout à l'heure. Pour l'anecdote, prenez la viande bovine. On a créé un label et on a vu le résultat : nous avons tous mangé du cheval...Arrêtons de penser que l'on va s'autoréguler et que l'on pourra imposer des stratégies. Démontrons que nous avons aujourd'hui des technologies qui peuvent rivaliser avec les technologies américaines et faisons en sorte qu'elles soient utilisées par tous. On ne peut pas imposer des lois. Plus on imposera des lois, plus les gens n'en feront qu'à leur tête.

Amélia ANDERSDOTTER
Une partie de notre législation ne convient pas. Nous avons la proposition de loi de copyright, la loi sur le secret des affaires, proposées par la commission, la législation sur les télécommunications, nous avons le débat sur la cybersécurité qui est adapté à un système centralisé... Dans presque tous les aspects du monde digital, l'Europe a une approche centralisatrice alors même que nous ne sommes pas bons quand nous centralisons. Pourquoi s'étonner que nous ne réussissions pas ? Pour moi, nous avons besoin d'une politique industrielle qui fasse l'effort sur la décentralisation et la distribution, où nous sommes bons. C'est une question de choix.

Mirva SALMINEN

J'apprécie un grand nombre des commentaires qui ont été faits ici, notamment ceux relatifs à une politique de protection excessive. Pour moi, construire une sorte de « forteresse Europe » n'a pas beaucoup de sens. Tant que les gens ne feront pas confiance en la technologie, ce sera difficile. Nous avons besoin de la confiance.

Philippe RAMON

S'agissant de la confiance, on revient sur des questions culturelles. Le problème ne se résoudra pas avec des textes législatifs. Pour faire évoluer l'attitude au quotidien, l'esprit entrepreneurial, il faut mettre en place des conditions adaptées. Sur la protection, il faut que les magistrats réalisent à quel point les attaques sont graves et qu'ils décident des sanctions qui soient véritablement dissuasives. Sur l'impérialisme, M. CAZALOT disait que nous sommes tous égaux devant l'économie et qu'il n'y a pas besoin de lois. Aujourd'hui, ce n'est pas tout à fait le cas, certaines lois sont appliquées différemment pour les Américains et les non-Américains. Cela relève d'un certain impérialisme et il faut que l'Europe arrive à y trouver une solution.

Clément CAZALOT

Aux États-Unis, Prism est hors la loi car il est illégal d'espionner des ressortissants américains. Il n'y avait pas de cadre légal pour le faire mais ils l'ont fait... D'autre part le numérique est mal compris par les législateurs. On a eu un président de la République qui parlait de « mulot » et une députée qui parlait d'Openoffice en croyant que c'était un firewall...On parle aujourd'hui de sujets nouveaux et évolutifs. On apprend tous les jours dans le domaine et on parle de créer des lois sur un sujet perpétuellement mouvant. Le vrai investissement pour le futur est de ne pas discriminer les PME au moment de l'achat public. Que les agences nationales regardent au moins les PME avant d'aller acheter à l'étranger. Appliquons une sorte de Small business act à la française. Continuons à former des élites technologiques et gardons les en les incitant à rester en France, en introduisant des cours d'entrepreneuriat.

Michel VAN DEN BERGHE

Je ne suis pas d'accord avec ce qui vient d'être dit. Aujourd'hui au FIC, deux ministres sont venus, on sent que de plus en plus de personnes et d'entreprises viennent participer. Il y a une vraie prise de conscience. Les politiques s'en mêlent et commencent à en parler. Les grands patrons d'entreprise prennent conscience qu'il faut promouvoir la cybersécurité.

Thierry GUERRIER

Merci à tous et à demain pour la prochaine plénière sur l'identité numérique.

P3 – Identité numérique : quelles stratégies pour les États

Participants

Modérateur : Thierry GUERRIER, Journaliste,

Daniel LETECHEUR, Program manager Infosec, FPS FEDICT, Royaume de Belgique.
Étienne GUEPRATTE, préfet, directeur de l'agence nationale des titres sécurisés. République Française.
Mathieu JEANDRON , chef du service stratégie et urbanisation, adjoint au directeur, secrétariat général pour la modernisation de l'action publique, République Française.
Milena HARITO, ministre d'État chargé de l'innovation et de l'administration publique, République d'Albanie.
Jaan PRISALU, Directeur Général, Estonian Information System Authority, République

Thierry GUERRIER

Notre approche de la question du traitement de l'identité numérique reposera sur la comparaison des stratégies retenues par trois États : l'Estonie, l'Albanie, la Belgique et celle des choix français. Pour cela nous allons bénéficier, outre celle de Milena HARITO, de l'expertise de Daniel LETECHEUR, chef de projet à la FEDICT, agence chargée de la mise en place de l'identité numérique en Belgique, de monsieur Mathieu Jeandron, du secrétariat général de l'administration publique française, de monsieur le Préfet Étienne GUEPRATTE, directeur de l'agence nationale des titres sécurisés et enfin de monsieur Jaan PRISALU, directeur des systèmes d'information d'Estonie.
Madame HARITO, nous allons commencer notre exploration avec vous. Nous bénéficions effectivement de trois exemples étrangers et de l'exemple français ce qui nous permet d'établir un État des lieux et des perspectives.
Madame, vous avez fait vos études à Tirana et vous les avez poursuivies en France où vous avez obtenu un doctorat et notamment travaillé avec France Telecom. À votre retour en Albanie, vous avez été élue au parlement puis nommée ministre et dans vos prérogatives vous avez à traiter de l'identité numérique. Pouvez-vous nous éclairer sur la façon dont s'est posée la question en Albanie.

Milena HARITO
Je voudrais tout d'abord vous remercier pour votre invitation au FIC auquel je participe pour la première fois ainsi que de celle de Monsieur Valls
L'Albanie est un petit pays qui a connu une dictature forte, jusqu'en 1990, qui était du type nord-coréen. Les premières élections ont eu lieu en 1991. Nous avons connu une transition démocratique compliquée. Les partis politiques comme les citoyens n'avaient pas confiance dans les processus électoraux. Il y a eu rapidement un consensus pour la création d'une carte d'identité sécurisée qui permette d'identifier très clairement les électeurs. C'est la raison essentielle pour laquelle les trois millions d'habitants de notre pays disposent d'une carte d'identité à puce qui a été déployée de 2005 à 2009. Cette opération s'inscrit donc dans un contexte historique de nouveaux processus électoraux et d'une grande méfiance par rapport à la composition des listes électorales et aux fraudes massives qui avaient marqué les premières élections.
Cette décision s'est établie, avec un consensus, vers les années 2000. Il a fallu encore 10 ans et les premières élections en 2013 pour qu'elle soit totalement mise en œuvre. Pour le moment, la carte ne permet pas d'accéder à d'autres services. Par contre, nous disposons tous des passeports biométriques. Cela était nécessaire du fait des contraintes imposées dans l'espace Schengen pour l'obtention de visas.

Thierry GUERRIER
Pouvez-vous nous éclairer sur les motifs du choix de la société et du cahier des charges ?

Milena HARITO
Les premiers éléments du cahier des charges ont surtout porté sur une solution pas trop chère, fortement sécurisée et distribuable partout du fait d'un contexte géographique difficile avec un relief montagneux et une infrastructure routière perfectible. Le projet a été monté en une année avec une distribution sur tout le territoire par des bureaux pour un prix inférieur à 10 euros qui constituait un paiement du service. La carte doit pouvoir offrir d'autres services publics. Elle sert pour toutes les identifications comme une carte de santé.
Il y a un besoin fort d'une identification émanant des citoyens. Il existe une différence dans les relations entre les citoyens et l'État selon qu'il est fort ou faible. Les citoyens d'un État faible ne lui font pas confiance et il reste toujours une arrière-pensée de fraude. Par exemple, en Albanie, depuis 4 à 5 ans, 100% des appels d'offres sont électroniques. C'est un des premiers pays au monde à avoir promu cette pratique de transparence en matière d'appels d'offres. Pourtant, ils suscitent toujours une méfiance des participants. Ces exemples montrent le besoin d'une identification forte.
Un autre exemple : en France, la

déclaration des impôts se fait en ligne avec un mot de passe et un numéro d'identification fourni par l'administration fiscale. Par contre, on ne reçoit plus comme il y a trois ou quatre ans un certificat. Dans un État fort, l'idée sous-jacente est que le citoyen a toujours la capacité d'un recours et de remédier à un dysfonctionnement. Dans un État faible, sans relation de confiance, on a besoin d'un certificat pour tous les avis officiels. Ils sont délivrés sous forme électronique dans tous les services gouvernementaux. D'autres exemples concernent un portage de service public avec une authentification par certificats.

Thierry GUERRIER
Dans le cadre de vos prospectives actuelles, quels sont vos objectifs, quels choix de produits et de technologies allez-vous faire, notamment dans le cadre d'un service public ?

Milena HARITO
Le défi est d'augmenter le nombre de services en collaboration avec le gouvernement. Il est nécessaire de développer l'e-commerce donc nous avons besoin d'une identification forte par carte à puce et d'une exploitation par téléphonie mobile du fait d'une bonne couverture nationale.

Thierry GUERRIER
Quel est le degré de confiance des utilisateurs ?

Milena HARITO
Nous sommes en amélioration mais c'est l'accoutumance aux nouveaux produits qui crée la confiance.

Thierry GUERRIER
Monsieur PRISALU, quelles sont les raisons pour lesquelles l'Estonie a été mise dans une situation d'améliorer les processus d'identification ?
La carte est-elle obligatoire ?

Jann PRISALU
Merci pour votre invitation et cette opportunité de m'exprimer ici. La raison qui a poussé l'Estonie à l'automatisation de l'identification est simple. L'Estonie est un petit pays, avec 1,3 million d'habitants seulement. Nous manquons de monde, y compris pour le travail administratif. C'est pourquoi, les charges administratives étant les mêmes que pour un grand pays, nous nous sommes tournés vers l'automatisation de certaines fonctions. Les Estoniens ont besoin de cartes d'identité. En 1994, nous en sommes venus à l'idée que la signature digitale serait un élément essentiel dans le futur et qu'elle attacherait les citoyens à leurs données. Il y a 40 millions de signatures digitales par an en Estonie, soit trois par semaine et par citoyen. La carte est obligatoire.

Thierry GUERRIER
Comment fonctionne ce que vous appelez la signature électronique et quel est son cadre technique ?

Jann PRISALU
La carte sert de stockage pour la clef. La carte à puce est une invention française. Nous devons utiliser de la cryptographie et la carte à puce permet de faire de la cryptographie sans complication pour l'usager. En matière de sécurité, force est de reconnaître que ce sont les solutions simples qui marchent. La signature permet de vérifier qu'un document n'a pas été modifié. Cela suppose une bonne gestion des clefs d'identification.

Thierry GUERRIER
Votre carte d'identité numérique offre-t-elle des services supplémentaires, tous les citoyens en disposent-ils et quels sont vos objectifs ?

Jann PRISALU
Chaque personne résidant en Estonie a une carte. Nous pensons que cette carte doit être aussi simple d'utilisation que possible. La carte en elle-même ne comporte aucune application. Celles-ci sont sur Internet. Par exemple, quand nous conduisons, la carte d'identité sert à justifier à la fois de notre identité et du fait que nous disposons des autorisations pour conduire. Ce n'est pas au conducteur de produire son permis de conduire, c'est le travail de la police, par le biais de la carte d'identité.

Thierry GUERRIER
La carte n'offre pas d'autres services mais permet aux services publics d'être en réseau. Comment cette carte a-t-elle été accueillie par la population et comment envisagez-vous d'améliorer encore ce service ?

Jann PRISALU
La signature et le chiffrement permettent de s'authentifier sur les services en ligne. Quand un gouvernement veut introduire une mesure qui touche les citoyens, c'est toujours difficile. Cela n'a pas été facile pour la carte d'identité. Nous avons d'abord monté le portail gouvernemental pour montrer aux citoyens le type d'informations que le gouvernement possédait sur eux. Nous avons décidé d'être transparents pour combattre la méfiance des gens. Ce système ne restera pas en l'état. Dans le futur, nous aurons beaucoup de moyens mobiles personnels. L'identité sur ces moyens mobiles sera liée à l'identité principale et à son contrôle. Nous avons besoin de cette identité forte et sécurisée pour pouvoir reconstituer une identité en cas de défaillance technique. Pour la vérification d'identité, nous utilisons les informations sur toute la durée de vie de l'identité. Il nous faut donc un enregistrement de ces informations.
Ce qui viendra également, c'est l'identité des entreprises. Nous vivons dans l'environnement du cloud. Nous pouvons utiliser ce cloud et la signature digitale pour conduire notre politique gouvernementale de façon immatérielle. Cela permet d'agir y compris en dehors des limites territoriales. C'est important parce que, sur le plan

militaire, ça nous aide à protéger notre territoire.

Thierry GUERRIER
Merci, nous reviendrons sur cet aspect de l'immigration dans un second temps. Monsieur LETECHEUR, l'exemple belge démarre dans les années 2000. Comment avez-vous commencé et où en êtes-vous aujourd'hui ?

Daniel LETECHEUR
Tout d'abord, je tiens à vous remercier pour votre invitation. En réalité, nous avons commencé dans les années 80 à intégrer la sécurité sociale et à avoir recours à une base d'un registre national qui était partagée entre différents prestataires et uniquement utilisée pour identifier les différents acteurs de la sécurité sociale. Nous avons ensuite constaté que nous pouvions utiliser cette base pour d'autres services et nous avons décidé au début des années 2000 de nous orienter vers une carte d'identité électronique qui nous offrirait plusieurs services : d'une part une identification de personnes comme une simple carte papier et d'autre part une identification au travers de mécanismes électroniques mais également la possibilité de signer des documents avec un certificat qualifié. C'étaient les trois objectifs fixés au démarrage de la carte. Dans un premier temps, nous l'avons diffusée au fur et à mesure du renouvellement des anciennes cartes puis dans une phase d'accélération du processus pour tous les citoyens ayant plus de 12 ans.

Thierry GUERRIER
Où en êtes-vous actuellement car nous sommes dans une autre dimension avec la Belgique ?

Daniel LETECHEUR
Tous les citoyens de plus de 12 ans ont une carte d'identité numérique. Pour les déplacements à l'étranger des moins de 12 ans, il est possible d'obtenir une « kids ID » qui n'a pas de capacité de signature. Nous sommes dans une phase de déploiement pour les résidents belges selon les mêmes concepts, notamment en matière d'accès à la sécurité sociale.
Dans les faits, aujourd'hui, nous sommes en train de déployer de services demandant des authentifications fortes : déclaration fiscale avec consultation en ligne, des solutions pour les entreprises, le domaine notarial, l'e-tendering pour les marchés publics, etc. Il y a également un déploiement qui se fait avec des partenaires privés pour un ticket de train en ligne avec un protocole de vérification que celui-ci a bien été octroyé pour le trajet.

Thierry GUERRIER
Nous trouvons là une dimension d'identification parfaite : signature, capacité d'engagement et de participation au commerce en ligne. Quelles sont les difficultés principales que vous avez rencontrées dans votre démarche ?

Daniel LETECHEUR
Au départ, un problème de distribution et de discrimination entre les titulaires et non-

titulaires de la carte. Une autre problématique a été de montrer la plus-value d'une carte électronique tant que des services n'étaient pas raccordés si ce n'est un aspect pratique et une résistance mécanique.

Thierry GUERRIER
Vous nous dites qu'il y avait une inquiétude et un blocage de la part des utilisateurs ?

Daniel LETECHEUR
Non mais il n'y avait pas dans la phase initiale de services conséquents et de plus l'évocation d'une carte d'identité validée au niveau d'un registre national a entretenu l'idée d'un effet « Big Brother » de contrôle de l'activité. À ce niveau-là, il a fallu rassurer la population sur le niveau de contrôle de la carte d'identité.

Thierry GUERRIER
Quelle a été l'évolution des mentalités et existe-t-il encore aujourd'hui des réticences ?

Daniel LETECHEUR
Les réticences sont abolies et les jeunes générations ont utilisé normalement leur carte électronique. Les derniers recensements ont montré que près de 3 millions de déclarations fiscales ont été effectuées en ligne en s'identifiant par une carte ou un moyen similaire, soit une couverture de 50 à 70% pour environ 6 millions de déclarants et une population totale de 11 millions d'habitants.

Thierry GUERRIER
Quels sont vos choix technologiques ?

Daniel LETECHEUR
Nous sommes partis sur un choix de carte à puce avec des certificats PTI avec une validation des processus de cryptographie par des départements d'université spécialisés pour obtenir une confiance par rapport à la technologie. Les certificats sont valides pour 5 ans et à l'époque pour des clés à 1024 bits. Il est évident qu'il faudra revoir la taille des clés au fur et à mesure des évolutions des solutions.

Thierry GUERRIER
Avez-vous connu des bugs importants ?

Daniel LETECHEUR
A ma connaissance non. Quelques études universitaires ont dénoncé des failles de sécurité qui n'ont pu être démontrées à ce jour. Pas de hacking mais des attaques théoriques d'experts non compatibles avec les technologies actuellement déployées.

Thierry GUERRIER
Quels ont été vos partenaires ?

Daniel LETECHEUR
Nous avons travaillé avec une société belge et une société française pour les cartes à puce. Pour la validation, nous nous sommes appuyés sur des universitaires. Pour le registre national nous avons bénéficié des experts du ministère de l'intérieur. Le service où je travaille, le FEDICT, s'est

occupé du middelware pour permettre aux partenaires un accès sécurisé et d'authentification de la carte.

Thierry GUERRIER
Il y a une dimension d'immigration et de contrôle que nous avons entrevue avec l'Estonie, mais outre la question de l'authentification, il subsiste celle de la garantie de la vie privée et des données personnelles des citoyens. C'est une des questions clés qui se pose aujourd'hui aux autorités françaises représentées par le Préfet GUEPRATTE et monsieur JEANDRON du secrétariat général à la modernisation de l'action publique. Monsieur JEANDRON pouvez-vous nous dire quel est l'état de l'art pour la France car il semble que nous soyons en retard ?

Mathieu JEANDRON
La volonté de mettre en place une carte électronique a été nette jusqu'à un projet de loi d'une carte biométrique, avec des fonctions d'administration, censurée par le Conseil constitutionnel. La raison est intéressante et va guider la suite de notre démarche. Il a été dénoncé un lien trop fort entre les mécanismes régaliens d'identification et l'usage au quotidien de la carte. Il existe également une crainte française d'un « Big brother » évoqué précédemment, une culture qui comprend l'empreinte de la CNIL, un fort cloisonnement entre les ministères. Le deuxième point de débat est celui de l'usage en ligne non déterminé, ce qui était compliqué à démontrer avant la création de la carte. Notre préoccupation a été de régler le sujet de l'identité numérique sans que la biométrie et la garantie de l'identité numérique soient au cœur du sujet et ensuite de s'attacher à travailler sur les usages.

Thierry GUERRIER
Pouvez-vous nous rappeler qui pilote le projet et quels sont ses acteurs majeurs ?

Mathieu JEANDRON
Les acteurs clés sont les ministères régaliens : intérieur et justice. Nous bénéficions de l'expertise technique de l'ANSSI, qui porte également au niveau européen la parole française en matière de partage de la confiance, et également de l'agence nationale des titres sécurisés qui est notre expert et notre opérateur interne. Nous avons une structure de pilotage au niveau du secrétariat à la modernisation. Une direction interministérielle y est l'embryon de la DSI de l'État bien qu'elle soit moins dimensionnée que des structures similaires dans d'autres États. Elle comprend une vingtaine de personnes.

Thierry GUERRIER
Vous êtes donc un des pilotes du cahier des charges. Quelle est la ressource humaine affectée à cette fonction, par exemple en Allemagne ?

Mathieu JEANDRON
Selon les pays, elle comprend entre 100 et 150 personnes. Elles sont près de 750 en Grande-Bretagne, associées aux services du premier ministre.,

Thierry GUERRIER
Quel est l'objectif du gouvernement et quels sont les principes retenus pour réaliser cette carte d'identité numérique ?

Mathieu JEANDRON
Il n'y a pas de projet de Carte d'identité électronique sur l'établi aujourd'hui. Il n'y a pas une personne ou un service qui est en train de concevoir dans l'ombre la carte électronique française.

Thierry GUERRIER
Vous en êtes au stade de la réflexion ?

Mathieu JEANDRON
Non. Dans le contexte, on n'a pas de décision du gouvernement de remettre en œuvre une procédure qui a été censurée par le Conseil constitutionnel. Une fois constatée cette décision négative, nous devons mettre en œuvre des processus car on a un besoin absolu en matière de souveraineté du fait du développement des mécanismes d'identification qualifiés par un certain nombre d'opérateurs privés, notamment nord-américains, qui ont une approche de la maîtrise des données personnelles différente et qui peut poser un certain nombre de questions. Il y a un important investissement des grands opérateurs du numérique dans l'identité numérique, certes pas certifiée mais qualifiée, qui est intéressante pour nombre d'acteurs car elle est facile à intégrer dans des systèmes d'information. Il nous faut donc réagir rapidement sous peine d'être débordés.

La deuxième chose est que l'administration électronique meurt à un moment donné de l'absence de moyens d'identifier l'usager. On fait donc de nombreuses démarches pour dématérialiser des procédures d'accès à des services en se heurtant à la preuve de l'identité avec un processus de rematérialisation.

Thierry GUERRIER
Vous êtes en train de nous dire que du fait de la pression de notre retard, du marché et de la nécessité de faire aboutir notre dématérialisation de procédures, vous êtes dans une posture d'apporter au gouvernement des solutions et la capacité d'organiser des choix politiques ?

Mathieu JEANDRON
Les orientations sont de plusieurs natures. Il faut organiser un écosystème. Il existe déjà en France des identités qui n'ont pas le niveau de certification évoqué dans d'autres pays. Ils sont portés notamment par les banques et la Poste ou ce type d'organismes. L'État a mis en place, avec un certain nombre d'entreprises privées, dont IDENUM, un écosystème de fourniture d'identité privée avec des mécanismes qui sont en cours de définition et un cahier de charges de la qualité de l'identification numérique qui puisse être utile à nombre de secteurs.
Deuxième élément, si on se réfère à une approche sur l'usage, on s'aperçoit que 90% des usages ne requièrent pas une identification certifiée. Prenons l'exemple du compte fiscal. L'identité numérique

utilisée par les impôts pourrait être mise à la disposition d'autres systèmes comme celui des demandes d'allocations car au fond l'identité fiscale est d'un bon niveau. Le point clé est que nous disposons en fait de niveaux d'identification qui ont été réalisés depuis 40 ans mais de manière cloisonnée. Un décloisonnement permettrait de travailler sur une identification commune. S'il existe bien un numéro de sécurité sociale, dont l'exploitation n'est pas autorisée dans les systèmes d'information, il n'y a pas en France de numéro commun du fait de la disparité des modes de gestion, de dénomination ou de l'approche de l'individu au travers des systèmes. Nous avons un certain nombre de sujets à régler en parallèle d'une évolution européenne qui nous pousse vers une identité certifiée de bon niveau et une plate-forme d'échange avec un usager au cœur du système dans un contexte de confiance.

Thierry GUERRIER

Monsieur le Préfet, comment l'agence, alors qu'il n'y a pas formellement d'instructions, aborde-t-elle le problème de l'identité numérique ?

Étienne GUEPRATTE

Pour nous, les choses sont simples. Nous sommes dans l'opérationnel car nous devons produire des titres régaliens : des passeports au nombre de plusieurs millions par an, des permis de conduire aux normes européennes depuis le mois de septembre 2013, le permis « Phaéton » et des visas. C'est l'essence de notre travail que de produire des titres qui garantissent l'identité de la personne qui porte le titre. C'est la raison pour laquelle l'agence existe et qu'elle est adossée au ministère de l'intérieur. C'est à l'État régalien de garantir l'identité numérique qui est une liberté individuelle fondamentale. Le rôle de l'agence est essentiel dans la garantie physique des cartes en liaison avec des partenaires, notamment l'imprimerie nationale, dans la garantie de process, de normes de fabrication sous l'égide de ministères qui sont fortement impliqués dans ces problématiques. Notre travail est d'être sûr que lorsque nous délivrons un titre régalien pour le compte de l'État, qui est aussi un instrument de la confiance numérique, il s'agit d'un titre de reconnaissance de citoyenneté, donc de liberté individuelle et de liberté publique.

Thierry GUERRIER

Où en est la notion d'identité numérique alors qu'il n'y a pas de décision de la créer ?

Étienne GUEPRATTE

Comme l'a dit mon voisin précédemment, on n'a pas obligatoirement besoin d'une carte d'identité numérisée en France puisque nous fonctionnons sans ce titre alors que les usages sont remplis. Quand vous voulez payer une facture, vous voulez réserver une place quelque part ou effectuer une démarche administrative, vous pouvez utiliser un titre régalien qui n'est pas une carte d'identité comme un permis de conduire qui contient une puce

électronique et qui est délivré par l'État, lequel suscite une confiance dans la transaction et le titre remis.

Thierry GUERRIER
Donc, en fait, on a contourné les problèmes de la carte unique en donnant cette mission de garantie à l'agence afin qu'aujourd'hui en France le citoyen dispose d'un moyen d'identification.

Étienne GUEPRATTE
Nos titres sont réputés comme sécurisés car les normes de confection sont sécurisées. Nous pouvons prendre l'exemple du plastique des cartes qui est utilisé selon des normes sécurisées et soumis à des tests systématiques. Nous sécurisons également les normes car nous avons une activité internationale avec l'OASIS1 et à Bruxelles afin de normaliser les titres qui vont être utilisés dans l'espace européen. C'est un travail que nous réalisons effectivement en amont de la production des titres.

Thierry GUERRIER
Je me tourne vers nos amis étrangers. Comment percevez-vous cette complexité du système français ? De quelle argumentation useriez-vous pour convaincre le gouvernement français d'adopter un titre unique ?

Milena HARITO
J'essaierai de répondre à deux niveaux. De manière sérieuse, la France n'a pas besoin de cela. D'un mode moins sérieux, je rappellerai une métaphore qui disait que ce n'étaient pas les traités sur la lampe à huile qui avaient poussé Edison à inventer l'électricité. Il est évident que tant qu'on n'a pas la carte numérique, on n'en a pas les usages. Je vais prendre un exemple comme celui du billet électronique SNCF qui est facile d'utilisation par voie numérique alors que l'on se contentait auparavant d'un envoi postal...Cela est donc une facilitation de la vie.

Thierry GUERRIER
Pensez-vous que l'on peut se passer de ce gap ?

Milena HARITO
Je crois qu'à moyen terme on ne pourra pas se passer d'une identité numérique. On peut vivre toutefois un certain temps sans ce document notamment dans un État régalien fort.

Thierry GUERRIER
Monsieur PRISALU, je vois que vous souhaitez intervenir.

Jann PRISALU
Je ne comprends vraiment pas le processus français. Notre Premier Ministre nous a écoutés, nous les techniciens, et il a pris la responsabilité politique de mettre en place cette carte d'identité. Je lui en sais toujours gré. Si le pouvoir politique n'avait pas appuyé cette décision, les techniciens ne seraient pas parvenus à réaliser ce projet. Une seconde chose importante est que nous étions soutenus par les banques. Ce

sont des grands acteurs. Leur motivation à partager des plates-formes communes avec le gouvernement reposait sur la simple idée qu'en acceptant des procédés de paiement elles n'auraient pas à créer la confiance en la sécurité du système. Avec la signature électronique, vous pouvez certifier les mouvements d'argent, alors même justement que les procédures de justification de la sécurité d'un système sont en général très onéreuses à mettre en place. Les cartes européennes sont utilisables hors des frontières. Avec une carte d'identité belge, vous pouvez créer une société en Estonie. La première année où nous avons ouvert cette possibilité, plus d'un millier de sociétés ont été créées avec des cartes d'identité finnoises. La France a deux voisins qui ont des cartes d'identité numériques, la Belgique et le Portugal. Je pense que cela viendra chez vous aussi.

Thierry GUERRIER

Vous avez vu les réactions de la salle et nous avons des interventions par twitter : en fin de compte, vous exprimez ce qui est un droit à l'identité numérique, car elle facilite la vie. Je vois monsieur JEANDRON que vous n'êtes pas d'accord. Une objection est également soulevée sur le sujet du risque d'attaque d'une identité numérique unique.

Monsieur le Préfet, si le gouvernement le décidait, quelles seraient les mesures utiles à la mise en œuvre d'une carte d'identité numérique ?

Étienne GUEPRATTE

Sur le plan technique, il n'y a aucun problème. Le savoir-faire français existe et je rappelle que nous avons inventé la puce électronique. Nous maîtrisons ces concepts et ces technologies. Le grand challenge qui se pose devant nous est de passer à des systèmes publics qui garantissent l'identité numérique des citoyens par l'intermédiaire des titres sécurisés. Il faut donc qu'un système permette au citoyen, même s'il n'a pas de titre sécurisé, de s'identifier facilement. C'est un projet, sur lequel nous travaillons avec les services de Mathieu JEANDRON, que nous appelons l'identité numérique mobile. Nous avons lancé un marché public et je pense que nous allons pouvoir démarrer vers l'été 2014 un projet qui puisse permettre à un usager utilisant un smartphone mobile d'être sûr que sa puce recèle une identité garantie par l'État par un système de passerelle d'informations de données d'un titre vers le téléphone en question. On travaille là-dessus ce qui permet d'avoir une garantie d'une manière plus simple et pratique auprès des usagers. Donc on passe d'un système à un autre.

Thierry GUERRIER

Si je vous comprends bien, la stratégie est non pas de revenir à l'idée de l'objet physique de la carte d'identité mais d'avoir une identité numérique, dont vous nous aviez à peu près décrit le processus, à laquelle on pourrait faire référence en allant sur internet, chez un commerçant, en utilisant notre portable et qui serait notre

carte d'identité virtuelle.

Étienne GUEPRATTE
Ce ne serait pas une carte d'identité électronique mais une sorte de certificat garanti par l'État qui permettrait à l'usager d'être sûr d'être identifié.

Thierry GUERRIER
C'est une information considérable. Où en est-on de ce processus et selon vous quelles sont les échéances pour obtenir ce certificat ?

Étienne GUEPRATTE
Tout d'abord, je ne sais pas si ce certificat sera obligatoire. Tout cela n'est pas encore défini, nous sommes en train de réfléchir sur la technologie même et l'application informatique permettant de le faire. On a effectivement un marché devant nous que nous allons exploiter dans les mois qui viennent mais c'est une piste possible car on peut s'interroger sur la nécessité de détenir une carte nationale d'identité. Le support n'est-il pas un certificat lié au monde de l'internet permettant d'avoir une garantie dans une sorte de coffre-fort qui serait à l'extérieur permettant une passerelle avec un titre ?

Thierry GUERRIER
Une sorte de cloud français dans lequel serait recevable ce certificat en fait dématérialisé.
Monsieur PRISALU, d'un mot on va conclure si vous le voulez bien.

Jann PRISALU
Je voudrais rappeler une chose. Les bases de ces authentifications sont toujours secrètes. La méthode d'authentification conduit à utiliser le secret mais ne le révèle pas. La carte virtuelle et la carte réelle en lesquelles vous avez confiance sont en quelque sorte un serveur central qui contient toutes les informations dont vous avez besoin.

Thierry GUERRIER
Monsieur JEANDRON, que répondez-vous à cette objection ?

JEANDRON Mathieu
Il y a un débat mais l'enjeu est la centralisation des données et l'objet de sécurité. Concernant le deuxième lien, on parle d'une identité numérique délivrée par l'État et à côté de cela on se heurte à des réactions au décloisonnement des systèmes d'information des administrations. Cela ne veut pas dire que toutes les administrations échangent toutes les données sur tout le monde à l'insu des individus. On a trouvé des solutions pour expliquer et mettre en transparence complète vis-à-vis de l'usager tous les transferts d'informations entre une administration et une autre autour d'un cockpit à disposition de l'usager. En pleine maîtrise de ses données d'identité qu'il gère et met à jour, il organise le transfert

aux différentes administrations. C'est là où on rejoint le besoin d'un outil technique. C'est cela décloisonner.

Thierry GUERRIER
C'est avoir son propre cloud de citoyenneté.

Mathieu JEANDRON
Exactement, changer, c'est organiser l'administration autour de l'usager et non autour de sa propre organisation. C'est la raison pour laquelle il faut une identité numérique car on a effectivement besoin d'un moyen de se faire reconnaître de la même manière par les administrations et de gérer finement les droits d'accès d'une administration à une autre administration et de la garantir fortement.

Thierry GUERRIER
Je me tourne vers nos amis étrangers. Comment réagissez-vous à cette idée que finalement la France n'est pas si en retard ? Malgré la réserve de la nécessité de garder en silo les informations et de ne pas transmettre trop d'informations, pour respecter les citoyens, la réflexion sur ce cloud et sur des outils de certificats semble pertinente.

Daniel LETECHEUR
Je crois que nous avons eu le même débat sur ce sujet : peut-on disposer d'un identifiant unique et partager les informations entre les différentes administrations ? C'était la première question et la deuxième question repose sur les mécanismes qu'il faut mettre en place pour s'assurer qu'il n'y a pas d'échanges d'informations indus, que l'information soit utilisée correctement et qu'il soit procuré à l'usager une plus-value, c'est-à-dire une démarche facilitée par rapport à l'administration. On est parti sur une centralisation de l'information, chaque ministère étant responsable de sa partie d'informations avec une consultation par le citoyen pour qu'il puisse voir quelle information a été utilisée et dans quel contexte. Il lui faut donc une capacité de se connecter à son dossier et déterminer une traçabilité des actes qui ont été faits.

Thierry GUERRIER
Je vous ai posé la question, monsieur GEPRATTE, sur la dimension technique. Vous me dites que c'est à l'étude. En conclusion, quelles sont vos échéances pour fournir au gouvernement les éléments lui permettant de trancher ? 5 ans, trois ans ?

Étienne GUEPRATTE
Non, ce projet particulier sera visible en septembre 2014 pour en discuter entre nous et voir si les ministères sont volontaires pour développer cette application. Pour le moment nous en sommes aux concepts, une piste intellectuelle qui mérite d'être approfondie.

Thierry GUERRIER

Merci à tous, merci madame la Ministre d'avoir accepté notre invitation, merci monsieur PRISALU d'être venu d'Estonie, monsieur LETECHEUR de Bruxelles et de votre présence dans ce carrefour lillois du FIC. On a pu constater cette année que le nombre de participants et l'intensité des débats sont des éléments du succès de cette manifestation.


TEOPAD. Sécurisez v
sensibles sur sma
Magasin d'applicat
Solution économique
Solution de sécurité
mobile innovante
15:4
Pour en savoir plus, scannez le
flash code ou rendez-vous sur
thalesgroup.com/teopad ou
contactez-nous au +33 (0)1 46 13 22 29


os données
rtphones et tablettes.
ions sécurisées
Large choix d'applications
Convivialité
Mar
25/0
Play Store
Maps
S Calendar
S Note
Readers Hub
Messagerie
Applications
Internet
Contacts
Téléphone
THALES
Together • Safer • Everywhere

A1 – Monnaies virtuelles, victimes des pratiques criminelles ?

Intervenants :

Jean-Luc DELANGLE, CREOGN,
- Erik BARNETT, Attaché, Homeland Security Investigations,
- Laurence DANIEL-PICO, Responsable de la cellule d'analyse stratégique, TRACFIN,
- Barbara LOUIS-SIDNEY, Consultante cybersécurité et droit des nouvelles technologies, CEIS,
- Myriam QUEMENER, Magistrat.

Résumé des interventions :

Les monnaies virtuelles, innovations technologiques majeures de ces dernières années, sont un moyen d'échange de valeurs, rapide, facile d'utilisation et échappant à tout contrôle d'autorité. Ces atouts sont plébiscités tant par les internautes que les cybercriminels qui les utilisent dans le cadre de leurs activités illicites, telles que le blanchiment d'argent notamment. Une réglementation mondiale des monnaies virtuelles est nécessaire tant dans la lutte contre la cybercriminalité que dans la mise en œuvre d'une innovation technologique majeure. Avec un meilleur contrôle, la confiance dans ces monnaies virtuelles pourra alors seulement être instaurée et permettre la mise en place d'un nouveau système financier plus sûr et plus accessible.

Face au système financier traditionnel, qui actuellement semble atteindre ses limites avec la crise mondiale que connaissent un certain nombre de pays, une innovation technologique pourrait être une alternative à la crise financière et à la défiance qui accompagne désormais le système traditionnel. Les monnaies virtuelles – à l'image du Bitcoin – représentent des moyens d'échanges peu coûteux, anonymes, faciles d'utilisation. Cependant si ces bitcoins sont accessibles à tout internaute, ils le sont aussi à la cybercriminalité qui profite de ses lacunes : notamment l'absence de contrôle. La confiance, fondement de la valeur des monnaies, doit donc passer par l'instauration d'une réglementation des monnaies virtuelles afin de protéger les utilisateurs et leur permettre de profiter de l'immense opportunité que représente cette innovation technologique.

I. La monnaie, un concept en évolution :

Ayant accompagné le développement des sociétés humaines, la monnaie a évolué au fil des siècles. Aristote, dès l'Antiquité, en définit trois fonctions majeures : un étalon de mesure de valeurs, un instrument d'échange et une réserve de valeur. De l'utilisation des coquillages à celle des comptes bancaires, la monnaie s'est progressivement dématérialisée. Différents types de monnaies coexistent désormais. La monnaie électronique est un bon d'achat, un coupon représentant une créance, permettant d'utiliser la monnaie traditionnelle sur Internet. La monnaie virtuelle, quant à elle, a une réelle existence sur Internet à l'instar de Perfect Money. Elle correspond à un fonds attribué dès sa création générant par la suite son propre circuit financier. Si la monnaie virtuelle reste liée au dollar, ce n'est pas le cas des crypto-monnaies (comme le Bitcoin). Totalement indépendant, le Bitcoin est décorrélé du système traditionnel. Indexé sur aucune valeur, il se génère par lui-même et peut s'échanger contre des devises virtuelles ou réelles. C'est cette absence de contrôle qui est exploitée par la cybercriminalité.

Les utilisateurs du Bitcoin voient dans cette nouvelle technologie, créée pour échapper à la régulation d'un système financier traditionnel en proie à la défiance, un placement fiable et décentralisé. Cependant la vulnérabilité de cette monnaie face aux cyberattaques (malwares) et son utilisation croissante par les cybercriminels sont génératrices d'une perte de confiance rendant le Bitcoin extrêmement volatile et peu fiable. À l'instar de Liberty Reserve, utilisée à des fins illicites, le Bitcoin, victime de son succès auprès de la cybercriminalité, pourrait faire l'objet d'une fermeture par le gouvernement américain. Or cette crypto-monnaie est une réelle innovation technologique qui présente des atouts certains.

II. La fiabilité relative de Bitcoin pour la cybercriminalité:

Utilisée sur les black markets, la crypto-monnaie, simple d'accès et d'utilisation, est un moyen pour les cybercriminels de maintenir leur anonymat et d'agir dans l'opacité sans être inquiétés. Cependant, si jusqu'en 2013 la cybercriminalité privilégiait Liberty Reserve, une monnaie virtuelle qui leur assurait fiabilité et sécurité pour fraude à la carte bancaire, piratage informatique, pornographie enfantine., etc., la mise en accusation des créateurs de cette monnaie a obligé les cybercriminels à évoluer vers d'autres produits moins fiables.

Le Bitcoin n'assure pas un anonymat complet à ses utilisateurs. Étant donné que les transactions apparaissent dans un historique public (blockchain), chaque portefeuille virtuel peut ainsi être tracé. Pour pallier cette perte de fiabilité, les cybercriminels se tournent vers des services leur permettant d'assurer leur anonymat et de blanchir les bitcoins. Ainsi, une initiative appelée Zerocoin est en train de voir le jour pour combler le manque d'anonymat que les utilisateurs de Bitcoin connaissent. Cette nouvelle crypto-monnaie alliée à Bitcoin représente de nouvelles opportunités pour le cybercrime.

III. La nécessité d'un cadre juridique pour réguler les monnaies virtuelles :

La cybercriminalité prend de nombreuses formes et ne connaît pas les frontières étatiques. Le problème ne vient pas de la monnaie virtuelle mais de l'utilisation frauduleuse qui en est faite, or il en existe actuellement plus de cinq cents, soit autant de risques d'escroqueries. Confrontés aux failles que connaît le système financier actuel, un certain nombre d'États tentent par le biais d'institutions et par des lois de lutter contre la cybercriminalité.

Le gouvernement américain, conscient des opportunités que représente la monnaie virtuelle, souhaite aussi réguler son utilisation. À l'origine de la fermeture de Liberty Reserve en 2013, le Sénat américain mène désormais une étude sur le Bitcoin qui, par son succès, est l'une des crypto-monnaies les plus utilisées et donc susceptible d'être privilégiée dans le cadre d'activités illégales.

Lutter contre les activités illégales peut passer par une action sur les échangeurs. En effet, des places ont été créées pour échanger les crypto-monnaies entre elles ou contre des devises réelles. Ces échangeurs, au même titre que des sociétés, doivent s'enregistrer auprès du Département du Trésor Américain. Il s'agit alors de veiller au montant de traces de transactions supérieures à une certaine somme.

En France, le service TRACFIN s'intéresse aux différents flux financiers de sociétés basées à l'étranger et servant d'intermédiaire lors de blanchiment de capitaux. L'usage de la monnaie virtuelle et les flux multidirectionnels des capitaux peuvent rendre la lutte contre la cybercriminalité difficile.
En Allemagne, une réglementation tente d'obliger les fournisseurs de service de paiement à acquérir un agrément auprès d'une autorité de paiement.

Prises isolément, ces réglementations ont un impact trop minime sur une cybercriminalité qui ne connaît pas les frontières. Face à une menace globale, la réponse doit être universelle. Si des obstacles légaux et des conceptions régaliennes persistent, la régulation du système financier doit se faire à l'échelle mondiale car toutes les institutions financières et tous les États sont concernés par ce phénomène de cybercriminalité.

A2 – Cybersécurité et confiance numérique: quels débouchés professionnels ?

Intervenants :

- Sylvaine LUCKX : Mag Securs,
- Alain BOUILLE : Président, CESIN,
- Joël COURTOIS : Directeur, EPITA
- Jean – Noël de GALZAIN : Président Directeur Général ,Wallix
- Guillaume LE MASNE de CHERMONT : Directeur, Mercuri Urval

Résumé des interventions :

Le RSSI opère sur toute une gamme de métiers en fonction de la taille de l'entreprise. On constate une pénurie de cette ressource et une difficulté pour identifier clairement ses fonctions et les qualités requises pour les remplir de manière transversale au sein de l'entreprise. La mise en place de formations spécifiques, de plans de carrière valorisants et la diversification des filières de recrutement constituent des pistes de réflexion qui permettraient de pallier cette carence fonctionnelle au sein des entreprises.

I – Les problématiques :

Les spécialistes en cybersécurité s'accordent à dire qu'il existe une véritable pénurie de RSSI. Même si les chiffres sont difficiles à obtenir, le besoin annuel s'établirait entre 1000 et 1200 spécialistes sachant que 200 à 300 personnes seulement sont formées chaque année.

Il apparaît que pour les entreprises, les RSSI sont difficiles à recruter mais également à garder. Le profil du RSSI apparaît comme suit : 70% ont plus de 5 ans dans l'entreprise et une grande proportion est titulaire d'un bac + 5. Ces derniers ayant dans leur majorité une formation plutôt orientée vers l'informatique que vers les techniques de sécurité. Concernant la formation, elle va être développée en formation continue. La création d'un Centre de formation continue à l'EPITA devrait répondre à ce besoin.

De manière générale, l'ingénieur RSSI est une denrée rare pour plusieurs raisons : il s'agit d'un débouché mal valorisé, les entreprises étrangères sont très actives dans leur recrutement et, de manière plus générale, il existe une fuite des cerveaux dans le domaine du « digital». Les cabinets de recrutement confirment cette difficulté à recruter. L'exemple de l'EPITA montrant que 20% des étudiants partent vers l'étranger dont 50 % aux États-Unis, est révélateur de cette tendance.

Si l'on s'attache aux profils, on s'aperçoit qu'il existe un véritable problème de nomenclature. Le terme qui apparaît le plus souvent est celui d'expert en informatique. Le profil souhaité par les entreprises s'apparente à la recherche d'un « mouton à cinq pattes » voire à « sept pattes ». Il existe donc un véritable enjeu en matière de référencement. À titre d'exemple, un ingénieur informatique ayant une vision opérationnelle des choses est recherché tout comme d'ailleurs des ingénieurs commerciaux. Dans ce métier plus que dans tout autre, une constante apparaît : la nécessité de se remettre en question de manière permanente.

II - Des solutions :

Face à la pénurie de spécialistes, les entreprises évoluent. Les process et les produits, de plus en plus internationalisés, augmentent ainsi les gisements d'emploi et un certain nombre de sociétés offrent des carrières complètes voire des tremplins pour d'autres métiers. Il y a consensus sur le fait que ce secteur est créateur d'emploi, notamment avec des créations de postes quel que soit d'ailleurs le niveau technique. L'étude des besoins met en évidence la nécessité de créer des passerelles entre les filières RH, communication et RSSI.

La formation RSSI n'intéresse pas que les grandes entreprises, les PME apparaissant

aussi comme un nouveau gisement d'emploi en la matière. On note également des propositions très intéressantes sur le plan international. Une bourse de l'emploi pour les métiers de la sécurité/RSSI devrait bientôt voir le jour. Face à un souci de nomenclature et afin de répondre à la question « de quoi parle-t-on ? », l'ANSSI est en train de labelliser et de qualifier les différents profils afin de répondre à ce véritable enjeu.

À l'heure actuelle, les entreprises cherchent en général des personnes ayant entre 5 et 10 ans d'expérience. Il apparaît important de diversifier le recrutement et de ne pas aller chercher simplement des candidats en sortie d'école. L'idéal est un RSSI ayant un bon sens commercial et possédant la « fibre » humaine. La population des « DUT » est intéressante. Du fait de leur formation, ce sont des acteurs inventifs, créatifs et capables de s'adapter avec des profils d'autodidacte. Les passerelles public-privé constituent également de véritables opportunités ; notamment pour les anciens militaires qui, outre leur expertise, apportent une expérience du management à un moment où le RSSI doit convaincre et pouvoir posséder des capacités commerciales, de marketing et de communication. En effet, le recruteur cherchant avant tout des talents, le passage du public vers le privé est une des possibilités sur ce marché de l'emploi spécifique.

A3 – Cloud et sécurité : comment sécuriser la donnée de bout en bout ?

Intervenants :

– Joseph GRACEFFA : CLUSIR INFO-NORD, Association R&D SSI,
- Cdt Michel DUBOIS : MINDEF, RSSI Service de santé des armées,
- Didier GRAS : RSSI BNP Paribas, membre association CESUN,
- Vincent LAURENS : Responsable sécurité SOGETI-BENELUX,
- Julien LAVESQUE : ITRUST.

Résumé des interventions :

Il est opportun pour une entreprise de participer au Cloud pour des raisons de marché. Cette option stratégique soulève la problématique de la gestion de la donnée, son cycle et sa valorisation. Elle doit bénéficier de l'accompagnement juridique de l'externalisation de la donnée par une capacité d'audit du prestataire et une adaptation aux législations étrangères. Elle impose de disposer d'une ressource humaine interne apte à gérer les phases juridiques et techniques de cette externalisation ou de faire appel à une expertise externe.

I. Une stratégie de la donnée

Le phénomène Cloud s'inscrit dans une géopolitique de la gestion de la donnée. On peut distinguer les Clouds selon la catégorisation : privés, publics ou hybrides. On peut aussi aborder ce phénomène sous l'aspect de trois sphères. La première relève de l'étatique (judiciaire, santé, etc...) auquel certains rattachent le domaine bancaire. Elle est soumise en Europe à des contraintes fortes. Sur cette première masse se joue un enjeu géostratégique qui oppose les Etats-Unis, l'Europe et les puissances asiatiques. La deuxième intéresse les « smart cities » et tous les systèmes de régulation de l'énergie et du transport. Enfin, le troisième ressort des réseaux pseudo-sociaux ou pseudo-publics. Le but des opérateurs est de pouvoir croiser les données de ces trois ensembles dans une option business. La question se pose de s'en préserver et de se prémunir d'une désintermédiation entre l'opérateur et le client. Cela suppose le respect de certains standards.

En termes de participation au Cloud, on note toutefois une différence de conception et de gestion selon les pays. Certains privilégient le secret bancaire avec des contraintes fortes, d'autres mettent l'accent sur la protection des données individuelles, notamment dans les pays nordiques, ce qui engendre des disparités législatives entre États. La localisation des données est importante quant aux capacités de leur utilisation « marketing » et du droit qui s'applique à leur régime de gestion et de stockage. Un pays émergent comme Dubaï, qui part d'une structure vierge, a totalement intégré cette dimension Cloud sans que l'on sache si cela est bénéfique.

II. L'utilité du Cloud :

Les entreprises ont une obligation d'être présentes sur le Cloud pour conserver une position sur les marchés. Ce choix stratégique implique une analyse du risque, une méthodologie pragmatique et une gestion de la donnée. Il ne faut pas gérer obligatoirement selon le contenant (réseau, base de données) mais plutôt en matière de valorisation des données. Le Cloud est un concept d'hébergement performant, spatialisé et mutualisé qui répond essentiellement à une demande de puissance et de disponibilité des éditeurs. Il permet de réaliser en fait un déport du risque qu'on ne peut gérer en interne et que l'on pourra contractualiser. Il faudra toutefois imposer un chiffrement et des modalités de reporting. La préoccupation sera de s'adapter à une réglementation internationale hétérogène, de déterminer ce que valent les données, de savoir quelle stratégie doit être adoptée par rapport à ces productions et

d'évaluer la consumérisation des données par le prestataire. Cela peut-être considéré comme une menace mais également comme une opportunité, en tant qu'acteur de sécurité, de s'interroger sur sa capacité à prendre la main sur ses propres données. Les investissements internes sont prohibitifs, mais on assiste au niveau international à une mutualisation au niveau des processus « métiers » et une rationalisation au niveau des équipes sur plusieurs pays. Il s'ensuit la mise en place de processus uniques qui sont ensuite réinternalisés au niveau national. Cela suscite une réflexion sur un Cloud privé qui serait maîtrisé et contrôlé. Il est conseillé pour les PME de s'engager vers des Cloud français après avoir vérifié si la société n'est pas une filiale masquée d'une major étrangère. Les entreprises ou les administrations qui en ont le potentiel peuvent évoluer vers un Cloud privé et sécurisé. Les banques optent également pour des data centers « propriétaires » mais il leur faut compter avec des traitements spécifiques ponctuels, gourmands en ressources, qui nécessitent des externalisations temporaires.

III. Un risque à gérer

On peut opter pour le Cloud avec une stratégie claire et une analyse de risque préparée. Il faut disposer de la compétence interne pour la rédaction des clauses contractuelles et de la capacité d'intégrer les données des audits techniques du Cloud, ainsi que les opérations de reporting. Les critères essentiels sont la disponibilité de la donnée et des services, la continuité de l'activité de l'entreprise, incluant un seuil de résilience, et le niveau de mutualisation du risque. Il existe des standards et une capacité d'audit de certains fournisseurs même si on bute sur la gestion de leurs matériels et une production de certifications internes pas toujours probantes. Rien ne vaut un accès à ce qui est pratiqué réellement par le prestataire. Les Européens ont un rôle à jouer dans les processus de certification et peuvent prendre une place significative sur ce marché.

L'externalisation doit faire l'objet d'une approche juridique avec une insertion contractuelle de clauses de sécurité. Il est parfois nécessaire de s'adjoindre les services de cabinets d'études spécialistes des marchés américains ou asiatiques, du fait des législations particulières de ces pays. Le processus juridique doit également prendre en compte les contraintes imposées à l'hébergeur qui gère les plates-formes ex-

ternalisées par une rédaction spécifique des CCTP (cahier des clauses techniques particulières). Il faut toutefois que ces garanties ne remettent pas en cause la viabilité de l'hébergeur pour ne pas perdre le service et les données par son extinction. On doit enfin veiller à ne pas externaliser des données personnelles hors d'Europe.

Les concepteurs des Cloud ont fait évoluer leurs structures vers un agrégat de services. Il convient désormais de faire une analyse juridique de l'utilisation des données traitées par ces services intégrés.
Les règles du marché, la maîtrise des coûts et la volonté des pouvoirs publics ont permis d'évoluer vers un modèle globalement identique, ainsi qu'une normalisation des contrats et des services. Les publications de l'ANSSI sont d'ailleurs une référence en la matière.
On peut toutefois estimer que la réglementation du pays hôte de la donnée doit être prise en compte. Le règlement des incidents doit donc être prévu contractuellement. Cela est conforté par le fait qu'ils doivent être déclarés par l'opérateur et notifiés à la personne dont les données ont été violées. Pour le moment, le contentieux est principalement localisé aux États-Unis, les cas d'espèce étant rares en Europe.

A4 – La sécurisation des communications mobiles

Intervenants :

- Daniel GUINIER (animateur) : Expert cybercriminalité près la cour pénale internationale de la Haye,
- Charles D'AUMALE : Responsable ligne produits sécurité, ERCOM,
- Laurent GIRAULT : Directeur de l'unité opérationnelle Terminaux sécurisés, Bull,
- Pierre Yves GOUARDIN : Conseiller en stratégie de mobilité, Orange Consulting,

Résumé des interventions :

La communication mobile est devenue une pierre angulaire de l'économie mondiale. La question de sa sécurisation s'est imposée comme un enjeu prioritaire tant d'un point de vue personnel que professionnel. L'utilisateur est une cible privilégiée pour un attaquant extérieur. Cette faiblesse liée au facteur humain est aggravée par les failles logicielles et matérielles. Les débats s'inscrivent surtout dans le contexte de l'entreprise, au niveau du Responsable de la Sécurité des Systèmes d'Information (RSSI). Il est proposé d'axer la politique de sécurité autour du maillon jugé le plus faible : l'Homme. Les solutions avancées sont multiples : éducation de l'usager, sécurité native des terminaux et une nouvelle approche sécuritaire en plaçant l'utilisateur au centre du développement de la stratégie de sécurité.

Si la question de la sécurisation des communications mobiles se posait déjà avec les téléphones traditionnels de type GSM, elle est d'autant plus prégnante avec l'adoption massive des smartphones, téléphones dits « intelligents » concentrant à eux seuls la quasi-totalité de nos correspondances (voix, courriels, textes et chats). De plus, la diversité et la multiplication des terminaux mobiles obligent à l'élaboration d'une stratégie de sécurité complexe et adaptée. Quels sont les enjeux ? Quelles sont les solutions existantes ? Quelles sont leurs limites ? L'étude s'inscrira dans le contexte de l'entreprise.

I. La place de la sécurisation des communications mobiles en entreprise

La communication mobile est actuellement présente tant dans la vie personnelle que professionnelle. À chaque fois, l'utilisateur constitue la cible privilégiée de personnes malveillantes. Ces dernières s'appuient à la fois sur les faiblesses logicielle, matérielle et humaine.

Par rebond, la compromission des données personnelles permet l'exploitation des données de l'entreprise. La sécurisation touche donc en tout premier lieu l'utilisateur que le responsable de la sécurité des systèmes d'information appelle « client ». Celui-ci ne veut pas entendre parler technique pour sa sécurisation. Il parle de son environnement : un usage, un besoin fonctionnel, une option d'utilisation. Ce sera donc au RSSI d'assurer une sécurité effective, c'est-à-dire une mise en œuvre d'une sécurité « utilisée » par ses clients.

Depuis ce que l'on appelle la digitalisation de l'entreprise, beaucoup de décideurs sont concernés par la sécurisation des communications mobiles. Pourtant, la sécurisation n'est qu'à la cinquième place des priorités des utilisateurs des communications mobiles. Cela doit être mis en contraste avec l'augmentation depuis 2012 de plus de 100 % des malwares mobiles tous les ans. Il existe ainsi une véritable problématique quant à l'importance que l'on accorde à cette question.

Un autre aspect de la question concerne la relation entre le RSSI et ses clients. En effet, il existe des pressions internes aux entreprises sur les RSSI car les utilisateurs veulent toutes les possibilités d'un téléphone mobile sans sécurité particulière clairement identifiée, celle qu'ils connaissent dans la sphère privée, mais avec la sécurité nécessaire au monde de l'entreprise. La politique de sécurité menée par le RSSI doit prendre en compte ce compromis entre l'ergonomie et la sécurité.

II. Les solutions et leurs limites

L'état de l'art montre que l'optimisation entre sécurité et ergonomie est difficile à at-

teindre pour un RSSI, l'un prenant souvent le pas sur l'autre, mais passé ce constat les solutions proposées sont multiples.

Il existe une réflexion sur la sécurité native, c'est-à-dire une sécurité réfléchie depuis la conception jusqu'à l'utilisation. Cela implique un coût de développement supérieur mais cette solution permet à l'utilisateur de ne pas réfléchir à l'utilisation d'une sécurité, cette dernière étant déjà implantée dans le téléphone. Cela abonde dans le sens de la sécurité ergonomique.

Un autre aspect de la solution est la solidité du chiffrement. Certaines entreprises ont un impératif important à ce niveau car elles traitent des données sensibles. Il existe trois niveaux dans ce marché des données : le plus faible est celui du « bring your own device », ensuite vient la diffusion restreinte et enfin le confidentiel/secret défense. Pour chaque strate, il existe des solutions de chiffrement spécifiques. Néanmoins, il a été soulevé que la limite n'est pas le fait de la cryptographie en tant que telle mais de son niveau d'implantation, par exemple par le choix d'une carte à puce, d'une clé de chiffrement. De plus, il faut voir le chiffrement de la donnée communiquée mais aussi de la métadonnée (c'est-à-dire une donnée servant à définir ou décrire une autre donnée quel que soit son support).

Les protocoles impératifs de sécurité sont également une solution mais montrent très vite des limites. En effet, on peut imposer à l'utilisateur un appareil sécurisé mais il peut, s'il en a la volonté, contourner cette gestion de la sécurité. Ainsi, il a été admis que le client doit être dans la boucle de conception de la solution de sécurisation. Cela passe par le choix du terminal mais aussi par la démarche du RSSI qui cherche à comprendre l'utilisation que va en faire son client. En effet, un mobile ultra-sécurisé laissé au fond d'un tiroir ne sert à rien !

Cette sécurisation passe d'abord par une acceptation de l'utilisateur. On peut prendre pour exemple celui de la mise à jour Apple d'iOS 7. En effet, en trois jours, 70 % des terminaux Apple dans le monde SONT passés à la nouvelle version d'iOS, uniquement sur la bonne volonté des utilisateurs des terminaux. La solution peut aussi venir d'une sécurité discrète, sans que l'utilisateur ne s'en rende compte. Cette sécurité est plus difficile à mettre en œuvre, plus limitée également, mais elle apporte une plus value à l'ergonomie finale.

Il existe un véritable problème d'éducation des utilisateurs des terminaux mobiles en entreprise. Une partie de la solution réside peut-être dans la résolution de cette lacune.

Enfin, une autre solution envisagée est celle du contrôle du matériel utilisé. Cela influencera le choix entre Android, source ouverte, et Apple, source fermée. La compréhension du matériel permet, en somme, d'apporter une solution de sécurisation

adéquate aux problèmes rencontrés.
Il faut savoir que la sécurisation des mobiles emprunte le même chemin que la sécurisation de l'internet, avec dix ans de retard cependant. Il est envisageable à la vue de la ressemblance entre les deux problématiques de s'inspirer de ce qui s'est fait sur le web pour le porter sur la communication mobile, tout en gardant à l'esprit les spécificités de ce secteur primordial pour une entreprise moderne.

A5 – Cyberdéfense, quelles perspectives après le Livre Blanc et la loi de programmation militaire ?

Intervenants :

- Nicolas ARPAGIAN, directeur scientifique à l'Institut National des Hautes Études de la Sécurité et de la Justice,
- Jacques BERTHOU, sénateur de l'Ain,
- Jean-Marie BOCKEL, sénateur du Haut-Rhin,
- Contre-amiral Arnaud COUSTILLIERE, officier général à la cyberdéfense, État-major des Armées,
- Christian DAVIOT, chargé de la stratégie, Agence Nationale de la Sécurité des Systèmes d'Information,
- Patrick HETZEL, député du Bas-Rhin,
- Eduardo RIHAN-CYPEL, député de Seine-et-Marne.
- Fabrice HATTEVILLE : Product Line Manager, Thales,
- Thierry SERVAIS : RSSI, KITS.

Résumé des interventions :

La notion de cyberdéfense est désormais entrée dans le champ législatif via le Livre Blanc sur la défense et la sécurité nationale et la LPM. Les compétences ont été clarifiées et de nouveaux pouvoirs ont été confiés à l'État, notamment via l'ANSSI. Il s'agit maintenant de consolider l'édifice mis en place et de s'interroger sur les évolutions souhaitables s'agissant de notre souveraineté, dans un contexte européen et international qui pèse sur chaque initiative.

I. Une problématique pleinement prise en compte par l'État :

La France a commencé à envisager sérieusement les questions de cybersécurité et de cyberdéfense à partir de 2008. L'année 2013 a vu aboutir deux textes essentiels (le Livre Blanc sur la défense et la sécurité nationale et la LPM). Ceux-ci affirment notamment la place de la cybersécurité au sein des domaines relevant de la sécurité nationale, fixent un cadre précis à l'action de l'État, précisent ses ambitions en la matière et imposent aux opérateurs d'importance vitale un certain nombre d'obligations. Par ailleurs, les capacités de recherche sont augmentées, notamment grâce à l'engagement résolu de la Direction Générale de l'Armement. Un effort de recrutement est consenti en faveur des agences spécialisées afin de doter l'État des outils dont il a besoin. S'agissant plus spécifiquement des armées, le ministère de la Défense a multiplié par trois ses investissements et, dans un contexte contraint, met en place des équipes spécialisées plus étoffées ainsi qu'un plan de formation spécifique. Il a également unifié sa chaîne de conduite des opérations cyber pour apporter une réponse plus efficace aux attaques. La notion de renseignement d'intérêt de cyberdéfense a émergé et il est aujourd'hui pleinement admis que l'espace cyber est un champ de bataille à part entière. La conduite des opérations inclut maintenant logiquement un volet cyber.

Le nombre de cyberattaques augmente tandis que leur niveau de perfectionnement croît sans cesse. L'affaire Snowden a fait prendre conscience aux gouvernements, mais aussi aux populations, des vulnérabilités des systèmes d'information et de l'impérieuse nécessité de changer radicalement la manière dont chacun doit appréhender la menace et adapter ses comportements. C'est en effet dès le niveau individuel que les bons réflexes doivent devenir automatiques. De cette manière seulement il sera possible d'éviter que les salariés reproduisent au sein de leur entreprise des comportements imprudents, voire dangereux, sur le plan de l'intégrité des systèmes d'information.

II. Un dispositif devant évoluer :

Si des avancées majeures ont été faites ces dernières années, la situation n'est pas pour autant entièrement satisfaisante. Ainsi, certains secteurs publics n'ont pas encore pris la complète mesure des enjeux. En matière de formation, l'enseignement supérieur et la recherche ne se sont pas encore mis en position de pouvoir fournir, dans des effectifs suffisants, les spécialistes nécessaires aux entrepreneurs. Ces derniers devraient mieux connaître leurs besoins, de façon à

permettre aux universités et aux écoles d'ingénieur de prendre conscience des débouchés s'offrant aux étudiants. Afin de sensibiliser l'ensemble des professionnels, on pourrait également imaginer, par exemple, que chaque formation d'ingénieur comporte un volet sur la sécurité des systèmes d'information.

En ce qui concerne la mise en œuvre des principes posés par les textes législatifs récents, il s'agit à présent de trouver des modalités pratiques d'application. Cette phase passe par des discussions avec les entrepreneurs et industriels. D'ici la fin de l'année 2014, l'objectif est d'arriver à un corpus de textes qui renforce la compétitivité des entreprises par la réduction de leurs vulnérabilités.

Sur le plan international, il semblerait cohérent qu'un certain nombre d'actions soit décidé et mises en œuvre de manière simultanée afin d'en optimiser les effets. Assurément, une simple juxtaposition de politiques nationales ne saurait avoir la même efficacité qu'une action coordonnée et concertée de la communauté internationale. Or, si certains pays ont adopté rapidement des politiques volontaires et se posent en maillon fort de la chaîne globale de cybersécurité, d'autres sont très en retrait et constituent d'inquiétants maillons faibles. Au sein de l'Union Européenne, un accord global de tous les États membres sur ces questions semble hypothétique. Des progrès pourraient cependant être obtenus en identifiant des sujets bien précis, sur lesquels un consensus serait vite établi et un mode d'action rapidement adopté. Procédant par touches successives, l'Europe pourrait ainsi évoluer, sans heurts et dans des délais raisonnables, vers un état de vulnérabilité réduite. Quoi qu'il en soit, il est fondamental de veiller au contrôle démocratique des démarches engagées. Il ne s'agit pas, en effet, d'opposer les libertés individuelles à la souveraineté nationale. Cette dernière se conçoit d'ailleurs en plusieurs cercles, le premier étant celui de l'individu, le second étant celui des acteurs privés, le troisième celui de l'État, chacun veillant à prendre les mesures de son niveau pour réduire les risques sur ses systèmes.

La bataille est également économique. Si la NSA œuvre au profit de la sécurité des Etats-Unis, elle travaille aussi clairement à protéger les intérêts des entreprises américaines. La France pourrait s'inspirer de cette démarche, en veillant cependant à ne pas verser dans un protectionnisme forcené. Le code des marchés publics, par exemple, est souvent considéré comme un handicap pour les entreprises françaises qui voient des contrats leur échapper au profit d'acteurs étrangers. Un volet de ce code concerne les produits de sécurité, avec des modalités adaptées. Les marchés portant sur les questions de cybersécurité devraient

entrer dans ce cadre qui est plus protecteur. Dans le même ordre d'idée, l'exploitation des sources ouvertes permet bien souvent d'obtenir des renseignements qui intéressent les entreprises. Ces dernières, notamment les plus petites, n'ont pas les moyens de mener cette recherche active du renseignement ouvert. L'État est en mesure de remplir cette fonction, mais il faut reconnaître que les structures actuelles peinent encore à avoir une production satisfaisante. Le délégué interministériel à l'intelligence économique a de grandes ambitions dans ce domaine. Il est désormais d'actualité que les entreprises représentent un intérêt pour le pays et qu'il convient que l'État contribue autant que possible à leur développement.

A6 – Cybersurveillance et vie privée.

Intervenants :

- Claire LEVALLOIS-BARTH, maître de conférences, Télécom Paris Tech,
- Gabriel VOISIN, avocat à la Cour, Bird & Bird,
- Arwaa YORK, Director, York Advisory,
- Neira JONES, Partner at Accourt, Chairman Global Advisory Board at CSCSS, FBCS
- Fabrice HATTEVILLE : Product Line Manager, Thales,
- Thierry SERVAIS : RSSI, KITS.

Résumé des interventions :

Les moyens de communication connectés permettent potentiellement de surveiller et suivre les activités des individus. Que ce soient les États, les entreprises ou les particuliers, nombreux sont ceux qui ont ou sont tentés d'avoir un regard sur les activités d'un individu ou d'un groupe d'individus. Il est essentiel de permettre aux citoyens d'exercer un contrôle sur leurs données personnelles et d'éviter les abus en matière d'accès à ces dernières. La solution passe sans doute par une éducation à une certaine hygiène informatique mais aussi par l'instauration de règles au niveau national ou communautaire (s'agissant de l'Europe).

I. Les données personnelles, objet de convoitise.

Les individus produisent aujourd'hui une masse d'informations à destination du cyberespace. Qu'il s'agisse de données sciemment déposées sur des réseaux sociaux, de données envoyées automatiquement par des appareils connectés (appareils de santé ou de bien-être, électroménager...) ou encore de documents et messages émis sur le réseau de l'entreprise qui les emploie, l'immense majorité de ces informations relèvent de la vie privée.

Ces données, qui pour certaines d'entre elles flottent dans un nuage virtuel, intéressent beaucoup de personnes ou d'organismes. L'État, dans le cadre de la sauvegarde de la sécurité nationale ou de la lutte contre la criminalité, recherche les personnes présentant un danger pour la communauté. Les entreprises cherchent, pour leur part, à améliorer la productivité des employés, à démarcher des clients potentiels et à percer les secrets de leurs concurrents. Certains individus, enfin, cherchent des informations destinées à être revendues ou à faire pression sur une personne ou une entreprise.

La protection de ces données est, de plus, liée à celle de l'identité des individus et à la confiance que ceux-ci peuvent mettre dans Internet.

La protection des données personnelles demande donc, à l'heure numérique, une attention toute particulière.

II. Des dispositifs nationaux de protection de la vie privée très divers.

Selon les pays, la protection de la vie privée peut être prise en compte par l'État de manière plus ou moins sérieuse. D'une manière générale, les Européens bénéficient de dispositions assez complètes, souvent anciennes (en tout cas antérieures à l'avènement d'Internet). Ainsi, la France a adopté la loi informatique et liberté en 1978. Entre autres dispositions, ce texte prévoit des garanties aux salariés en matière de protection de leur intimité sur leur lieu de travail. Ainsi, un chef d'entreprise ne peut installer de système de surveillance des employés et des locaux que sous la triple condition que l'ensemble du personnel en soit informé,que la Commission Nationale Informatique et Liberté soit avisée ou ait délivré une autorisation (selon le type de dispositif) et enfin que le dispositif ait été présenté aux représentants du personnel. Cette transparence s'impose aux chefs d'entreprise sous peine de condamnation au civil ou au pénal. Par ailleurs, toute sanction prise sur la base d'informations récupérées par des moyens non déclarés ou non conformes à la déclaration a vocation à être annulée. En France comme dans d'autres pays, une autorité indépendante est chargée de vérifier la bonne application des principes légaux. D'une manière générale, les pays européens sont bien plus matures en matière de protection des données

personnelles que les Etats-Unis, par exemple, où aucun dispositif de protection comparable n'existe.
Cette constatation s'accompagne logiquement d'un questionnement quant à l'intégrité et la restriction d'accès des données qui sont stockées sur le sol américain. Force est de constater que la technologie a rattrapé puis dépassé les textes historiques européens. Il est par conséquent d'autant plus important pour l'Europe de prendre des mesures de protection de ses ressortissants.

III – Une sécurité à plusieurs niveaux.

L'utilisation des technologies de communication ne peut se développer que dans un climat de confiance. Les usagers doivent pouvoir compter sur une sécurité minimale de leurs données personnelles. Il s'agit d'un challenge pour les services publics qui doivent bâtir un lien de confiance avec les administrés et, ensuite, maintenir cette confiance par une gestion attentive des données collectées. La confiance repose notamment sur une nécessaire transparence. L'internaute doit savoir qui fait quoi avec ses données. Il serait intéressant qu'il puisse bénéficier d'indicateurs clairs en matière de respect de la vie privée afin de savoir exactement le niveau de sécurité offert par les services publics en ligne. De même, l'établissement de mesures de sécurité standardisées permettrait d'aider à l'instauration d'un niveau général de sécurité.
Si la question de l'éducation des usagers à la sécurité est importante, il est également essentiel de développer le niveau de sécurité des objets et appareils connectés dès leur conception. Cette sécurité intégrée à la conception doit également prendre en compte la nécessaire protection de la vie privée. Les citoyens français peuvent d'ores et déjà demander à accéder aux données les concernant auprès d'administrations. Ils devraient pouvoir compter aussi sur un niveau acceptable de sécurité des objets connectés.
S'agissant des entreprises enfin, les nouvelles générations d'outils de protection contre la cybercriminalité intègrent désormais des éléments qui peuvent porter atteinte à la vie privée des salariés. Leur intégration au sein des SIC de l'entreprise doit se réaliser avec précaution. Il est nécessaire de faire une évaluation préalable (Privacy Impact Assesment) qui prenne en compte les dispositions légales du pays concerné en matière de protection des données personnelles et de la vie privée. Cette action doit être menée par le responsable de la sécurité informatique en lien étroit avec les services techniques et juridiques de l'entreprise.


FIC
2014

A7 – Qu'est-ce que cyberespace national ?

Intervenants :

- Gérard de BOISBOISSEL, ingénieur de recherche, Écoles de Saint-Cyr Coëtquidan.
- Jean-Marc BOURGUIGNON, hacktiviste, Télécomix.
- Cécile DOUTRIAUX, avocate, Doutriaux-Vilar & Associés.
- Hervé George LUCAS, Professor at Stockdale Center for Ethical Leadership, US NavaL Academy.

Résumé des interventions :

Une nation se définit par un groupe humain établi sur un territoire délimité par des frontières géographiques et représenté par une autorité souveraine. Or, le cyberespace n'est pas, de par ses caractéristiques intrinsèques, délimité par des frontières physiques. À la matérialité de ces dernières s'oppose le caractère intangible de l'espace numérique, ses données circulant d'un point à l'autre du globe, ses identités virtuelles, ses chemins aléatoires... L'État, qui est l'expression d'une nation, peut faire valoir sa législation sur le cyberespace et mettre en place des dispositifs pour sa sûreté. Cependant, les obstacles à l'exercice de sa souveraineté sont nombreux.

I – La souveraineté nationale sur le cyberespace

Un État exerce l'ensemble de ses pouvoirs : exécutif, législatif et judiciaire à l'intérieur de frontières nationales reconnues par les autres États. Il se défend contre les atteintes à ses infrastructures vitales et à sa population dont il a le devoir de protéger les intérêts.

À ce titre, l'État exerce sa souveraineté sur le cyberespace par l'application de ses lois nationales. Leur mise en œuvre est aisée en ce qui concerne les infrastructures physiques et la couche logicielle car elles sont localisées, rattachées à un territoire et à des juridictions données. Si l'emprise sur les données qui transitent sur le Net est moins importante et moins efficace, il est néanmoins possible de lutter contre des contenus illégaux et des agissements réprimés par le droit national.

En effet, le principe de territorialité s'exerce pour les infractions relatives aux nouvelles technologies, même pour celles commises à l'extérieur, en vertu de critères de rattachement tels que la nationalité ou le domicile de la victime. Conformément à la théorie de l'émission et de la réception, l'État peut agir si une infraction produit ses effets sur son territoire national. Dans les pays démocratiques, la justice peut être saisie ou des accords à l'amiable peuvent être passés d'État à État, pour filtrer ou bloquer des contenus illégaux.

La loi de programmation militaire du 18 décembre 2013 prévoit un renforcement des pouvoirs étatiques sur le monde cyber. Effectivement, sur les quatre mesures relatives à la sécurité des systèmes d'information, l'une dispose que des contrôles de sécurité pourront être effectués à la discrétion du Premier ministre et aux frais des opérateurs par l'ANSSI. Une autre disposition établit qu'en cas de crise majeure, le Premier ministre peut imposer des mesures aux opérateurs.

L'État dispose d'autres leviers pour contrôler et réguler le cyberespace. Ce sont des organismes et services de surveillance publics ou privés pour lesquels il faudrait augmenter le nombre d'enquêteurs spécialisés. Il peut aussi mettre à contribution le « netcitoyen » qui a un rôle de vigilance à jouer, potentiellement au moyen des plateformes de signalement (par exemple, signaler un site pédopornographique, un site djihadiste), tout en veillant à ce que ce citoyen ne se substitue pas aux pouvoirs de justice.

A ce contrôle exercé sur le cyberespace par l'État s'ajoute une obligation de protection des données numériques personnelles de ses citoyens. Des mesures devraient être prises afin de favoriser le développement d'une responsabilité citoyenne. Si une prise de conscience progressive conduit déjà de plus en plus les usagers à modifier leurs comportements sur le Net et à contrôler leurs données sur le Cloud, cette évolution sera facilitée par le développement de solutions nationales d'hébergement et

d'outils de stockage de données dans un cadre local.
L'Europe cherche également à mieux protéger la vie privée de ses ressortissants, avec la mise en place d'un « Schengen » des données. La proposition de règlement « Data Protection » a été votée le 21 octobre 2013 par la Commission des libertés civiles, de la justice et des affaires intérieures et le parlement européen a adopté le projet de règlement le 12 mars 2014, pour une application effective en 2016.

II – Les limites à cette souveraineté

La sphère d'intervention et la capacité de sécurisation de l'État correspondent davantage à une utopie qu'à la réalité. Elle reste effectivement très difficile à mettre en œuvre pour plusieurs raisons.
Les données ne sont pas toujours reliées à un identifiant qui caractérise leur propriété. Elles peuvent être stockées à des endroits différents et être dupliquées. La preuve à charge, obligatoire dans le droit français, est souvent difficile à établir en ce qui concerne les preuves numériques car les actes illicites ne sont pas aisément attribuables à une personne clairement identifiée. Dans le cas des botnets malveillants, remonter à la source de l'agression est complexe. Il existe des moyens techniques, tels que le réseau TOR, qui permettent de crypter et d'anonymiser les données. Le blocage de certaines pages représente une contrainte économique trop élevée pour les fournisseurs d'accès. Enfin, un site interdit et fermé peut réapparaître sur des sites-miroirs, les informations peuvent être hébergées sur d'autres serveurs, comme ce fut le cas pour les télégrammes diplomatiques de Wikileaks.
Les bitcoins remettent également en cause une prérogative fondamentale de l'État, qui est de battre monnaie. Cette monnaie, devenue rapidement populaire auprès des internautes, s'échange en dehors de tout contrôle étatique. Les utilisateurs de ce dispositif se réclament généralement de la mouvance libertarienne dont l'objectif classique est de lutter contre l'intervention de l'État dans le domaine économique. Elle constitue un danger pour la démocratie et induit évidemment un risque important d'activités criminelles à l'instar de la fraude fiscale, des détournements de fonds ou du blanchiment d'argent.
Les entreprises numériques internationales, très puissantes et influentes, remettent également en cause la souveraineté des États. Les échanges et les transactions sont facilités par le principe d'interopérabilité et de nouveaux outils d'anonymisation.
Actuellement on constate la domination des Américains et une extension extraterritoriale de leurs pouvoirs, grâce à l'implantation de câbles et de nombreux opérateurs Internet sur leur territoire. Cette hégémonie, qu'ils confortent par leurs liens

avec l'ICANN, leurs logiciels, leurs outils numériques et leurs nombreux services en ligne vendus dans le monde entier est encore amplifiée par le Cloud. Ils imposent leur législation, même pour les data centers installés hors de leur territoire, par le biais de contrats d'adhésion (pour lesquels la part de négociation est quasi inexistante) qui permettent de contourner la loi nationale devant s'appliquer aux cyberstructures. Depuis 2001, la Loi Patriot Act autorise, au nom de la lutte contre le terrorisme, l'accès aux données sans le consentement et l'information des utilisateurs. Cette collecte, ce stockage et cette analyse des données selon leur pertinence par les organismes internes et externes en charge de la sécurité nationale, soulève la question, dans les régimes démocratiques, du libre consentement des citoyens à l'activité de renseignement, par essence secrète, sur le territoire national.

Les États-Unis ont l'avantage de pouvoir mobiliser une forte ressource humaine et financière affectée à des moyens d'enquête et d'investigation. Nous sommes donc face à un déséquilibre originel de l'Internet et à une dépendance vis-à-vis des États-Unis qui limite la marge de manœuvre des autres États. Instaurer des frontières nécessiterait de contrôler la totalité de flux entrants et sortants ce qui entraînerait des dépenses considérables. Toutefois, devant l'ampleur de l'espionnage pratiqué par les États-Unis, révélée par l'affaire Prism, les autres États semblent réagir par une réaffirmation du caractère national et une volonté de plus grande autonomie de leur cyberespace.

Internet est par nature transnational. Il serait contraire à son esprit et à sa neutralité, un de ses trois principes fondateurs, de lui imposer des frontières. Il reviendrait alors à chaque État d'établir ses propres normes, ce qui enlèverait à Internet sa raison d'être, ralentirait son fonctionnement et augmenterait les risques de conflits. La Chine et l'Iran tentent de mettre en place un Internet de dimension nationale ce qui est techniquement difficile tant le contournement des barrières est possible.

Les nations se confrontent ou s'entendent pour délimiter leurs espaces nationaux propres en mer et dans l'espace. Un parallèle peut être établi avec l'espace numérique. En effet, puisque les États ne peuvent ériger leurs propres règles de manière unilatérale sans remettre en cause le fonctionnement et le fondement même d'Internet, une entente est nécessaire dans le cadre d'une gouvernance mondiale. La Convention de Budapest, ratifiée par 42 pays, concrétise cet effort de coopération. Elle n'est cependant pas toujours appliquée par certains pays signataires. Il existe en effet aujourd'hui davantage de conventions bilatérales de coopération policière ou judiciaire que d'accords multilatéraux.

A8 – Quel avenir pour la convention de Budapest

Intervenant :

- Alexander SEGER : Secrétaire du Comité de la Convention sur la Cybercriminalité et chef de Division de la Protection des données et de la Division cybercriminalité au Conseil de l'Europe

Résumé de l'intervention :

La Convention est à l'origine d'une législation plus forte et plus uniforme de la lutte contre la cybercriminalité, d'une coopération internationale plus efficace entre les partis, d'une meilleure performance de la cybersécurité. Les projets régionaux, CyberCrime@IPA et CyberCrime@EAP ont renforcé les moyens en matière de justice pénale, de stratégie prioritaire, de formation judiciaire et des forces de l'ordre. Cette maîtrise a aussi favorisé le partenariat entre le public et le privé. Elle a été un catalyseur pour le renforcement des capacités de la cybersécurité.

Alors que des profonds désaccords divisent les États, la Convention reste le seul texte international établi sur un consensus international. L'évolution des enjeux et des technologies n'est pas un frein à son application. La coopération technique et l'adoption de protocoles peuvent la prolonger. La Convention reste d'actualité et reste attractive par les coopérations qu'elle favorise.

I. La Convention de Budapest et son application

La Convention sur la cybercriminalité du Conseil de l'Europe votée en 2001 est le seul instrument international contraignant concernant la question de la cybercriminalité. 41 États sont signataires. En tout 125 pays s'en réfèrent pour élaborer une législation exhaustive en matière de cybercriminalité. De fait, la convention est un cadre pour la coopération internationale contre la cybercriminalité parmi les États Parties.
En 2003, la convention a été complétée par le protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques. Ce protocole élargit le champ d'application de la Convention, y compris ses dispositions en matière de droit matériel, de procédure pénale et de coopération internationale, de sorte à couvrir également les infractions de propagande raciste ou xénophobe. Ainsi, outre l'harmonisation des éléments de droit matériel de tels comportements, le protocole facilite l'utilisation par les parties des moyens et voies de coopération internationale établis, dans ce domaine, dans la Convention. Des notes de guidance du Comité de la Convention Cybercrime (T-CY) permettent de lutter contre les nouvelles menaces d'une manière pragmatique.
La réussite de la lutte contre la cybercriminalité est possible si les parties mettent en place les conditions nécessaires à l'application de leur adhésion à la convention. Beaucoup expriment le besoin d'une assistance supplémentaire afin d'assurer une mise en œuvre législative complète. Un document de travail est disponible pour contribuer aux discussions internationales sur le renforcement des capacités comme moyen efficace de relever le défi de la cybercriminalité. Les gouvernements ont l'obligation de protéger leurs populations contre la criminalité à la condition de respecter les exigences posées par le respect de l'État de droit et des droits de l'homme lors des investigations en matière de cybercriminalité. C'est pourquoi le Conseil de l'Europe met en avant les sauvegardes de l'article 15 de la convention et soutient la modernisation de la Convention 108 sur la protection des données.

II. Une convention en avenir

L'impact de la convention est à considérer en termes de qualité et de quantité. La notion de qualité requiert le droit matériel, le droit procédural et la coopération internationale. Il faut aussi introduire dans l'équation d'analyse, son champ d'action. En l'occurrence, celui-ci ne se réduit pas aux actes de cybercriminalité mais à toutes enquêtes spécifiques où il y a intervention d'une preuve électronique. Il est important de rappeler que la Convention ne légitime

en rien la surveillance généralisée, elle est strictement circonscrite aux enquêtes spécifiques. Par contre, elle favorise les moyens de lutter contre toutes les formes de cybercriminalité. Un ensemble d'outils a été développé afin d'utiliser l'étude comparée en matière de droit pénal sur la Convention de Budapest et la Convention de Lanzarote sur la protection des enfants contre l'exploitation et les abus sexuels et afin de lutter contre les flux financiers criminels et le blanchiment d'argent sur Internet.

Dans un certain nombre de pays africains l'adoption de la Convention se limite au droit matériel et se heurte à difficulté de la mise en œuvre de la législation par manque de professionnels dans la justice et la police. Dans ces cas, une assistance technique est très attendue car elle participe à l'adhésion de ces pays à la Convention. En tout une soixantaine de pays peuvent adhérer à la Convention grâce à ce soutien logistique.

En octobre 2013, le Conseil de l'Europe et l'Union européenne ont signé un nouveau projet joint dénommé Action mondiale sur la Cybercriminalité (GLACY). Ce projet, sur une durée de 3 ans, soutiendra les pays à l'échelle mondiale dans la mise en œuvre de la Convention de Budapest sur la cybercriminalité. GLACY est financé par l'instrument de stabilité de l'Union européenne (IdS) et le Conseil de l'Europe. Afin d'optimiser cette coopération et assurer la gestion de ses projets relatifs au renforcement des capacités en matière de cybercriminalité, le Conseil de l'Europe mettra en place un Bureau de programme sur la cybercriminalité à Bucarest en 2014. À cet effet, un Protocole d'accord a été signé. La communauté internationale est parvenue à un large consensus sur le renforcement des capacités pour aborder avec efficacité le défi de la cybercriminalité. La mise en place de C-PROC permettra au Conseil de l'Europe de répondre de manière efficace au nombre croissant de demandes d'assistance. En matière de législation sur la cybercriminalité, sur les 193 membres des Nations unies, 140 États ont entrepris des réformes et 90 % de ces pays ont utilisé la Convention comme feuille d'orientation ou source.

La révélation du programme Prism a soulevé de multiples interrogations tournant autour de la liberté individuelle, l'utilisation des données personnelles par des acteurs économiques privés ou encore la clause de confidentialité qui lie l'internaute aux entreprises américaines. Cette affaire a largement impacté les travaux de la Convention sur la coopération des opérateurs avec les polices. Un certain nombre d'accords existe déjà au niveau national entre les différents partenaires, par contre la coopération transfrontalière est encore en discussion. Ces travaux avec la Convention ne pourront redémarrer que sur de nouvelles bases de confiance.

La principale critique à la Convention porte sur le fait qu'elle ne serait plus d'actualité. La pérennité de la Convention tient dans ses modes d'application, d'évaluation et de formation des parties en absence de protocoles additionnels. Les notes de guidance aident à lutter contre les nouvelles menaces d'une façon pragmatique. L'article 9 de la Convention qui donne un droit de réserve aux pays signataires, loin de vider la Convention de sa substance, est un moyen d'élargir son assise et d'asseoir son expertise. C'est la coopération et l'aide à l'éducation de la lutte contre la cybercriminalité qui participent à long terme à la pleine acceptation des parties. Les travaux préparatoires à l'élaboration de la Convention ont duré 13 ans, alors qu'à l'époque il y avait un accord des États sur la nécessité de produire un instrument européen ou international de lutte contre la cybercriminalité. Aujourd'hui il n'existe plus cet accord à minima pour un nouvel outil. La Convention existe, par contre s'il y a des lacunes, la coopération technique et l'adoption de protocoles peuvent la prolonger.

A la dernière Conférence Octopus sur la Cybercriminalité en décembre 2013, le conseil européen a noté une augmentation, sur le plan international, de l'harmonisation législative en matière de cybercriminalité. Le Conseil a aussi souligné que des organisations telles que l'Organisation des États Américains (OAS) et la Conférence des Ministres des États Ibéro-américains (COMJIB) a recommandé l'adhésion à la Convention de Budapest sur la Cybercriminalité.

A9 – Assurances : état du marché

Intervenants :

- Jean-Philippe BICHARD – Rédacteur en chef de Cyber Risques News
- Nadia COTE – Directrice générale de l'assureur ACE Group
- Jérôme GOSSE – expert chez Zurich
- Sébastien HÉON – Directeur des relations institutionnelles de Cassidian
- Jean-Laurent SANTONI – PDG Clever-Courtage

Résumé des interventions :

Plusieurs tendances nées des risques cyber se dessinent en matière d'assurances. La première tendance consiste en un rapprochement entre assureurs et acteurs, la seconde réside dans l'augmentation de la cybermenace avec des risques qui se professionnalisent et se propagent. Les acteurs, les assureurs, les courtiers, les réassureurs ont réfléchi à des manœuvres pour faire face à ces menaces protéiformes et ont déployé des stratégies pour prévenir des cyberrisques.

I - Les problématiques

Il subsiste un questionnement sur la teneur d'un marché de la cyberassurance, de ses contours et de la qualité de ses acteurs. Le marché est aujourd'hui estimé à 700 millions d'euros à l'échelle de l'Europe et à 1,3 milliard de dollars pour les États-Unis. En 2013, on estime que les PME-PMI ont perdu 200 millions d'euros notamment par l'utilisation des techniques de virements abusifs. Par ailleurs, il faut compter en moyenne 284 jours pour que les grandes entreprises françaises et européennes détectent une cyberattaque et moins de 24h pour que les cyberdélinquants accomplissent leurs attaques.

Le marché de la cyberassurance ou de l'assurance des risques immatériels enregistre une augmentation de la cybermenace, avec des cyberrisques qui se professionnalisent, la multiplication des risques industriels, notamment sur les systèmes d'automatismes de type Scada, et l'extension des attaques sur les données personnelles principalement avec les Data Breaches. Au-delà des industries et des OIV, les banques, l'e-commerce, les grands comptes sont susceptibles de faire l'objet de menaces diverses : piratage informatique, sabotage, rançonnage et extorsion en ligne...

L'expérience acquise depuis 1998, date des premiers contrats, a permis une mutualisation des risques et généré l'apport d'une expertise aux assurés dans leur compréhension. Le marché de l'assurance des risques immatériels et du financement de leur prévention a influé sur le travail des assureurs. Leurs objectifs englobent l'accompagnement des petites et grandes entreprises, l'apport de solutions de transferts des risques et la garantie des conséquences financières subies par les assurés : frais de notifications, dépenses liées à la reconstitution d'information, à l'intégration de la manœuvre nécessaire pour faire face à certaines cyberattaques ou encore au sabotage qui engendre une perte d'exploitation liée à l'arrêt d'activité....

La pratique des polices et des contrats souscrits pose cependant une problématique relative à l'achat de l'assurance. En effet, la prise en charge est souvent effectuée par divers acteurs (tantôt les services achats, tantôt les services assurances, les risk managers...) qui œuvrent pour un même objectif, mais l'abordent chacun avec un regard différent ainsi sans concertation.

Les accords de coopération conclus entre assureurs et acteurs promeuvent la sensibilisation des dirigeants des grandes entreprises aux cyberrisques. La mise en place des programmes d'identification et de prévention pose un questionnement relatif à « l'aversion » au risque et à la gradation de sa perception : s'agit-il dès lors d'un risque d'intensité (forte probabilité-impact fort) ou d'un risque de fréquence ? La répartition des demandeurs

en matière d'assurances de dommages, de responsabilité professionnelle et de responsabilité des mandataires sociaux s'effectue en trois catégories : les sceptiques, les légalistes et les proactifs :

- Les sceptiques se questionnent quant à leur éligibilité à un sinistre cyber au vu des difficultés qu'ils ont à visualiser les contours des risques cyber. La pertinence de la souscription d'un nouveau contrat ne leur semble pas évidente dans la mesure où les contrats de dommages paraissent être de « formidables » outils de couverture des risques matériels et immatériels alors qu'ils estiment disposer déjà d'une couverture en responsabilité civile.
- Les légalistes, considérés comme opportunistes, vont patienter jusqu'à la mise en vigueur du projet de Règlement européen prévu en 2016. En l'absence de dispositions législatives françaises et européennes prescrivant une obligation de souscription à une assurance en vue d'une protection des cyberrisques ou d'une indemnisation des victimes, ils patientent et observent ceux qui sont soumis à des régimes particuliers notamment les hébergeurs de santé ou bien tous ceux qui ont des obligations CNIL.
- Les proactifs, voyant les assurances comme un moyen de financement du risque, veulent une garantie de la fortification de leurs fonds propres par les assureurs. Pour eux, l'assurance est un moyen d'augmenter leurs fonds propres, leur prise de risques et d'accroître la garantie qu'ils peuvent délivrer à leurs clients.

En l'état actuel des choses, les sceptiques ne demandent rien, les légalistes attendent la Directive européenne, les proactifs intègrent l'assurance comme un outil de financement des risques.

II - Les stratégies

Une prise de conscience plus large a conduit à la mise en place d'une évaluation des risques permettant une compréhension des menaces envers l'entreprise. Cette analyse des risques et cette prise de conscience sont d'une importance capitale dans la promotion de ce marché du cyberrisque. L'assureur évalue la maturité du client par l'intermédiaire de questionnaires ou par une analyse de risques. À l'issue de ce bilan assurantiel, le client et le courtier présentent à l'assureur leurs exigences en termes de périmètre de couverture et de plafond de garantie. La plupart des assureurs essaient de répondre aux assurés en leur proposant une offre dédiée ou sur mesure, adaptée à leurs besoins, avec des contrats standards qui peuvent être ajustés par rapport aux risques encourus. En analysant les vulnérabilités des systèmes d'information et de sécurité, l'objectif des ingénieurs spécialisés est de restituer aux clients une visibilité. Certains assureurs vont même jusqu'à garantir une perte de brevet suite à une attaque informatique.

Le traitement et l'approche technique d'un sinistre cyber s'effectuent en deux temps. En amont, il s'agit de mesurer, quantifier, calibrer le risque puis proposer des mesures qui diminuent son exposition. Il faut des plans d'action mesurables, évaluables dans le temps. En aval, il faut gérer les crises et répondre aux incidents, en particulier chez les clients qui n'ont pas développé une grande maturité sur le sujet. Il y a une problématique réglementaire très forte car le régime juridique n'est pas le même d'un pays à un autre ; se pose ainsi le problème de réglementation sectorielle. De l'amont (prévention des risques et compréhension de son exposition) à l'aval (gestion de crise), il y a toute une palette de métiers techniques qui sont indispensables pour bien comprendre le sinistre. Cet ensemble cohérent de compétences connexes fait qu'aujourd'hui dans le cadre de règles d'audit interne et de contrôle, la priorité demeure l'analyse, le traitement, le financement et l'indemnisation.

Malgré le rapprochement entre assureurs et entreprises, la réalité montre davantage de sceptiques que de fervents acheteurs d'assurances. La question relative à la protection et à la confidentialité des données sensibles n'a donné lieu à aucune réponse satisfaisante.

A10 – Comment mobiliser un COMEX autour de la sécurité de l'information ?

Intervenants :
- Franck BOURDEAU, consultant en vision stratégique
- Gérard GAUDIN, consultant indépendant (G2C) et président du Club R2GS
- Christian AGHROUM, chief security officer, SICPA
- André COISNE, directeur général, Bforbank
- Stéphanie CHARLAIX-MEYER, director digital ecommerce, Air France KLM
- Jean-Paul DEFRANSURE, senior vice-président, project director d'EADS cybersecurity improvement plan
- Eric DOYEN, RSSI Humanis
- Marc LEYMONERIE, RSSI Air France KLM

Résumé des interventions :
Le développement de pratiques innovantes en matière de sécurité est basé sur la mobilisation de l'intelligence collective. Un système de management de l'awareness engendre des interactions nouvelles qui, en plus de renforcer la cyber sécurité, contribuent à plus de valeur, pour l'entreprise, pour ses employés et pour ses clients. Il s'agit d'une approche basée sur l'humain, donc avant tout managériale que seul un COMEX (Comité Exécutif) peut impulser.

Comment obtenir la juste mobilisation d'un COMEX s'il n'est pas assez - ou trop - impliqué dans les enjeux de sécurité de l'entreprise? Quels sont les secteurs critiques à protéger ? Comment assurer une intégrité de la politique de sécurité dans une société sans pour autant en faire une forteresse inaccessible pour l'usager ? Les questions évoquées en préliminaire de cet atelier mettent en exergue l'ampleur de la problématique à résoudre.

Dans un premier temps, la connaissance partagée et commune des actifs à risques IT et des impacts associés est le point de départ prioritaire pour les échanges au plus haut niveau, le SMSI intervenant en phase plus opérationnelle. Il s'agit de faire prendre conscience au COMEX des enjeux et du rôle que joue le management dans le dispositif de sécurité. L'objectif étant de trouver en permanence l'équilibre entre protection et ouverture à l'égard des employés et de la clientèle.

Pour protéger les actifs sensibles de l'entreprise, cinq leviers d'action peuvent être - à des degrés divers – activés. Les leviers « infrastructures sécurité » et « processus sécurité » relèvent d'un domaine plus technologique, ceux basés sur la « communication », le « développement du niveau de conscience sécurité » et « l'intégration de la sécurité dans les processus métiers » permettent d'ajuster la sécurité au niveau souhaité.

Dans un contexte en perpétuelle évolution (système cloud, BYOD, ouverture généralisée...) dont la maîtrise est de plus en plus difficile, il est patent de constater que la protection de l'organisation repose encore massivement sur les systèmes de sécurité informatiques et accuse un certain retard sur des aspects comme l'évaluation de l'état réel de son niveau de sécurité ou la mobilisation de l'intelligence des usagers. Il serait illusoire et même dangereux de penser que la technologie « peut tout » alors que, paradoxalement, le facteur humain est impliqué dans près de 70 % des incidents de sécurité. Enfin, il faut garder à l'esprit que les cybercriminels sont aujourd'hui très organisés et particulièrement motivés, à l'inverse bien souvent de l'entreprise qui, d'un point de vue sécurité, reste ignorante du niveau et de la nature des dangers qui la menacent.

Des capteurs intelligents

Pour que les mesures et les investissements réalisés en SSI soient réellement efficaces, il est nécessaire de s'appuyer sur 2 piliers qui vont se renforcer l'un l'autre. D'une part, prendre des mesures opérationnelles priorisées, strictement liées au risque et surveillées en permanence. D'autre part mobiliser tous les acteurs autour d'un système défensif avec la mise en œuvre de moyens participatifs et concrets.
L'objectif est de transformer le maillon faible, le facteur humain en facteur de

détection et de réactivité grâce à la mise en place d'un système d'Assurance Sécurité.
En s'inspirant du modèle Total Quality Management, le dispositif SAM : Security Awareness Management permet de mobiliser de façon systématique et organisée l'ensemble des collaborateurs de l'entreprise pour assurer un niveau de sécurité choisi. Le COMEX peut voir dans cette démarche un projet fédérateur suscitant un fort consensus au sein de l'entreprise.
Une forte dose de management est nécessaire pour favoriser le partage des enjeux, la répartition des responsabilités et le développement de scénarios de risques métier - impliquant les différents niveaux de l'organisation - menant à une « vision » globale de la sécurité au sein de l'entreprise. L'ambition ultime serait que l'ensemble des collaborateurs deviennent des « capteurs intelligents », connectés entre eux, de manière à disposer d'un système de détection étendu et avec une vitesse de réaction accélérée ; en bref, il s'agit de donner du sens à l'ensemble des actions visant à la sécurité et de créer ainsi un véritable développement de l'intelligence collective.
Dans ce type d'approche, l'accent est mis sur l'adaptation des dispositifs SSI aux besoins des métiers ou des fonctions avec en filigrane la recherche de l'équilibre optimum entre la fluidité nécessaire et le niveau de vulnérabilité que chaque responsable métier ou fonction est prêt à assumer. L'instauration d'un référent au niveau du COMEX assure que les interactions vont bien se faire au niveau transverse. Ce référent est le sponsor des opérations de sensibilisation des collaborateurs qui contribuent à donner du crédit à cette politique volontariste.
Enfin, pour renforcer le premier pilier, il convient de mettre en place un système d'indicateurs et de mesures pour suivre l'évolution des niveaux de sécurité et donner envie d'une meilleure hygiène sécurité. Une phase proactive (accélération des temps de réactivité, préparation aux incidents graves, amélioration de la prévention) doit s'accompagner d'un système de reconnaissance pour le personnel de manière à faire de l'aptitude à la sécurité un nouvel atout dans un CV.

Une force collective encadrée par des professionnels de premier choix

Cette mobilisation générale doit être relayée par celle des personnels en charge des opérations IT au quotidien, considérés encore bien trop souvent comme un coût et rarement comme un atout producteur de valeur. Experts, opérateurs, administrateurs des réseaux, systèmes ou sécurité constitueront, s'ils sont mobilisés dans ce sens et mieux considérés, l'infrastructure du dispositif d'intelligence collective. De ce point de vue, un expert SOC (security operations center), capable de détecter des incidents furtifs, est

essentiel pour faire évoluer les règles d'hygiène de base, capitaliser le savoir et produire des indicateurs pour un suivi fin du niveau de sécurité. Il convient aussi de modifier progressivement, au sein de l'entreprise, le postulat qui érige le maintien de la disponibilité en dogme - au détriment de l'intégrité et de confidentialité - alors même qu'il n'est souvent pas justifié par une analyse objective des risques.

Une SSI rénovée

À travers la mise en œuvre d'un système de Security Awareness Management, le RSSI se transforme en animateur global avec des alliés naturels tels que la sûreté, la conformité, les ressources humaines.
De nombreux impacts sont attendus :
- simplification des procédures de sécurité ;
- adaptation des niveaux de défense en fonction des choix des responsables métiers ;
- reconnaissance des compétences IT de l'ensemble des utilisateurs ;
- résilience accrue aux événements ;
- renforcement de l'image de sérieux ;
- avantage compétitif lié à une agilité accrue ;
- positionner l'organisation au-delà de la compliance ;
- faciliter l'innovation ;
- placer la Sécurité au cœur des valeurs ;
- démonstration de l'engagement des salariés à travers leurs comportements ;
- intégration plus facile de nouvelles filiales dans le dispositif SSI.

L'entreprise va être animée par un souffle nouveau où l'humain devient un facteur clef de sa protection.

Ainsi, sur une échelle de maturité, où la 1re étape aura été la conformité sans discernement et par conséquent chère, une seconde étape plus centrée sur les risques, on engage une 3e étape d'âge adulte où chacun des acteurs devient un acteur responsable de la défense de son entreprise et conduit à un équilibre entre le ciblage sur les risques principaux et la conformité plus transverse.

A11 – Cyber menaces : des modes opératoires de plus en plus sophistiqués

Intervenants :

- Florence PUYBAREAU, Journaliste indépendante,
- Éric CAPELLLARI, Responsable cellule e-fraude, Société Générale,
- Léonard DAHAN, Country Manager France & Benelux, Stonesoft,
- Gil DELILLE, RSSI Crédit Agricole,
- Loïc GUEZO, Security Evangelist Southern Europe, Director, Trend Micro,
- Benjamin MARECHAL, Manager – FIDS, EY.

Résumé des interventions :

Pendant les dix dernières années, nous avons connu de grandes évolutions tant dans le domaine des usages (comptes bancaires en ligne, paiement avec mobile, etc.) que des techniques à proprement parler. Les fraudeurs se sont donc adaptés à ces évolutions, si nombreuses soient-elles, pour pouvoir toujours être en mesure de profiter des opportunités qui leur sont offertes. L'ingénierie sociale est une des grandes avancées utilisées par ces derniers. Cela permet de cibler très précisément l'entité qu'ils attaquent. Aux méthodes de piratage globales, dont les taux de réussite étaient relativement aléatoires, ont succédé des protocoles bien plus spécifiques et dirigés. Néanmoins, les spécialistes ont constaté que les méthodes des hackers restent souvent basiques.

I. Révolution ou simples évolutions ?

Face à la modernisation des moyens de prévention et d'investigation dédiés au traitement des infractions cybercriminelles, les cyber délinquants haussent le niveau de leurs modes opératoires.

Le phishing est une technique relativement ancienne mais qui rencontre toujours un franc succès. Dorénavant, les cyberdélinquants n'hésitent pas à apposer des logos bien connus (groupes bancaires, compagnies de distribution d'électricité ou encore administrations gouvernementales) mais cela n'en fait pas une véritable évolution technique. De même, le temps où les adresses mails des champs expéditeurs pouvaient nous renseigner sur la légitimité toute relative du mail reçu n'est pas si lointain. Les hackers prennent désormais la peine d'adopter des noms de domaine en cohérence avec le message qu'ils veulent faire passer.

En règle générale, les belles attaques, au sens de celles qui sont les plus efficaces, sont des combinaisons d'attaques basiques qui, prises individuellement, seraient relativement simples à traiter mais qui deviennent extrêmement complexes lorsqu'il s'agit de les analyser dans leur globalité.

Le véritable changement dans le monde de la cybercriminalité vient de l'utilisation de plus en plus poussée de l'ingénierie sociale : les cyberdélinquants étudient dorénavant en détail les points caractéristiques et les habitudes de leurs cibles.

Finalement, les fraudeurs ont « simplement » affiné leurs modes opératoires en améliorant principalement leur efficacité.

II. De nouveaux risques

La démocratisation des smartphones a ouvert une nouvelle faille dans laquelle se sont précipités les cyberdélinquants. Bien que les téléphones mobiles soient d'usage courant depuis plus de 10 ans, ce sont les nouvelles fonctionnalités offertes par ces derniers qui ont suscité l'attention des fraudeurs. Les smartphones deviennent de véritables petits ordinateurs et contiennent tout autant de données sensibles propres à l'utilisateur. Les nouvelles capacités de paiements sans contact offertes par les smartphones ouvrent également de nouvelles perspectives pour les clients d'une part, mais aussi pour les fraudeurs.

Par ailleurs, le nombre grandissant de transit d'informations sensibles utilisant des modes de transport de plus en plus variés (wifi, bluetooth, …) laisse présager de l'augmentation du nombre de piratages de données par les fraudeurs.

III. Les réactions face aux cybermenaces

Globalement, le secteur industriel tarde à se mettre à jour et à lutter efficacement contre les cyberattaques. Malgré la publication au CERT d'une liste de 23 techniques de contournement en 2010, il est toujours d'actualité de mettre à mal les réseaux de grands groupes avec celles-ci. Il est très aisé d'effectuer des mises à jour sur la partie software. A contrario, les mises à jour sont lentes notamment à cause des hardwares. Le cycle « produit », qu'on peut estimer en moyenne de 5 à 8 ans, génère une certaine inertie dans les adaptations des constructeurs sur la partie hardware.

La voie privilégiée de nos jours ne porte pas tant sur les évolutions techniques, pour lutter contre les attaques, que sur l'évolution des comportements des utilisateurs, de manière à les sensibiliser aux tentatives de fraude et de leur permettre de les identifier.

Enfin, le secteur bancaire se révèle être particulièrement en pointe dans le domaine de la veille contre les fraudes diverses. En effet, un des buts premiers des fraudeurs est de gagner de l'argent. On comprend donc aisément que les sites bancaires soient particulièrement touchés par les attaques. De fausses applications smartphones de grands groupes bancaires ont par exemple vu le jour et se sont trouvées proposées aux utilisateurs pendant plusieurs jours. On comprendra bien la sensibilité des informations qui sont nécessaires à la configuration de ces applications, informations qui peuvent aisément être récupérées par les fraudeurs pour être utilisées à leur profit.


MINISTÈRE DE L'INTÉRIEUR
POINT
TRE LA CRIMINALITÉ LIÉE
HOLOGIES NUMÉRIQUES
260
+1000
20
Gendarmerie nationale

A12 – Comment améliorer la résilience des infrastructures critiques ?

Intervenants :

- Jérôme SAIZ, journaliste, Qualys Security Community
- Laurent HESLAULT, Directeur des stratégies de cybersécurité, Symantec
- Laurent MAYMARD, Responsable du business développement sur le marché Défense, Alcatel-Lucent
- Rytis RAINYS, Directeur du Département Sécurité de l'information et du réseau, Autorité de régulation des communications, Lituanie
- Neira JONES, Président du conseil consultatif, CSCSS (Centre For Strategic Cyberspace & Security Science ; organisation à but non lucratif), Royaume-Uni
- Jan DE MEER, Ingénieur en chef, smartspacelab.eu GmbH, Allemagne
- Mark N. JONES, Directeur Gestion, conformité et sécurité informatiques, British Airport Authority, Royaume-Uni

Résumé des interventions :

Les infrastructures critiques jouissent d'une sécurité informatique souvent obsolète. La quantité de « zero-day » découverte régulièrement en témoigne. Les cas Stuxnet ou Flame ont démontré leur vulnérabilité et il est désormais urgent de renforcer la cybersécurité de ces systèmes industriels critiques. Mais la protection en amont de ces infrastructures ne saurait occulter la mise en place de stratégies de résilience performantes. L'État a un rôle à jouer pour définir les niveaux de résilience et les moyens de les mettre en place.

I. Infrastructures critiques et résilience

Une infrastructure critique est une infrastructure qui permet à un État de fonctionner. Cette notion recouvre plusieurs domaines tels que la santé publique, l'énergie, les services financiers, le transport, l'administration, etc. Par ailleurs, la résilience est la capacité de se préparer et de s'adapter à un environnement changeant et de faire face à l'insécurité et aux divers risques qui menacent une organisation (pays ou entreprise). La résilience doit être proactive (ou préventive) et réactive.

La mesure du degré de criticité d'une infrastructure relève de la responsabilité du gouvernement. Elle nécessite de procéder à une évaluation des risques. Le monde évolue constamment et il convient en effet de se protéger tant des menaces actuelles que de celles qui peuvent venir à plus ou moins brève échéance.

Il semble difficile d'assurer à la résilience des infrastructures critiques une gouvernance identique pour celles relevant du secteur public et celles relevant du secteur privé. Les motivations de l'un et de l'autre diffèrent en effet et cette différence justifie une approche spécifique de chaque secteur.

Quoi qu'il en soit, la responsabilité se situe à trois niveaux : responsabilité au niveau national, responsabilité en matière de gestion et responsabilité opérationnelle. La résilience et les infrastructures critiques sont plus une question de gouvernance qu'une question de technologie. La question essentielle ici est celle du rôle du gouvernement. Pour certains, le gouvernement apparaît en mesure de tout gérer. Sa position aux rênes du pays et son rôle de coordinateur favorisent une coopération efficace entre secteurs privé et public. Il veille au partage des responsabilités entre chaque secteur qui se trouve responsable de sa propre résilience.

II. État – privé : des échanges à sens unique ?

Le rôle central de l'État impose un partage d'informations. Se pose alors le problème de confidentialité des informations partagées et de confiance entre acteurs privés et publics. Les entreprises du secteur privé fournissent des informations aux gouvernements, mais n'en obtiennent que fort peu en retour. Cet état de fait n'est pas incitatif pour les entreprises qui, sauf à y être contraintes, ont tendance à garder pour elles des éléments qui pourraient être utiles à tous. Les gouvernements et les entreprises ont des responsabilités qui leur sont propres. Il faut les déterminer, les connaître et les accepter. Les gouvernements ont pour responsabilité de financer, fournir et gérer certaines infrastructures. Ils devraient également faire bénéficier les entrepreneurs de leurs analyses et du travail de renseignement économique qu'ils réalisent. Les États-Unis

le font très bien.
L'amélioration du niveau de sécurité dans le secteur public passe également par la formation sur les systèmes de sécurité. Le Royaume-Uni encourage l'application de bonnes pratiques en matière de gestion des menaces. Par ailleurs, il n'y a pas de schéma de formation à la sécurité informatique au niveau européen (sauf peut-être en Allemagne). Perfectionner les aptitudes en matière de cybersécurité ne passe pas seulement par l'amélioration des outils, mais aussi par celle des compétences des personnes.

III. Quelle gestion du risque ?

La gestion du risque est une notion bien connue du monde de l'entreprise. On pourrait imaginer que les gouvernements adoptent une gestion du risque unique pour toutes les infrastructures nationales. Dans le monde de l'entreprise, les agences de cotation (ex : Moody's) augmentent ou baissent la cote d'une entreprise, ce qui a un effet sur le prix de l'action. Les États eux-mêmes sont soumis à ce type d'évaluation. Aujourd'hui, les nations sont de plus en plus confrontées à des infrastructures numériques. On peut penser qu'un pays pourrait évaluer le risque représenté dans ce domaine par un autre État avant de faire affaire avec celui-ci. Dans les faits, il existe des bonnes pratiques, mais il n'y a pas d'organisme unique de cotation du risque. Il est facile de dire quel marché est plus sûr qu'un autre. Transposer ce type de cotation au niveau des États ou estimer qu'une infrastructure informatique est plus sûre qu'une autre reste difficile.
Le cœur du problème est que l'on essaie d'avoir une gouvernance du risque correcte alors que l'on ne dispose pas des moyens d'évaluation appropriés. Il serait possible d'adopter les standards communément acceptés par la plupart des organisations à travers le monde, de procéder à des examens plus poussés, des audits plus nombreux et plus précis sur les infrastructures à propos des problèmes de cybersécurité. Notons également qu'il n'existe pas de cadre légal international. Mais la collaboration en matière de cybersécurité existe (ex : Japon et États-Unis).

Internet est le dénominateur commun aux infrastructures critiques. La restructuration des infrastructures internet est nécessaire pour en assurer une résilience minimale : les décisions doivent être prises par les autorités. Un travail en commun est en cours, notamment au travers de l'ENISA. Internet semble résilient mais il n'est pas sûr. Il conviendrait donc, autant que possible, d'éviter de connecter les EIV au réseau.
Au niveau de l'entreprise, disposer d'un BCP (Business continuity plan) n'est pas une réponse au problème de la résilience.

Par ailleurs, le BCP représente une contrainte. L'évaluation du risque est incompatible avec les BCP. Le secteur financier semble plus résilient que les autres mais il est difficile d'établir une hiérarchie, car de trop grandes différences existent entre secteurs.

A13 – Exploiter le Big Data pour améliorer la cybersécurité

Intervenants :
- Daniel GUINIER : Expert cybercriminalité, Cour Pénale Internationale
- Rémi LISSAJOUX : Directeur marketing IBM spécialisé solution i2
- Olivier PATOLE : Manager IT Advisory, cabinet DELOITTE
- Dominique LOISELET : Directeur Général Blue Coat France et Afrique francophone
- Matthieu ESTRADE : Directeur technique de QUALYS chargé de la Stratégie Produits liés à la plate-forme QualysGuard

Résumé des interventions :

La cybercriminalité moderne est de plus en plus complexe à combattre. Détecter, identifier et analyser les menaces sont des préalables nécessaires pour comprendre les modes opératoires, élaborer les ripostes et les protections efficaces. Il est d'un grand intérêt de considérer comment la mise en œuvre du Big Data permet de consolider les historiques d'informations internes et externes afin de détecter, comprendre, analyser et de répondre au cybermenaces.

I. Le « Big Data » : définition et contexte

90% de l'ensemble des données produites dans le monde ont été créés au cours des deux dernières années, avec un volume quotidien de 2,5 pétaoctets (10 puissance 15) . Ces données sont de nature variée et proviennent de sources diverses : chaque jour sur Facebook, 250 millions de photos sont postées, 800 millions d'utilisateurs sont actifs, avec plus de 900 millions d'objets. Avec ce gigantisme d'information, 432 millions de « pirates » transfèrent plus de 9,5 pétaoctets de données chaque mois

Le concept de « Big Data » est associé à la règle dite « des 3V », caractéristiques essentielles de « Volume », « Variété », « Vélocité », auxquelles il faut ajouter « Véracité », « Visuel » et « Valeur ».

Les enjeux sont donc de disposer de solutions adaptées pour pouvoir traiter un volume gigantesque de données disparates, structurées ou non, émanant de terminaux : ordinateurs, Smartphones, tablettes, objets communicants, etc. Il s'agit d'un des plus grands défis informatiques de la décennie 2010-2020, tout comme le service du Cloud Computing.

Pour améliorer la vélocité, ces solutions s'appuient sur l'association de plusieurs technologies comme les mémoires dynamiques (DRAM ou Flash), les moyens de traitement massivement parallèles, les bases de données non relationnelles performantes et l'architecture du système de fichiers tel que Zettabyte (ZFS).

Le « Big Data » nécessite un engagement de la part des décisionnaires, en charge des systèmes d'information, pour modifier leurs politiques relatives aux données, à l'intérieur comme à l'extérieur de l'entreprise. En prévention des implications ultérieures encore méconnues, les entreprises doivent s'assurer que l'utilisation du « Big Data » est conforme à la législation et aux règlements actuels, tout en anticipant les contraintes à venir.

2. Application à la cybersécurité

Le « Big Data » peut être vu comme une opportunité pour renforcer la cybersécurité et lutter contre la cybercriminalité. En utilisant ces nouvelles données, le « Big Data » permet, grâce à son analyse, d'en tirer des signaux objectifs afin d'intervenir de façon prédictive et proactive.

Si les entreprises n'ont pas toujours besoin de comprendre les détails techniques du fonctionnement des attaques, elles doivent disposer d'éléments d'analyse pour comprendre les défaillances de leurs systèmes. Plus que la réaction aux incidents, la capacité d'anticipation doit guider la prise de décision. Malheureusement, si un certain nombre d'entreprises utilisent le

« Big Data » pour améliorer leurs affaires, peu ont conscience du potentiel qu'elles pourraient en tirer en matière de sécurité.

Au-delà de la sécurité classique des systèmes d'information, la question est maintenant de savoir quand et comment un organisme peut être attaqué, car il le sera ! La survie de l'entreprise dépendra donc de sa capacité à réagir, à comprendre le "qui, quoi, comment, quand", et à mesurer l'impact du préjudice en un délai le plus court possible.

Le « Big Data » stocke, analyse, classifie et archive chronologiquement la totalité des trafics d'informations s'opérant sur le réseau. Il permet la recherche des sources de menaces et de leurs conséquences en remontant sur les « données d'expériences passées ». Il introduit donc les notions de « sécurité analytique » et de « confirmation de conformité ». Il permettra enfin de construire des dossiers avec les éléments de preuve, pour les déclarations de soupçons, les poursuites en justice et les actions en recouvrement de préjudice. En termes de « Big Data », l'objectif pour l'entreprise n'est donc pas de stocker de l'information, mais bien de pouvoir l'utiliser pour comprendre ce qui se passe avant, pendant et après l'attaque.

La diversité des sources et des formats de données (Smartphones, tablettes, objets connectés, etc..), à la fois structurées et non structurées, multiplie le volume, le format et la sémantique des données disponibles. Retrouver une information ou un événement dans le Big Data revient à retrouver une aiguille dans des milliers de bottes de foins.
À partir du moment où l'on considère que les données sources sont non structurées et que par ailleurs on augmente la fréquence d'acquisition, il faut alors relever deux défis :
La gestion du volume exponentiel des données à traiter,
La fréquence élevée à laquelle il faut réaliser les traitements et les analyses.
Ces deux défis nécessitent la mise au point d'une algorithmique et d'outils spécifiques, pour fournir par exemple le positionnement automatique des données sur des taxonomies et la détection de signaux faibles.

L'entreprise doit intégrer sa technologie dans une infrastructure globale qui doit nécessairement combiner sécurité et « Big Data ». Il est nécessaire de coupler les solutions de traitement des données aux analyses prédictives et post-mortem qu'elles soient statistiques, à base de règles, etc.
C'est la mise en correspondance de toutes ces données hétérogènes qui permet une analyse globale de la situation, que ce soit pour identifier les risques, les événements ou les menaces.


IDENTITÉ
NUMÉRIQUE ET
CONFIANCE

A14 – Enjeux de puissance dans le cyberespace

Intervenants :

- Solange GUERNAOUTI, Professeur, Université de Lausanne.
- Laurent BLOCH, DSI, Université Paris Dauphine,
- Laurent BOURRA , CEO, Nano JV,
- Olivier KEMPF , Maître de conférences, Science po,
- Daniel VENTRE , CESDIP.,
- Guillaume TISSIER, Directeur général, CEIS.

Résumé des interventions :

Nous sommes dépendants dans le cyberespace de moyens qui souvent nous échappent. La puissance n'y est pas que technique mais elle est également une affaire de communication. Les infrastructures comme la position géographique d'un pays sont essentielles comme d'ailleurs la capacité de ce dernier à se doter d'une véritable capacité industrielle en la matière.

I – Les problématiques :

Quotidiennement les médias rappellent l'usage abusif, détourné ou criminel des technologies de l'information ou de l'Internet. Un certain nombre de cas médiatisés, dont récemment la première attaque sur des objets connectés, en sont l'exemple.
Plusieurs raisons expliquent cet état de fait : une dépendance à des services et infrastructures internet que nous maîtrisons très difficilement, une exposition croissante des institutions, des organisations et des états à de nouveaux risques pouvant déboucher sur des crises économiques et politiques mais également sur des problèmes globaux de gouvernance. Enfin, la prise de pouvoir et de contrôle de certains secteurs d'activité dans le cyberespace par des entités commerciales et gouvernementales démontre notre faible capacité à prévenir, à réagir et à faire respecter nos droits.

Un certain nombre de questions méritent d'être posées : quels sont les acteurs de ce cyberespace ?
Y a-t-il un exemple concret de la puissance dans le cyberespace ? En quoi consiste-t-elle concrètement ?
Par ailleurs, comment peut-on définir la souveraineté nationale, sachant que puissance et souveraineté sont relativement proches. Traditionnellement, la souveraineté est symbolisée par une frontière définie alors que la souveraineté politique pose la question de la reconnaissance qui instrumente une position par rapport à la communauté internationale.
La souveraineté existe mais de manière différente dans le cyberespace. Elle se manifeste par le contrôle des capacités industrielles, par celui des infrastructures de réseaux et par la gestion des opérateurs importants. Un État risque d'être privé de souveraineté dans le cyberespace s'il ne peut mobiliser de telles capacités au prix d'une R&D pilotée dans le cadre de partenariats actifs et d'une gouvernance encadrée. À titre exemple, la Russie est un acteur majeur dans le Cyberespace, car elle possède une réelle puissance de nuisance. Il est estimé que les meilleurs opérateurs en termes d'attaques et que les meilleurs hackers sont russes.
On peut s'interroger sur les obstacles que doit lever la France en tant que puissance dans le cyberespace et sur la valeur de ses atouts. Cela amène également à évaluer notre capacité à assurer un rôle de leader dans le cyberespace notamment dans le domaine industriel.

II - Des solutions :

Il est devenu urgent d'abandonner ce qui peut être considéré comme une cécité stratégique et il faut être lucide sur ce qui se joue dans le cyberespace. Nous sommes tous concernés comme acteurs du

cyberespace, il est donc absolument nécessaire de maîtriser notre environnement Cyber en toute indépendance et de comprendre les enjeux du cyberespace pour ne pas subir mais participer aux manœuvres politiques, industrielles, commerciales et culturelles qui s'y nouent.

En ce qui concerne les acteurs du cyberespace force est de constater que les États sont les acteurs dominants avec des moyens civils et militaires cohérents, ce qui fait que les acteurs non étatiques sont de fait en retrait. Un exemple concret de puissance dans le cyberespace peut être illustré par l'affaire Stuxnet, très médiatisée, générée par Israël, dont le centre de gravité a été à Washington. Dans cette affaire, la puissance s'est avant tout exprimée de manière médiatique avec pour moyen un triple enjeu d'influence, de pouvoir et de dissuasion. Cet exemple montre que l'un des facteurs de puissance est la communication qui est plus importante que la « cyber puissance pure ». En effet, en l'espèce, d'un point de vue technique le but n'a pas été atteint. Il s'agit bien d'une cyber puissance médiatisée qui est une véritable forme de conflit qui n'est guère évoquée.

Quand la souveraineté politique est reconnue, elle entraîne l'acquisition d'une indépendance qui est l'attribut essentiel de la souveraineté. Ceci ne fonctionne pas dans le cyberespace car les acteurs sont tous dépendants des uns des autres. De plus, dans le cyberespace existe la règle de l'inattribution de l'action à un ennemi à la différence d'une guerre traditionnelle. On peut construire des schémas opérationnels, avoir des ennemis mais pas nécessairement être en mesure de formaliser les faits juridiques et techniques qui permettraient de manière probatoire de les désigner et de les qualifier en tant que tels. Le spécialiste ou le hacker peut avoir des actions masquées et cette opacité augure d'un cybermonde sans frontière.

Prism nous a permis de recentrer notre attention sur des choses que nous avions eu tendance à oublier, le cyberespace n'est pas simplement virtuel et, quoi que l'on ait pu penser, il repose sur des infrastructures physiques. Le cyberespace n'existe pas sans les fibres optiques transatlantiques, trans-pacifique ou transcontinentales. Ces infrastructures physiques sont des points de vulnérabilité où s'exercent les actions de puissance. Les grands points d'échange de l'Internet ont autant d'importance que les Dardanelles à l'époque du traité de San Stephano ou le canal de Suez en 1940. Le contrôle, la gestion et la gouvernance de ces infrastructures sont essentiels et les pays qui ont cette maîtrise ont une capacité de puissance par rapport aux autres.

La France a intérêt à recenser ses atouts dans les rapports de puissance dans le

cyberespace. Sa position géographique est un avantage dans cette typologie physique de l'Internet, notamment en termes d'infrastructures physiques. Elle possède également des acteurs industriels très bien placés. La France se doit, par exemple, de militer pour une agence internationale nouvelle avec de vraies compétences. Enfin, elle doit posséder de véritables capacités industrielles, celles qui accompagnent les évolutions d'Internet à l'instar des États-Unis, de l'Allemagne, de Taïwan, de la Corée du sud et d'Israël.

A15 – La coopération internationale, pilier de la lutte contre la cybercriminalité

Intervenants :

- Jean-Dominique NOLLET : EUROPOL, (animateur),
- Andy ARCHIBALD : NCA,
- Laurent BAILLE : Gendarmerie nationale,
- Adèle DESIRS : INTERPOL,
- Nicolas DILEONE : CEPOL,
- Valérie MALDONADO : OCLCTIC.

Résumé des interventions :

La coopération internationale en matière de lutte contre la cybercriminalité a fait de réelles avancées. Il s'agit désormais de lui donner davantage d'outils juridiques, et cela rapidement, pour répondre à la progression fulgurante de la cybercriminalité. Si les obstacles à la coopération internationale doivent tomber, la lutte contre la cybercriminalité passe également par une prise de conscience des populations et des industries. Les conflits d'intérêts entre États face à une menace globale n'ont pas lieu d'être.

La criminalité et notamment la cybercriminalité, telle que la pédopornographie, tirent profit des nouvelles opportunités que représentent les nouvelles technologies dans le cadre d'échanges mondialisés et des moyens de communication de plus en plus rapides et variés. Face à ce fléau, les États, via leurs organismes de police nationaux, tentent de répondre aux menaces en les identifiant et en les traquant. Cependant cette menace globale souvent protéiforme nécessite que les États y répondent par une étroite coopération. C'est par une collaboration internationale que des échanges d'information pourront se faire et faciliter la lutte contre la cybercriminalité.

I. La coopération internationale, une évolution positive :

L'enjeu pour les forces de sécurité est d'identifier rapidement les menaces et les auteurs d'infraction qui se servent des moyens internet pour répandre ou échanger des données. Se jouant des frontières et des obstacles administratifs, toutes les plates-formes d'échanges et les nouvelles technologies (facebook, mails...) sont d'excellents vecteurs pour participer à la cybercriminalité. Il s'agit pour les structures d'investigation policières d'obtenir des preuves dans un délai très contraint car les données se diffusent rapidement et sont souvent volatiles. De plus dans le cadre de la pédopornographie par exemple, toute la difficulté vient du fait qu'il faut identifier la victime avant de remonter à l'auteur de l'infraction. Cela nécessite des analyses spécifiques notamment quand l'auteur de l'infraction est un proche de la victime. Cependant à cette recherche fastidieuse s'ajoute le fait que parfois les images sur lesquelles travaille le service de police ont en fait déjà été traitées par un autre service de police travaillant dans un autre État et que l'affaire a été résolue.

Conscient de ces lacunes, les polices criminelles apprennent à travailler ensemble. En effet, les cyberdélinquants sont souvent les même qu'ils agissent en France ou au Royaume-Uni. Les notions de territorialité deviennent alors accessoires lorsque l'enquête nécessite une coopération. La convention de Budapest a permis l'élaboration de directives européennes et qu'un système de gel des données soit mis en place. Des bases de données communes tel que IXE (base de données pédo-criminalistique) sont mises en œuvre. Interpol contribue à mettre en relation les différentes polices criminelles notamment dans le cadre de relations bilatérales et malgré que bien souvent les États possèdent une structure centralisée permettant de traiter les données.

II. Une lutte qui passe par des outils supplémentaires et une action auprès des acteurs privés :

Si une réponse policière coordonnée existe avec INTERPOL, EUROPOL, EUROJUST... il s'agit pour les enquêteurs de trouver une combinaison entre la protection des droits individuels et des moyens d'investigation efficace. La lutte semble parfois déséquilibrée et des nouveaux outils doivent être créés. Concrètement, trois outils pour les besoins des enquêteurs sont à créer ou à améliorer : lors de cyber-patrouille permettre une extension des enquêtes sous pseudonyme dans tous les cadres d'enquêtes pour accéder à certaines plateformes d'échanges de données, obtenir une reconnaissance juridique de l'utilisation des réquisitions pour les sociétés étrangères afin de pouvoir réaliser des « cyber-perquisitions », permettre une captation des données à distance dans le cadre de perquisitions (via un « cloud compting »).
Un Schengen numérique dans un premier temps voire un réseau international d'échanges de données policières doit permettre de remédier aux procédures de réquisition nationales trop contraignantes et d'améliorer la qualité des échanges en matières de preuves et de renseignement. De même, les qualifications d'infractions nécessitent d'être standardisées au niveau international pour faciliter les échanges entre les différents services de police. La création de plates-formes d'échanges de données peut également participer à la réduction des coûts que représentent les écoutes judiciaires.
Les entreprises sont aussi des acteurs dans la lutte contre la cyber-délinquance. Dans une approche globale, les industriels peuvent avoir un rôle à jouer en mettant par exemple en place des filtres dans leurs programmes et leurs systèmes d'information et éviter ainsi que ne se diffuse sur Internet des données à caractère pédopornographique ou autres.

III. La nécessité du respect d'un cadre légal pour lutter efficacement contre cette menace :

Cependant la volonté de créer et de collecter des données dans de vastes sphères virtuelles (cloud) ne doit pas être un obstacle supplémentaire à la coopération internationale et bafouer le cadre légal. En effet l'excès de données en rendrait son traitement trop difficile et au niveau juridique se poserait la question de savoir qui serait le fournisseur d'accès à ce cloud et quel service y serait affilié. En matière de coopération internationale, il faut certes des outils juridiques adaptés aux besoins des enquêteurs mais qui restent pour le moins légaux.
Envers la population, les lois doivent être proactives pour dissuader les cyberdélinquants et faire évoluer positivement le comportement des

utilisateurs. Il s'agit de créer des infrastructures juridictionnelles pour protéger les victimes, d'éduquer les populations sur la cybercriminalité et ses dangers mais également de rassurer sur l'utilisation des données privées. Les services de police doivent garantir le fait que les informations privées collectées dans le cadre d'enquête ne servent pas à des fins criminelles.

Ainsi face à une menace globale qui semble toujours avoir un temps d'avance, la coopération internationale est nécessaire. Des outils existent et de nouvelles technologies sont à mettre au service des différents services de police. Tout en respectant le cadre légal et en alliant le respect des droits individuels avec des moyens de perquisitions pertinents, il s'agit désormais de continuer à abaisser les barrières juridictionnelles des différents États pour avoir une action percutante sur la cyber-délinquance et cela au niveau mondial.

A16 – Confiance numérique : quelle politique d'innovation pour l'Europe.

Intervenants :

- Yann SERRA : Journaliste, animateur,
- Gustav KALBE : commission européenne (programme horizon 2020),
- Pierre AUBRY : Imprimerie nationale (pôle sécurité, carte d'identité),
- Thierry WINTER : Bull.

Résumé des interventions :

L'Europe a le potentiel pour mener une politique d'innovation en matière de sécurité et de confiance numérique. Elle doit s'appuyer sur des programmes européens (Horizon 2020, ITEA) moyennant le montage d'un dossier partenarial, structuré selon une visibilité industrielle et une forte normalisation. Il convient pour favoriser les initiatives européennes d'alléger les démarches administratives et d'unifier les marchés afin de créer une profondeur dans les marchés et les débouchés selon un seuil critique comparable au contexte des Etats-Unis. C'est une condition essentielle de la viabilité des projets et à la rétention des chercheurs en Europe.

I - Un potentiel non négligeable :

L'Europe a un potentiel d'innovation en matière de numérique et de confiance numérique. Il n'y a pas de géants identifiés et les Etats-Unis ne sont pas propriétaires de toutes les technologies et de toutes les industries en la matière. La prise de conscience par les utilisateurs que le monde numérique constituait un risque a conduit à l'émergence d'un marché de la confiance que l'Europe peut satisfaire. Un exemple est celui des portables qui peuvent être utilisés dans le domaine professionnel avec un fort niveau de sécurisation. Ces solutions, d'ailleurs présentées par la société Bull, proposent, par exemple, un produit hautement sécurisé avec capteur digital. L'Europe est également en avance en matière de technologies embarquées. Si L'Europe ne conçoit pas certains produits, elle tente toutefois de répondre aux besoins d'opérateurs extérieurs qui, eux, ont besoin des technologies européennes.

Ce potentiel ne peut se mettre en œuvre que dans le respect des législations. Il est donc nécessaire de déterminer les compétences nécessaires à la satisfaction du marché tout en restant dans le cadre juridique européen très contraint. Le respect de ces normes « fortes » rend exportables les produits européens sur des marchés extérieurs du fait de la confiance qu'ils procurent.

II - Des financements européens :

Les programmes « Horizon 2020 » sont des programmes de recherche-cadre évoluant dans le cadre de politiques d'innovation visant des marchés porteurs d'emploi, de compétitivité et la création de nouvelles entreprises. Ils comportent également un volet évaluation car ils promeuvent une vision à long terme d'un « business model » intégrant la sécurité dès la conception des composants pour susciter la confiance. Les développements doivent s'inscrire dans un compromis entre les normes de sécurité et la demande de l'utilisateur.

Le processus d'obtention des fonds passe par un portail qui publie des appels à proposition (http://ec.europa.eu/programmes/horizon2020/h2020-sections) selon de grands thèmes. Par exemple, en matière de cybersécurité, sont visées la protection des données et la protection de la vie privée. Les consortiums intéressés choisissent leur contribution. Les dossiers déposés doivent exposer un besoin à satisfaire et proposer un suivi industriel de la solution proposée. Il ne s'agit pas d'une substitution à des programmes nationaux. Le consortium doit comprendre au moins trois participants venant d'au moins trois pays européens et issus d'entités légales distinctes, dont la nature est indifférente : association de centre de recherche, groupes d'industriels, *etc.* Une commission effectue un classement par ordre de qualité qui sert de

base au financement jusqu'à épuisement des fonds. Pour le domaine cyber, l'enveloppe s'élève à 140 millions d'euros. Le cycle de sélection dure jusqu'à neuf mois. Les projets portent sur deux à trois ans.

Les programmes ITEA portent sur des études et des innovations avec un fort retour d'investissement. Le processus comporte une « session d'émergence » et une « phase de labellisation » du produit. Les projets portent sur 2 à 3 ans. Ils nécessitent l'engagement d'opérateurs venant d'au moins deux pays différents. Les partenaires peuvent être des universités, des chercheurs, des PME, etc. Cet ensemble de programmes vise à fortifier la recherche et à garder les chercheurs en Europe. Il tend également à mettre sur le marché des produits satisfaisants, à conforter les revenus des entreprises par une nouvelle offre et à générer de l'emploi. Si on prend le cas d'activités suscitant une forte demande de confiance (Passeports, CNI, …), on est obligé au niveau européen de se rapprocher d'autres partenaires et de mutualiser certaines technologies en termes d'interopérabilité : par exemple la création d'applicatifs prenant en compte la normalisation du temps de travail des chauffeurs routiers au niveau européen. Les opérateurs européens ont une priorité, car ils sont alignés en termes de contraintes réglementaires ce qui facilite la coopération. Cela évite de se voir imposer un modèle qui ne convient pas à l'Europe. C'est le cas de la gestion protégée des données personnelles qui est minimisée sur d'autres théâtres et qui fait l'objet d'un lobbying dans ce sens. Si on prend l'exemple de la carte d'identité numérique, il existe un fort enjeu d'authentification sur les réseaux et une demande de plus de services, notamment sur la banque. La signature électronique peut être incluse à l'offre ce qui permettrait par exemple des crédits en ligne. Cela revêt une importance vitale car on ne peut la déléguer à une signature électronique « facebook » fragile et volatile.

A titre d'exemple, en projet ITEA, une étude porteuse consisterait en une capacité à créer une politique de sécurité en ligne qui contrerait une divergence lente des mesures mises en place. Elle mettrait en œuvre des mécanismes et une sémantique qui participeraient d'une intelligence artificielle maîtrisée qui soit capable d'introduire de la cohérence et des propositions dans un système de sécurité : proposer de supprimer des droits d'une personne qui n'utilise pas une application, dénoncer une utilisation d'une application par quelqu'un qui n'a pas badgé à son arrivée, etc.

III. Quelle réglementation pour l'Europe ?

Les directives européennes ont vocation à une transposition nationale qui donne lieu à des interprétations divergentes et parfois des incompatibilités avec les lois existantes.

La commission européenne a la possibilité d'une réglementation applicable sans transpositions. C'est le cas pour l'identité numérique. Tous les pays devront fournir une entité numérique pour tous leurs citoyens qui sera reconnue par tous les états membres. Dans ce domaine, il ne faudra pas prendre de retard.
On peut s'interroger sur le format porteur de ces projets : petites start-up ou gros projets du type Airbus de la cybersécurité. La crise économique montre que la création de start-up est bénéfique car elles s'adaptent plus rapidement au marché par leur dynamisme. Un Google européen fait défaut du fait que nous n'avons pas réalisé le marché européen intérieur ce qui rend difficile la création de sociétés qui n'ont pas un marché potentiel de 500 millions d'habitants. On peut considérer qu'une Europe à 28 est un frein à la décision. Sur les projets ITEA une piste de progrès résiderait dans la réduction du délai entre la phase de labellisation et celle de projet. Horizon 2020 comporte également des lourdeurs administratives. Ceci explique les migrations des projets vers les Etats-Unis qui comportent un espace juridique unique, un marché important et peu de freins pour l'industrialisation. À l'inverse, en Europe, chaque pays présente ses spécificités. Il reste à rechercher une valorisation des produits fournis et à fixer des chercheurs sur des *business plans* touchant à des marchés et des fonctions bien identifiés.

A17 – La sécurité des systèmes industriels

Intervenants :

- Bertrand GARÉ, Rédacteur en chef, L'informaticien,
- Pierre CALAIS, Directeur adjoint, Arkoon / Netasq,
- Isabelle DUMONT, Director of Industry Marketing, Palo Alto,
- Emmanuel DUPONT, RSSI, Holcim France Benelux,
- Thieyacine FALL, Directeur de Mission, Thales Communications & Security,
- Christian GUERRINI, Directeur de mission cybersécurité, Sogeti,
- Stéphane MEYNET, Chef de projet systèmes industriels, ANSSI.

Résumé des interventions :

L'année 2013 a été marquée par une prise de conscience des problématiques de sécurité des systèmes industriels. Ceux-ci, peu adaptés, sont en effet particulièrement vulnérables aux cyberattaques et pourraient être la cause de pertes financières voire humaines lourdes. L'approche les concernant doit donc évoluer de la sûreté vers la sécurité, en utilisant, à défaut de futures solutions spécifiques, les méthodes et produits existants en matière de sécurisation des systèmes d'information.

I. Une prise de conscience mondiale

Après Stuxnet, Flame et de nombreux vols de données personnelles ou bancaires, l'année 2013 se caractérise comme une année de prise de conscience en matière de cybersécurité.

Sur le plan des systèmes industriels, Stuxnet a démontré, en 2010, la possibilité d'une cyberattaque aux conséquences matérielles. En 2013, deux ingénieurs financés par la DARPA ont pris le contrôle du freinage, de l'accélération et de la direction d'une Toyota Prius et d'une Ford Escape.

Qu'ils soient anodins, comme l'information relative au fait qu'un réfrigérateur soit vide, ou plus critiques par la connaissance des paramètres de gestion des fours d'une cimenterie renfermant 20 tonnes de magma à 1500°C, les systèmes automatisés voire connectés ou intelligents, qui imprègnent les industries et notre vie courante, sont autant de vecteurs d'attaques, soit comme relais vers d'autres installations informatiques, soit comme cible pour des dommages matériels ou humains. La cybersécurité n'est plus seulement un enjeu financier mais elle revêt également une dimension de prévention de dommages humains.

Ces questions peuvent donc avoir un impact sur les pays, a minima sur le domaine économique mais également en matière de défense nationale ou de sécurité publique. Ainsi, la France a intégré la cyberdéfense à l'article 22 de la loi de programmation militaire (LPM 2014-2019). L'ANSSI, qui a édité en 2012 un « Guide SCADA », participe avec un groupe de travail à la mise en place de mesures organisationnelles et techniques de sécurité des systèmes industriels. Ces travaux devraient aboutir à une classification des installations industrielles en trois classes de criticité, avec une déclinaison sectorielle des modalités d'application de la LPM, l'homologation des installations critiques, notamment pour les OIV, étant un objectif final.

II. Des systèmes peu adaptés à la sécurité : vers une évolution des mentalités

Historiquement, les systèmes industriels n'ont pas été conçus par des informaticiens, mais par des électroniciens ou des automaticiens utilisant l'informatique comme n'importe quel autre outil. Ils sont dotés d'un cycle de vie très long et sont généralement confiés à des responsables de production sans aucun lien avec les Directions des systèmes d'information. Bien que robustes sur le plan de la sûreté de fonctionnement, ces systèmes interconnectés sont particulièrement vulnérables en matière de sécurité : les mots de passe, déjà trop peu présents, sont souvent laissés à leurs valeurs par défaut ou intégrés en dur dans les consoles de gestion.

À la différence des systèmes d'exploitation auxquels nous sommes habitués, les systèmes industriels sont difficiles voire impossibles à « patcher », à mettre à jour et donc à protéger de manière autonome. Leur criticité en matière de productivité restreint également leur évolution, en préférant laisser fonctionner un système, même sans mise à jour, plutôt que de risquer une interruption de la production. De plus, une conception issue d'équipementiers différents a fait émerger des protocoles réseaux peu connus et peu documentés qui compliquent la sécurisation. Enfin, la nature des systèmes industriels, très spécialisés, ne leur permet de répondre qu'à des jeux d'instructions très limités qui peuvent donc assez facilement faire l'objet d'une attaque par force brute, sans compter également les bulletins de vulnérabilités publiés sur Internet.

En acceptant dès aujourd'hui cette cybermenace, notamment par l'acculturation des responsables de ces systèmes aux problématiques de cybersécurité, il faut donc évoluer d'une approche de sûreté, qui excluait par définition toute malveillance, vers une approche de sécurité combinant les différents aspects. Ainsi, les équipementiers intègrent progressivement de la sécurité dans leurs solutions, par exemple par des mots de passes dans les SCADA ou en ne requérant pas les droits administrateur sur les consoles d'administration et de maintenance.

III. Utiliser les méthodes existantes et développer de nouveaux produits de sécurité

Premier élément à noter, les mesures de sûreté de fonctionnement déjà en place contribuent à la sécurité des systèmes. Elles doivent servir de base à toutes les mesures de renforcement de la SSI. Ceci considéré, la première mesure à prendre doit être de cartographier précisément le système industriel et d'analyser le risque avec la méthodologie classique.

Ensuite, et en première réponse, utiliser les méthodes déjà existantes pour sécuriser les systèmes d'information « de gestion » : segmenter le réseau au maximum, mettre en place des pare-feux, construire l'infrastructure sous forme des bastions, limiter l'exposition en utilisant des liaisons filaires plutôt que radio, limiter les connexions entrantes sur les SCADA à une liste blanche, nettoyer les vecteurs d'infection comme les clefs USB, les consoles de programmations ou les postes de travail en adaptant à chaque fois l'existant aux contraintes des systèmes industriels.

Au-delà de l'approche par l'utilisation de moyens techniques, la réponse doit également passer par le monitoring du comportement des systèmes et en réagissant de manière proportionnée sous peine d'atteinte à la disponibilité.

La prise en compte de ce risque ouvre de nouvelles opportunités, en conseil et audit,

mais également vers de nouveaux produits de sécurité, adaptés spécifiquement aux systèmes industriels et leurs protocoles. L'analyse comportementale des systèmes apparaît comme un bon axe de travail, sans cependant être intrusif, en identifiant les séquences d'instructions légitimes et en réagissant à des successions d'instructions aberrantes comme une alternance « avant toute » « arrière toute », par une alerte aux opérateurs ou un arrêt en douceur des installations.

A18 – Retour d'expérience des CERT nationaux européens

Intervenants :

- Valery MARCHIVE, journaliste, Le Mag IT,
- Franck DEZEURE, CERT Europe,
- Alexandre DULAUNOY, CIRCL Luxembourg,
- Chris GIBSON, CERT-UK,
- Steve PURSER, ENISA,
- Ulrich SELDESLACHTS, LSEC (Leaders in SECurity, organisation européenne sans but lucratif).

Résumé des interventions :

Le réseau des CERT a déjà une longue existence. Créé dès 1999, le CERTA, devenu CERT-FR le 21 janvier 2014, devait déjà, selon la décision du comité interministériel pour la société de l'information, s'insérer dans le réseau mondial des CERT. Hébergé par le COSSI, le CERT-FR apporte un soutien aux ministères, institutions et autres structures administratives en matière de gestion d'incidents informatiques. Au sein de l'Union européenne, les CERT nationaux sont de création plus ou moins récente et une structure européenne a été créée en 2012. Un bref état des lieux de quelques structures nationales montre à la fois les progrès déjà enregistrés et le chemin qui reste à parcourir en matière de sécurité des systèmes de communication et de transmission.

I – Le CERT, élément incontournable du dispositif national SSI.

Devant le caractère de plus en plus systématique et dangereux des agressions touchant les systèmes d'information, l'existence d'un CERT devient progressivement la norme pour les États membres de l'Union européenne. Si les structures peuvent s'appuyer sur une expérience plus ou moins longue (le CERT-UK, de création récente, est sur le point de devenir opérationnel tandis que le CERT-FR a déjà 15 ans d'existence), leur logique de fonctionnement est souvent comparable. Ces centres sont systématiquement le point unique de contact avec les services gouvernementaux dès lors qu'il s'agit de délinquance ou de malveillance cyber, tant pour les CERT des autres pays que pour les entreprises et administrations nationales.
Le CERT-UK compte environ soixante-dix collaborateurs répartis en cinq équipes. Une équipe s'occupe des incidents qui sont portés à la connaissance du centre, la deuxième effectue une veille à l'échelle internationale et une troisième prend en compte la communication en matière d'incidents SSI et les réponses à ces derniers. Enfin, les deux dernières équipes s'occupent des interventions sur le terrain, au Royaume-Uni et dans le monde. Pour autant, la mission du centre n'est pas de résoudre les difficultés mais d'aider ceux qui en sont victimes à le faire eux-mêmes. Il en est de même pour le CIRCL, pour lequel il est essentiel de comprendre à quel type d'attaque le solliciteur est confronté : tentative de vol de données, simple test de résistance préparatoire à une attaque ultérieure de plus grande envergure ou encore piratage pur mené par un hacker ? Le Luxembourg, siège de nombreuses sociétés, est particulièrement attentif à ces questions. Enfin, les CERT assurent un rôle essentiel en contribuant à l'échange des données concernant les attaques. En effet, chaque démarche malveillante constitue en soi une occasion d'en apprendre davantage sur les techniques utilisées par les cyberdélinquants. Dès lors, les entreprises et administrations ont tout intérêt à faire connaître leurs propres expériences afin de renforcer la capacité générale à se prémunir contre les attaques. L'information recherchée est celle qui ne se trouve pas dans le domaine public. Lorsque c'est le cas, l'assaillant sait que sa technique est éventée et il en change immédiatement. Il convient dès lors aux victimes de diffuser au plus vite l'information concernant l'attaque qui les a touchés afin de permettre aux autres de prendre sans délai les mesures qui conviennent pour se protéger. Dans cette course de vitesse, les CERT agissent comme des accélérateurs de l'information et contribuent, directement et activement, à sécuriser leurs interlocuteurs.

II – Les organismes européens de réponse informatique d'urgence

Après une phase pilote d'un an, l'UE a décidé de créer en septembre 2012 un CERT européen. Cette structure opérationnelle est modeste par sa taille (16 personnes). Comme les CERT nationaux, elle n'a pas vocation à intervenir directement auprès d'une structure en difficulté mais elle aide les entreprises à régler leurs problèmes. Elle a également une fonction d'alerte et ambitionne d'aider les pays les moins en avance dans la cybersécurité à rattraper leur retard. Lors de l'exercice 2013, le CERT-EU a lancé 650 alertes, une vingtaine d'entre elles concernant de gros incidents. Les risques d'occurrence d'une attaque ne sont donc pas à sous-estimer puisque, statistiquement, deux alertes par jour sont lancées au niveau européen. Le CERT-EU a le même souci de partage de l'information que ses homologues nationaux. Il est en permanence à la recherche de partenaires avec lesquels il pourra développer un réseau efficace de lutte contre la cyber insécurité. Il entretient bien sûr des contacts avec les structures étatiques et souligne la nécessité pour les États membres de créer et entretenir une industrie européenne de sécurité informatique.

Autre structure européenne, l'ENISA est née en 2004 de la volonté de créer une communauté proactive de sécurité de l'information en Europe. Cette agence européenne s'efforce de donner le ton au niveau communautaire en matière de sécurité de l'information. Elle agit comme une tête de réseau et œuvre à la dissémination intelligente et rapide des données relatives aux menaces cyber. Elle promeut les bonnes pratiques à travers un guide destiné tant aux institutions qu'aux acteurs économiques. Elle intervient comme expert auprès des CERT et les aide à préparer, mener et débriefer les exercices de cybersécurité. Une de ses difficultés principales consiste à établir des relations de confiance avec les industriels mais également avec les CERT nationaux. C'est une entreprise délicate alors que se mènent de féroces combats économiques dans un contexte international très concurrentiel.

Des structures non étatiques, associatives, s'efforcent également d'aider les acteurs économiques à mener une lutte efficace contre la délinquance informatique. Il s'agit pour elles d'assister les membres de ces structures confrontés à des incidents ou attaques de type cyber. On observe d'ailleurs que les entreprises peuvent très bien être l'objet d'une attaque sans qu'elles s'en rendent compte immédiatement. C'est la raison pour laquelle, encore une fois, le partage des informations est si essentiel. Lorsque cette logique d'entraide est bien comprise, elle permet de dépasser les réticences liées à la concurrence entre professionnels et de prendre une longueur d'avance sur les délinquants.

Orange Cyberdefense

stratégie de défense numérique et cyberdéfense active

Les expertises d'Atheos et d'Orange Business Services sont désormais réunies sous une bannière commune nommée Orange Cyberdefense

www.orange-business.com

atheos

Business Services

orange

A19 – Confiance numérique et e-administration dans les collectivités

Intervenants :

- Sabine BLANC, journaliste, Lagazette.fr
- Matthieu GILLON, RSSI, Préfecture du Nord-Pas-de-Calais,
- Salvator ERBA, Docapost,
- Christophe CAVELIER, La Poste,
- Emmanuel MICHAUD, Imprimerie Nationale,
- Jean-Marc RIETSCH, FedISA.

Résumé des interventions :

Le succès du développement de la e-administration dans les collectivités territoriales repose sur la confiance que les citoyens peuvent lui accorder. Il leur faut donc des « signes extérieurs de confiance », lesquels reposent autant sur la qualité visible des services proposés que sur leur sécurité.

La réussite de ces objectifs est fondée sur une double confiance, interne cette fois. D'une part, les agents doivent comprendre les enjeux et les changements induits par la mise en place de nouveaux canaux de services – lesquels ne remplacent pas les anciens – et d'autre part, les élus, qui en dernier ressort valident les solutions sans être forcément des techniciens, doivent pouvoir s'appuyer sur un référentiel fiable pour être garant des choix techniques et organisationnels faits.

La e-administration qui consiste en des échanges de données de l'administration - aussi bien de collectivités territoriales que l'État – avec les citoyens ou entre administrations est en plein développement. Selon un récent sondage de l'ACSEL, il y a pourtant une baisse de confiance dans cette e-administration, malgré le renforcement des règles de sécurité. Certes, plus de 70 % des Français lui font confiance et c'est beaucoup plus que l'e-commerce, mais c'est 10 points de moins qu'il y a 2 ans. Les citoyens appréhendent un usage non conforme des données, un risque d'erreur dans l'identité – voire une usurpation d'identité – et une perte de confidentialité. Pourtant l'usage s'en développe très fortement, comme le montre le recours croissant aux télédéclarations de revenus.

I. Créer les conditions de la confiance

Il est donc important que les citoyens puissent disposer de signes tangibles pour fonder leur confiance. L'État, les collectivités ou les entreprises remplissant une mission de service public manipulent une masse considérable de données confidentielles. Ainsi, Docaposte, du groupe La Poste, gère le site « jedeclare.com » qui permet à 8000 experts-comptables de transmettre les données fiscales et sociales de presque 2 millions d'entreprises. La gestion du dossier médicalisé est tout autant exigeante en raison de l'extrême sensibilité des informations conservées. Le citoyen n'acceptera jamais que les informations qu'ils donnent soient « piratées » ou vendues à l'encans : « la confiance existe tant qu'elle n'a pas été trahie ».

Il est donc essentiel que les dispositions de la loi « informatique et liberté » soient rigoureusement respectées, pour garantir notamment la protection, la non-divulgation et la non-réutilisation des données.

L'État a encadré dans un décret du 4 juillet 2013 les 10 domaines pour lesquels les collectivités locales peuvent créer des téléservices et posé des règles prudentielles à respecter.

Le citoyen, enfin, doit constater immédiatement la qualité des services. Une exigence est que ces derniers fonctionnent en continu – rien n'est pire qu'une interruption du service pour rompre la chaîne de confiance -, avec en corollaire, la possibilité d'accéder en permanence à ses données. Enfin, l'usager doit disposer d'une charte qui lui précise ce qui se passe lorsqu'il entre sur le service.

L'objectif, c'est améliorer les relations avec l'usager, lequel est de plus en plus technophile, de plus en plus connecté et de plus en plus impatient. Il attend de la réactivité mais dans le même temps, il refuse une administration de plus en plus déshumanisée.

II. Mettre les moyens nécessaires

Mettre en place un téléservice, c'est modifier en conséquence le fonctionnement de l'administration. Un préalable nécessaire, c'est de former les agents du service public à ces changements. En clair, il est nécessaire que la confiance existe en interne et que ceux qui doivent mettre les mettre en œuvre les appréhendent, les comprennent et les acceptent Ainsi, l'administration danoise accepte les factures électroniques depuis 2005 alors qu'en France, il a fallu attendre 2013. Et ce d'autant plus qu'à l'heure où l'on parle de projets d'ampleur nationale comme « MAP » - modernisation de l'action publique - ou de « COMEC » - communication électronique des données de l'état civil, piloté par le ministère de la justice -, c'est l'organisation du service public concerné qui doit être refondue pour prendre en compte ce nouveau type de fonctionnement. De surcroît, la contrainte budgétaire devient incontournable, il faut être en mesure de dégager des économies et des gains de productivité. Le recours à des tiers – comme pour l'archivage numérique par exemple – doit permettre une mutualisation qui réduit les coûts.
Cependant, le téléservice ne se substitue pas aux formes de relations existantes, il les complète. On arrive ainsi à une administration « multicanale ».

Ces préalables étant posés, il reste ensuite la gestion de la complexité. Des volets techniques ont émergé depuis une quinzaine d'années : cryptage, horodatage, signature électronique ... Les degrés d'authentification doivent être proportionnels à ce qu'on protège. Le principe de la e-administration, c'est de conjuguer la simplification des accès et la sécurité. Enfin, le numérique est pour l'État un patrimoine informationnel, et comme tout patrimoine, il doit être protégé.
On dispose d'un cadre précis, le « référentiel général des services » (RGS). Ce référentiel – qui n'est pas une obligation – met notamment l'accent sur la maîtrise des risques par des réponses tout autant techniques qu'organisationnelles.

Au final, c'est l'élu local qui valide la solution retenue. Investi de la confiance de ses concitoyens – qui l'ont élu -, il répond de cette confiance par son choix. Ce peut être d'autant plus difficile que les petites collectivités n'ont pas toujours les moyens de participer aux travaux préparatoires ni de disposer d'un RSSI.
Il est très important pour l'élu de disposer d'un référentiel qui l'éclaire sur la qualité des choix techniques et organisationnels qui sont ainsi faits.

A20 – Gouvernance d'Internet : quels scénarios ?

Intervenants :

- François-Bernard HUYGHE, Directeur de recherche, IRIS
- Xu LONGDI, chercheur au China Institute of International Studies
- Tris ACATRINEI, juriste, consultante en sécurité informatique
- Jérémie ZIMMERMAN, cofondateur et porte-parole, La Quadrature du Net
- Nicolas ARPAGIAN, Directeur du cycle « Sécurité numérique », INHESJ
- Loïc DAMILAVILE, Assistant CEO, AFMC

Résumé des interventions :

À la suite de la conférence de Dubaï de décembre 2012, certaines voix demandent un rôle accru des États dans la gouvernance d'Internet, d'autres militent pour la libre circulation des informations. Le Conseil économique, social et environnemental (CESE) propose une troisième voie qui éviterait les écueils des deux premières approches : fragmentation du Web ou privatisation par les compagnies américaines.

La présence des entreprises privées sur Internet soulève la question relative à la manière de combiner les intérêts économiques et le souci du bien commun. Faut-il légiférer davantage ou, tout au moins, développer une réflexion politique globale pour donner un cadre aux activités sur Internet ou encore laisser le pouvoir de décision à un réseau décentralisé d'acteurs ?

I. Un modèle multi-acteurs de gouvernance

Puisque le cyberespace est fait d'interconnexions, une liberté absolue n'est pas plus envisageable qu'une sécurité absolue. Cela dit, la multiplication des cybermenaces rend nécessaire une gouvernance efficace d'Internet. Un modèle multiforme de gouvernance a l'avantage d'impliquer :

- de nombreux acteurs : individus, groupes, États, organisations internationales, chacun devant contribuer à la cybersécurité.
- de nombreux niveaux : les efforts de ces divers acteurs, pour qu'ils soient efficaces, doivent faire l'objet d'une concertation aux niveaux local, national et international.
- de nombreuses sphères d'activités : la cybersécurité relève de domaines techniques, politiques, économiques, culturels, juridiques, judiciaires et militaires.

Les technologies de l'information et de la communication étant en perpétuelle évolution, aucun acteur, aucun niveau, aucune sphère ne peut, seul, maîtriser les menaces qu'elles peuvent produire. En revanche, un modèle multi-acteurs de gouvernance peut permettre une concertation efficace où les besoins de chacun s'expriment et où des liens de confiance se bâtissent. Dans ce modèle, l'État occupe un rôle central puisqu'il est le seul à même de mobiliser les parties prenantes, de faire le lien entre les politiques générales et les caractéristiques techniques d'Internet, entre le niveau national et la sphère internationale. Enfin l'État est en mesure de procéder à une répartition des tâches pour que chacun joue pleinement son rôle dans le développement de la cybersécurité. En somme, ce modèle permet des réglementations mondiales dont la mise en application s'adapte aux réalités locales.

II. La gouvernance envisagée comme l'ensemble des décisions qui ont un impact sur Internet

Il est possible de distinguer les décisions technologiques et les décisions politiques. Les décisions technologiques sont le plus souvent d'envergure mondiale et il est crucial de les suivre de près si on ne veut pas assister à une hégémonie des acteurs économiques. Par exemple, il existe une influence croissante des entreprises sur les processus de nommage. Par ailleurs, lorsqu'un protocole nouvellement adopté devient une norme comme BitTorent, on constate qu'une expérimentation menée par un groupe d'individus peut faire considérablement évoluer Internet. Ainsi, les citoyens ont un rôle à jouer dans la gouvernance d'Internet.

A titre d'exemple de décision politique, on peut citer la mise en place d'un pare-feu en Chine et en Iran. Ce type d'action a pour conséquence de fragmenter Internet. À l'échelle mondiale, les orientations de l'Union Internationale des Télécoms (UIT) n'ont qu'une force de proposition et ne peuvent imposer une volonté politique.

Pour que l'ensemble de ces décisions fassent émerger des grandes lignes supranationales, il faudrait s'accorder sur des principes à la base d'intérêts communs pour les entreprises, les individus et les acteurs politiques. Des conférences sur les utilisateurs et administrateurs d'Internet permettraient d'arrêter si ces derniers doivent être gérés par l'État ou les entreprises, la décision revenant aux citoyens. En effet, les entreprises n'ont pas à être mises au même niveau que les citoyens car elles n'ont pas le droit de vote. Il est urgent que les citoyens reprennent les commandes des infrastructures d'Internet. On devrait aussi s'accorder sur l'universalité d'Internet (pour identifier les pays qui souscrivent à ce principe) et sur le respect des libertés fondamentales dans les prises de décision concernant Internet. Il apparaît nécessaire d'envisager Internet comme un bien commun.

III. Vers une position politique européenne sur la gouvernance d'Internet

Pour qu'une telle vision européenne émerge, les citoyens doivent en premier lieu développer leur connaissance du fonctionnement d'Internet. Les Français ont la particularité d'être des utilisateurs efficaces d'Internet sans être à l'origine de la technologie qui le sous-tend. Ils ne sont donc pas en position de contester ou de modifier facilement leur manière de l'utiliser. On peut aussi relever le paradoxe qui réunit chez nos concitoyens attachement à la vie privée et déballage de données personnelles sur les réseaux sociaux. Un débat public est donc nécessaire pour réfléchir au rôle des citoyens sur Internet.

En second lieu, il convient de s'appuyer sur les institutions existantes. Le citoyen doit demander à ses représentants politiques d'exprimer des propositions pour la gouvernance d'Internet. Ces propositions, synthèse des points de vue juridiques, techniques et de l'approche de la société civile, définiraient où se situe l'intérêt général. Si l'on souhaite établir des lois efficaces régissant Internet, le niveau européen apparaît un minimum pour équilibrer le poids des Américains. D'ailleurs, une inaction européenne en la matière entérine de fait la suprématie américaine puisqu'elle entraîne l'application des lois fédérales et des règles dictées par des entreprises comme Google ou Facebook.

Si on s'intéresse à l'identification sur Internet, le simple fait d'être détenteur d'un compte est souvent suffisant aujourd'hui pour effectuer des transactions, car les entreprises ont établi leur propre système d'authentification et d'échange d'informations. En l'absence de normes internationales sur l'identification et les transactions sur Internet, les utilisateurs se retrouvent régis par un système mis en place par des groupes d'entreprises, sans possibilité de recours.
De la même façon, on peut considérer l'ano-

nymat en ligne comme un moyen permettant aux internautes de s'exprimer librement mais une entreprise comme Facebook propose à ses membres de révéler les noms derrière les pseudonymes. Par ailleurs, l'anonymat peut poser un problème pour les forces de l'ordre et, selon certains députés américains, le simple fait de recourir au réseau Tor pour rester anonyme pourrait constituer un début de preuve que l'on cache des activités suspectes. Ces approches fondamentalement différentes d'une même question illustrent la nécessité d'établir des lois défendant des principes fondamentaux et l'intérêt général.

Pour autant, légiférer davantage est problématique à deux titres. En effet, les lois nationales peinent à s'appliquer dans le cadre d'Internet. On pourrait en conclure que la meilleure manière de protéger le cyberespace est de le laisser se développer sans qu'il fasse l'objet de réglementations. D'autre part, la multiplication des lois soulève le défi de leur réelle application (HADOPI, LOPPSI), sans même évoquer la difficulté pour les citoyens de toutes les connaître. Si nul n'est censé ignorer la loi, encore faut-il que la loi soit suffisamment simple ou compréhensible pour ne pas être ignorée. Envisager une loi sur le cyberharcèlement quand il existe déjà une loi sur le harcèlement apparaît par exemple superflu.

IV. Une gouvernance par un réseau décentralisé d'acteurs ?

Lors de la réunion des ingénieurs du Net (Internet Engineering Task Force - IETF) à Vancouver en novembre 2013, ces derniers ont décidé de réagir à la surveillance de masse en sécurisant les protocoles les plus utilisés, ce qui constituait une réponse politique par le biais d'outils techniques. Il peut donc exister un lien entre les décisions technologiques et les décisions politiques. On constate aussi que des décisions technologiques peuvent changer la politique et pas l'inverse. Ainsi la communauté scientifique s'est-elle opposée à la loi HADOPI. La gouvernance d'Internet pourrait au final revenir à une multitude d'acteurs qui, avec des stratégies communes et des tactiques différentes, obtiendraient de véritables résultats, un réseau décentralisé d'acteurs prenant des décisions allant dans la même direction.

Alcatel-Lucent's **cyber security solutions** and **Security Operations Center help you** anticipate and manage current and future threats to protect your networks, information, and applications in real-time.

For more information, visit our website:
alcatel-lucent.com

Alcatel·Lucent

B1 - La lutte contre les contenus illégaux sur Internet

Intervenants :

- Cécile DOUTRIAUX, avocate, Doutriaux-Vilar & Associés.
- Corinne THIERACHE, Avocat Associé, Responsable du Pôle Droit des nouvelles technologies, Droit de la propriété industrielle et droit pharmaceutique, SELARL CARBONNIER LAMAZE RASLE & Associés.
- Alexandre SOUILLE, Président, Olféo.
- Jean-François MASSELIS, Directeur, SIAVIC / INAVEM.
- Patrick PEGEOT, Mission interministérielle de lutte contre la drogue et la toxicomanie (MILDT).

Résumé des interventions :

Résumé des interventions : Considéré par beaucoup comme un espace de liberté d'expression, assurant l'égalité de traitement des flux de données, Internet n'est cependant pas un espace de non-droit. Il existe plusieurs types de contenus illégaux sur Internet : injures, diffamation, incitation à la haine raciale, menaces, harcèlement, provocation au suicide, atteintes à la vie privée ou au droit à l'image, atteintes à la propriété intellectuelle (y compris la contrefaçon de médicaments), pédopornographie, vente de stupéfiants... Selon les contenus, les moyens d'action, qu'ils soient répressifs ou préventifs, diffèrent et ont leurs limites.

I. Moyens de répression

La répression s'exerce en vertu de la législation française et, pour les sites hébergés à l'étranger, de la compétence internationale des tribunaux français, selon les théories de l'accessibilité, de la destination et de la focalisation, retenues alternativement par les jurisprudences successives, ce qui peut créer une instabilité juridique.

Les recours peuvent être exercés devant une juridiction civile ou pénale, selon les cas et l'objectif recherché. En effet, il n'est pas possible d'assigner contre X au civil. Or, les responsables de l'infraction commise ne sont pas toujours identifiés, en raison des caractéristiques d'Internet. Il est certes possible d'obtenir une adresse IP auprès des fournisseurs d'accès à Internet, en adressant une réquisition au Tribunal de Grande Instance, mais le propriétaire de l'ordinateur n'est pas nécessairement le responsable du délit. Une plainte au pénal, si elle aboutit, permet d'obtenir que la condamnation soit affichée sur le site, ce que privilégient certains ayants droit. En revanche, dans le cas des atteintes au droit d'auteur, notamment en France, une plainte au civil permet souvent de mieux compenser les dégâts économiques. Lorsque des organisations criminelles sont impliquées dans la contrefaçon, les services d'enquête cherchent toutefois de plus en plus à démontrer l'enrichissement. L'objectif est, en effet, que les avoirs criminels puissent être saisis à l'issue du procès pénal. Très souvent, l'insolvabilité des personnes responsables constitue un obstacle à l'obtention d'une indemnisation.

Concernant les atteintes à la personnalité et à l'e-réputation, c'est le droit de la presse qui s'applique. Le délai de prescription est passé de trois mois à un an depuis l'adoption de la loi n°2014-56 visant à harmoniser les délais de prescription des infractions prévues par la loi sur la liberté de presse. Selon la loi du 21 juin 2004 pour la Confiance dans l'économie numérique (CEN), le prestataire technique a un rôle neutre dès lors qu'il fait preuve de réactivité à la notification du site mis en cause. S'agissant des hébergeurs, il existe une jurisprudence fondatrice (Estelle Hallyday - Arrêt de la Cour d'appel de Paris du 10 février 1999) qui les assimile à des éditeurs. Le fournisseur d'hébergement qui permet la diffusion des contenus sur son serveur informatique voit sa responsabilité engagée puisqu'il n'est plus un simple vecteur de l'information, mais effectue une prestation durable de stockage des informations qu'il rend accessibles et qu'il a la possibilité de vérifier.

Le blocage des sites ou de certaines pages n'est pas toujours une solution facile à mettre en place : cette procédure est en effet très coûteuse pour les fournisseurs d'accès qui, par conséquent, peuvent s'y opposer. De plus, les sites litigieux peuvent réapparaître sur des sites-miroirs. Aussi peut-il être plus efficace de demander un dé-référencement, qui fait disparaître les contenus illicites des résultats ou du moins des premières pages des moteurs de recherche. Parfois, la solution

peut être de ne pas agir, car intenter une action produit une forme de publicité, «l'effet Barbara Streisand», qui peut se révéler plus néfaste que l'atteinte initiale et aller à l'encontre de l'effet recherché. Les avocats traitent donc chaque affaire avec attention pour adapter la réponse au mieux des intérêts de leurs clients.

En France, le choix a été fait de confier la lutte contre le téléchargement illégal et contre les jeux en ligne à deux Autorités administratives indépendantes : HADOPI (Haute autorité administrative indépendante pour la diffusion des œuvres et la protection des droits sur Internet) et ARJEL (Autorité de régulation des jeux en ligne). Force est de constater que la deuxième a davantage fait preuve de son efficacité : 29 dossiers transmis au juge par l'HADOPI contre 45 décisions de justice de blocage obtenues par l'ARJEL.

La lutte contre le trafic de drogues sur Internet, en pleine expansion, a quant à elle ses propres spécificités et constitue un enjeu de santé publique. La difficulté majeure est de contrer un phénomène nouveau qui se développe très rapidement. Pour ce type de trafics, les signalements sont très rares, il n'y a pas de trouble à l'ordre public et les bénéfices sont considérables, avec une prise de risque moindre. S'agissant des drogues « classiques », leur vente est facilitée par le « Darknet ». Fermer les sites, comme ont réussi à y parvenir le FBI et le Drug Enforcement Administration (DEA) en 2011 et 2012, nécessitent beaucoup de moyens et de nombreux enquêteurs. S'agissant des drogues de synthèse, composées de molécules non encore classifiées qui imitent les effets des drogues, elles ont la particularité de n'être ni autorisées, ni interdites. Elles sont proposées sur des sites de vente facilement accessibles, pour un prix deux à trois fois moins élevé que dans le cas d'une vente dans la rue, sans intermédiaire. Un des moyens de lutte consiste, en cas de saisie par les douanes de substances de synthèse, à retenir une infraction au Code de la santé publique ou d'exercice illégal de la médecine. La répression ne pourra cependant pas s'exercer efficacement sans une coopération internationale à laquelle travaille actuellement, au sein du conseil de l'Europe, le groupe Pompidou.

II. Moyens de prévention

Pour agir en amont sur les risques de contenus illégaux, il est indispensable d'informer et d'éduquer les individus. Dans le cas du harcèlement par Internet, il s'agit préalablement de mieux connaître le profil des auteurs. Une enquête réalisée dans le Nord-Pas-de-Calais auprès de 3 000 jeunes fait apparaître que dans 70% des cas de cyberintimidation et de cyberharcèlement, la victime connaît l'auteur, que ce dernier est souvent mineur et de plus en plus souvent de sexe féminin. Un tiers environ des jeunes interrogés se déclarent victimes d'insultes, de messages haineux, de menaces ; l'écart entre victimes filles et garçons est faible. Un travail de sensibilisation, qui mériterait d'être généralisé, est mené

auprès des jeunes de 15-18 ans, afin de les faire réfléchir aux enjeux de l'univers numérique, au statut de victime et de leur faire prendre conscience qu'ils peuvent eux-mêmes devenir acteurs. Les spécificités d'Internet permettent de renverser le rapport de force qui prévaut dans la vie réelle et d'encourager les auteurs en leur donnant une impression de confidentialité et d'impunité.

D'une manière générale, l'auto-responsabilisation des citoyens peut réduire le nombre de victimes de contenus illégaux. Ainsi, en France, la liste des 50 sites autorisés à vendre des médicaments, consultable en ligne, devrait éveiller la méfiance des individus quant à la qualité des médicaments disponibles sur d'autres sites. Les citoyens ont également la possibilité de signaler sur une plate-forme dédiée les sites, pages ou propos qu'ils jugent illicites ou contraires aux bonnes mœurs. Cet objectif de sensibilisation peut toutefois être manqué. Ainsi, Hadopi n'est pas parvenue à convaincre que tout travail de création mérite rémunération. En l'occurrence, une autre voie pourrait consister dans le développement par les sociétés commercialisant des biens culturels de nouveaux modèles économiques, adaptés aux usages actuels. Pour contrer la vente des drogues de synthèse, une grande réactivité est nécessaire afin que la classification en substance stupéfiante intervienne plus rapidement, une nouvelle substance apparaissant chaque jour sur le marché. Les usagers sont en effet attachés à un produit dont ils connaissent la qualité et hésitent à en changer. Il faudrait développer également une politique de réduction des risques, qui consiste à prévenir par un message d'avertissement le consommateur de l'ensemble des conséquences de l'usage des drogues, en veillant à ne pas faciliter la commission de l'infraction.

Une autre solution est d'avoir recours à des dispositifs de filtrage. Entre 70 et 80% des entreprises s'équipent et décident librement des accès qu'elles autorisent à leurs employés. Elles se protègent également par des logins nominatifs attribués à chaque collaborateur et par des chartes informatiques . Celles-ci, signées par toutes les parties, rappellent la loi et les usages afin de responsabiliser chaque collaborateur. Les entreprises procèdent ainsi à la régulation à l'intérieur de son entité entre libertés et contraintes.

Au niveau international, s'il existe quelques points d'accord, tels que la lutte contre la pédopornographie, beaucoup de divergences demeurent. Chaque État adapte sa lutte et pratique des dénis d'accès en fonction de sa législation, de ses valeurs et de sa culture. Les États-Unis souhaiteraient que soient censurées des catégories identiques dans tous les pays du monde, selon une conception universaliste de ce qui est acceptable ou non.

B2 – La coopération public privé : quel rôle pour les acteurs privés ?

Intervenants :

- Pierre-Luc REFALO, Directeur des offres de conseil sécurité, Sogeti France
- Philippe BLOT, Chef de division produits et services de sécurité, ANSSI
- Jaan PRISALU, Directeur général de l'Estonian Information System's Authority
- Thierry ROUQUET, Président de la Commission Cyber Sécurité, AFDEL
- Ulrich SELDESLACHTS, Managing Director, Leaders in Security (LSEC)

Résumé des interventions :

Les entreprises privées sont en première ligne dans la mise en place d'une démarche globale de cyberdéfense nationale. Leur maîtrise des données (hébergeurs, opérateurs, fournisseurs de services Web en tous genres) renforce l'intérêt du partage d'informations sensibles au sein de réseaux de confiance associant entreprises et agences gouvernementales. Leur expertise peut quant à elle être mise à profit via la fourniture de services et de produits de cybersécurité. L'absence de frontières dans l'espace de la microéconomie et de la cybercriminalité rend nécessaire le développement de collaborations internationales en matière de cyberingénierie. Une harmonisation des exigences technologiques et de confidentialité entre les États permettrait de répondre aux organisations cybercriminelles supranationales.

I - Des fraudeurs de plus en plus efficaces

D'après les récentes études du Centre d'Analyse Stratégique, il est primordial d'élever le niveau de sécurité des systèmes d'information pour pouvoir préserver notre compétitivité économique et la souveraineté nationale dans le domaine informatique. En effet, la confiance des utilisateurs dans le système global de cybersécurité est fragilisée en cas d'attaques.

Les cyberattaques deviennent de plus en plus complexes et les fraudeurs sont désormais de véritables professionnels qui peuvent aisément s'affranchir des frontières au sein du cyberespace. Aujourd'hui, la cybercriminalité relève véritablement du crime organisé : atteinte à la vie privée par les processus d'ingénierie sociale, fraude voire vols d'identifiants bancaires, etc.

Par ailleurs, les usages modernes tels que le « cloud computing » rendent les systèmes d'information particulièrement vulnérables. En effet, de plus en plus d'appareils du quotidien sont connectés entre eux et des données sensibles circulent des uns aux autres via Wifi ou encore Bluetooth. Malgré la création en 2009 de l'Agence Nationale de Sécurité des Systèmes d'Informations (ANSSI), le niveau global de sécurité informatique reste insuffisant face à l'efficacité des cyberdélinquants du 21e siècle.

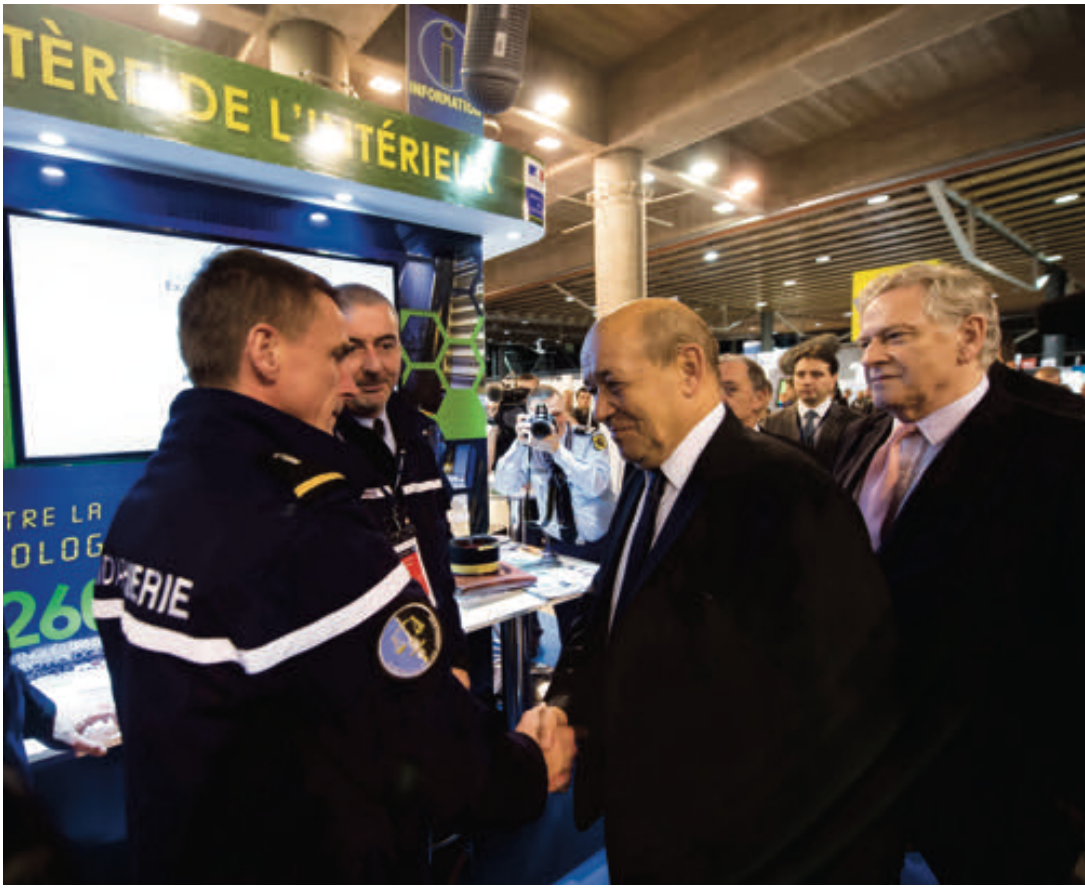
II - Une coopération public-privé délicate à mettre en œuvre

Il faut s'interroger sur le rôle que doit jouer le secteur privé vis-à-vis du secteur public. À titre d'exemple, une des missions de l'ANSSI est de définir des standards de sécurité auxquels doivent se conformer les industriels qui éditent les différents logiciels disponibles sur le marché. Les éditeurs de logiciels ont besoin d'une feuille de route commune leur permettant de contribuer à l'émergence d'une offre nationale. Ceci afin, d'une part, de garantir la conquête de l'export et, d'autre part, renforcer les entreprises nationales en cybersécurité.
La disparition des frontières dans le cyberespace génère dans le même temps des problématiques de coopération internationale. Une bonne coopération public-privé est donc importante afin que les acteurs publics et privés, au niveau national et international, progressent au même rythme en termes de besoin et d'offre.

Par ailleurs, un des problèmes majeurs rencontrés aujourd'hui en cybersécurité est la timidité des investisseurs qui ne perçoivent pas l'étendue des bénéfices à tirer de ce secteur. Le cadre politique général ne favoriserait pas non l'investissement en cybersécurité. Pourtant, l'émergence des fonds privés est un gage de progrès en matière de sécurité : l'investissement qui en résulte permet de

porter l'effort sur la recherche et le développement. Mais là encore, les difficultés sont nombreuses et le cadre juridique, jugé trop restrictif, limite le champ de travail des chercheurs en informatique. La structuration des éditeurs de logiciels de sécurité repose donc sur deux conditions fondamentales : la première porte sur l'obtention de financements publics nationaux ou supranationaux pour stimuler la recherche et le développement afin de pouvoir générer l'innovation nécessaire dans le domaine de la cybersécurité. La seconde condition porte sur la création de partenariats entre les grands groupes européens et les PME, souvent très innovantes mais trop fragiles pour pouvoir se lancer seules sur le marché de l'export.

Enfin, il semble complètement illusoire de vouloir progresser en développant la coopération sur une base exclusivement nationale. En effet, puisque le cyberespace n'a pas de frontière physique, les acteurs de la cybersécurité ne peuvent qu'avoir une portée supranationale. Une industrie forte ne peut donc émerger qu'avec l'appui d'une organisation cohérente a minima au niveau européen pour pouvoir faire face à la toute-puissance américaine et à son marché intérieur considérable. Mais les exigences européennes sont différentes de celles des États-Unis. La France, qui est un gros pôle de certification de logiciels, souhaite un niveau de confidentialité de la production nationale de logiciels supérieur à celui des États-Unis. Par ailleurs, un éditeur de logiciels certifié en France n'est pas forcément reconnu comme tel en Allemagne ou au Royaume-Uni. Face à ces incohérences, il semble nécessaire de s'efforcer d'établir un label de confiance à un niveau plus global pour pouvoir apporter une réponse de même ampleur que celle développée par les organisations de fraudeurs.


DE L'
TÉRIEUR
TRE LA
OLOG
GENDARMERIE

B3 – Réponse à incident en entreprise

Intervenants :

- Colonel Éric FREYSSINET, Chef de la division de lutte contre la cybercriminalité, Gendarmerie Nationale
- Blandine POIDEVIN, avocat, Juris Expert
- Guillaume ARCAS, Sekoia
- Cyrile BARTHELEMY, Directeur associé – Activité sécurité, INTRISEC
- David BOUCHER, Consultant en Sécurité des SI, Orange Business Services
- David BIZEUL, Responsable Computer Incident Response Team (CSIRT), Cassidian Cybersecurity
- Laurent MARECHAL, Directeur Conseil SSI – Opérateur Publics, Thales Communication & Security

Résumé des interventions :

De nombreux problèmes touchent aujourd'hui les sociétés en termes d'attaque informatique et en particulier d'atteinte aux systèmes de traitement automatisé de données. Il est dès lors essentiel d'identifier les bons comportements afin de répondre à l'incident de façon optimale. Cette démarche implique nécessairement de planifier la gestion des mécanismes de sécurité, de connaître les risques et d'appliquer de bonnes pratiques de sécurité et de surveillance.

I – Prévoir, c'est déjouer les crises

Le constat est alarmant. Trop peu de clients aujourd'hui font appel aux sociétés spécialisées dans la protection logicielle en prévention d'attaques de leur système informatique. Lorsque l'attaque se produit, il est malheureusement trop tard. Une démarche préparatoire aurait pourtant permis de s'organiser et de trouver des solutions par des processus adaptés et spécialement orientés vers la détection.

La prévention de ce type d'incident permet aux entreprises d'acquérir les bons réflexes pendant que la situation est normale et d'être accompagnées lors d'une attaque. Il s'agit de réagir en limitant les dégâts, c'est-à-dire de restreindre l'attaque, soit d'une manière physique en arrêtant ses machines, soit par le biais de logiciels spécialisés dans les contre-mesures. Ces méthodes ont pour objectif d'analyser en profondeur les systèmes infectés pour identifier l'auteur de l'intrusion et d'ajuster la réponse des systèmes de sécurité.

Les sociétés de sécurité informatique œuvrent aujourd'hui auprès des dirigeants pour les convaincre d'investir, de modifier et d'améliorer la sécurité de leurs systèmes, en prévention d'une attaque. Le point clef pour les clients est désormais de connaître les risques inhérents à leurs installations et les limites de leur système de défense afin de trouver la meilleure réponse en cas d'attaque. 2009 de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI), le niveau global de sécurité informatique reste insuffisant face à l'efficacité des cyberdélinquants du XXIe siècle.

II - Résoudre avec un coût réduit et dans un temps minimum

Une fois les systèmes hors service, les entreprises ont besoin de solutions immédiates. Il s'agit pour elles de trouver le meilleur compromis entre le temps de résolution et le coût engendré. Du point de vue des professionnels de la sécurité informatique, remettre les systèmes en marche ne permet pas de se prémunir contre une nouvelle attaque similaire. Il est nécessaire de réaliser une analyse plus profonde afin de déterminer les origines exactes de l'attaque. Cette démarche est cependant chronophage et donc coûteuse pour les clients. Il s'agit de leur expliquer que leur intérêt, malgré les apparences, passe par cette action curative et préventive en profondeur.

La solution semble simple : mettre en place des partenariats de protection sur le long terme afin de limiter les coûts non planifiés. Cela permet, d'une part, aux clients, de connaître le coût de leur sécurité et de leur intégrité informatique, et d'autre part, aux professionnels, de mettre en place un suivi de chaque client avec une connaissance de ses points faibles dans le but de lui apporter une réponse optimale.

III – Vérité et image de marque

Le sentiment de malaise, lorsqu'un pirate parvient à pénétrer un système de sécurité d'une banque ou d'une assurance, est réel. Comment expliquer aux clients que l'ensemble de leurs informations

personnelles ont été détournées ou même simplement que quelqu'un a pu y accéder malgré les protections du serveur ? Toute entreprise tient avant tout à préserver son image. L'impact qu'aurait par exemple une attaque massive réussie sur une grande banque et la révélation du piratage des numéros de compte de tous ses clients est aisément imaginable. Pour les sociétés d'antivirus, une grosse difficulté réside dans le fait qu'elles ne sont que rarement informées des problèmes majeurs rencontrés par leurs clients, ces derniers craignant d'ébruiter un problème de sécurité. Ce manque de confiance dans les sociétés de sécurité informatique entraîne, en outre, une perte de temps non négligeable dans les réponses que ces dernières peuvent apporter.

IV - Enquête et réparation

Il est délicat d'estimer un préjudice à la suite d'une attaque informatique. Le temps passé à réparer le système n'est pas le seul paramètre financier à prendre en compte. La valeur des informations dérobées ou détruites doit aussi être évaluée. La souscription d'un contrat avec une société d'antivirus permet de réaliser un audit des données de la société cliente (droit d'auteur, secret professionnel), mais aussi de connaître le cadre juridique spécifique qui s'applique aux salariés et aux sous-traitants. Les entreprises qui n'appellent à l'aide qu'une fois attaquées rendent beaucoup plus difficile la quantification du préjudice. Sans connaissance des systèmes initiaux et des données qui s'y trouvaient, les experts ont les plus grandes difficultés à évaluer l'étendue des préjudices. Il leur est également difficile d'estimer la durée nécessaire à la remise en route d'un système qui leur est inconnu. Or, il est nécessaire d'établir un constat du préjudice subi pour entamer dans de bonnes conditions une démarche de remboursement, soit par une assurance, soit par la justice en cas de procès.

Conclusion

Appliquer les bonnes pratiques ainsi que des protocoles rigoureux de sécurité passant notamment par une protection logicielle adaptée peut permettre de détecter une difficulté. La mise en place des outils techniques ainsi que la sensibilisation des utilisateurs devraient être des réflexes, tout comme appeler un professionnel dès lors qu'une attaque semble se produire. Il s'agit de ne pas perdre de temps afin de stopper l'attaque et de pouvoir la tracer.
Les clients ont trois exigences. Ils veulent savoir comment s'organiser face à une attaque, comment mettre en œuvre le process spécifique installé par le professionnel de la sécurité informatique et, enfin, pouvoir faire appel sans délai à des ressources en interne ou à des prestataires de services afin de juguler l'attaque.

L'objectif pour les professionnels est, en outre, de capitaliser les différentes expériences après chaque intervention afin d'adapter les process et ainsi de réagir plus vite dans les situations d'intervention futures. La gestion de la pré-crise reste, en effet, un axe d'effort.

B4 – Peut-on réellement être anonyme sur Internet ? Technologies et limites.

Intervenants :

- Jean-Paul PINTE, Maître de conférences, Cybercriminologie, université catholique de Lille,
- Stéphane BORTZMEYER, Ingénieur Recherche et développement, AFNIC
- Garance MATHIAS, Avocat à la Cour, Cabinet d'Avocats Mathias
- Grégoire POUGET, RSF, Responsable nouveaux Médias
- Erik BULLIER, EBI-Consulting, COE

Résumé des interventions :

La liberté de l'information, l'égalité de l'accès à l'information, l'universalité des moyens d'information et l'absence de frontières dans le cyberespace sont des « leurres numériques ». L'anonymat n'est pas un droit et, malgré différents outils qui peuvent favoriser une moindre vulnérabilité de l'internaute, l'identité numérique trace durablement chaque utilisateur. Le respect de la vie privée de chaque internaute dans l'espace numérique se conçoit par référence à l'article 12 de la Convention universelle des droits de l'homme. L'enjeu de la libre circulation des informations et de l'utilisation des données personnelles n'est pas seulement politique et idéologique, mais aussi économique.

L'application du droit à l'anonymat est possible. Il implique la réappropriation de l'identité et le respect du principe de consentement. Les évolutions porteront sur les conditions de portabilité des données, le droit à l'oubli et le droit de s'opposer à la collecte d'information. L'une des solutions serait de déployer des systèmes qui sont anonymes par défaut et non des systèmes obligeant l'internaute à se protéger. Enfin, l'internaute est un citoyen numérique avec des droits mais aussi des devoirs. Les institutions devraient être en mesure de déterminer l'espace de la vie privée.

La protection d'une aire de vie privée existe mais elle est inégalitaire et discriminatoire. Elle favorise la vulnérabilité de populations d'internautes qui n'ont pas de connaissance des outils et surtout aucune éducation relative à leurs droits et devoirs d'individu sur internet. des outils et surtout aucune éducation relative à leurs droits et devoirs d'individu sur internet.

I – Les enjeux de l'anonymat sur internet

L'interpénétration d'Internet dans les actes quotidiens de chacun implique qu'aujourd'hui toute action laisse des traces numériques. Les internautes ne sont pas conscients que la décision de renoncer à l'anonymat et de perdre un peu de vie privée est le plus souvent prise sans consentement éclairé de leur part. De plus le sentiment de sécurité des individus s'exprime essentiellement dans l'environnement physique de chacun. L'espace numérique est inodore, informel, intemporel c'est-à-dire invisible et ses dangers sont plus difficiles à appréhender. Ainsi, il n'a pas d'existence pour beaucoup d'internautes. En fait, on peut se demander où est l'enjeu de l'anonymat alors que la majorité de la population internaute semble avoir intégré la réduction de l'espace privé comme un progrès des relations sociales.

Le corollaire de la notion du droit à l'information est celle du consentement libre et éclairé de chaque internaute. Le droit à l'anonymat et le droit à l'oubli sont inhérents aux droits de l'homme et plus particulièrement à la notion de vie privée telle que la conçoit l'article 12 de la déclaration universelle des droits de l'homme. La directive européenne du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données constitue le socle commun pour tous les pays de l'Union européenne en matière de protection des données personnelles. La directive a été transposée en droit français par la loi du 6 août 2004 relative à la protection des personnes physiques concernant les traitements de données à caractère personnel.

Il convient d'aller dans le sens de l'histoire sans nier le modèle de l'internet basé sur l'économie de la multitude. En revanche, les internautes sont responsables et acteurs de la protection de leur vie privée. Tout le monde devrait avoir droit à l'anonymat, c'est un élément essentiel de la liberté individuelle.

II – Les moyens d'action des internautes. technologiques et policières

L'accès à l'anonymat est très inégalitaire, notamment au regard des outils à maîtriser. En effet, alors que l'anonymat devrait être institué par défaut à tous les niveaux d'entrée sur internet, la démarche est en réalité difficile et coûteuse. Les outils comme Tor, les proxys, les VPN sont complexes d'utilisation. Ils sont par ailleurs onéreux et peuvent altérer la qualité de connexion de l'internaute selon les performances de son matériel. Aussi, ils nécessitent une maîtrise parfaite de l'environnement numérique. Alors que l'imbrication des mondes matériel et immatériel est de plus en plus forte, la décision de protéger son anonymat résulte d'une prise de conscience d'un danger immatériel. Chacun connaît la notion de danger et la nécessité de se protéger physiquement. Cette notion doit désormais intégrer l'espace informel

numérique où la protection de l'intégrité virtuelle implique une quatrième dimension de notre identité. Le droit à la sécurité et au maintien le plus large de sa vie privée n'est accessible qu'à ceux qui ont la pratique, la connaissance et les moyens de comprendre et d'utiliser ces outils.

Il peut y avoir trois niveaux d'action pour permettre la réappropriation d'une partie de sa vie privée par le respect du droit à l'anonymat sur Internet. Les pouvoirs publics ont les moyens d'intervenir par une législation plus protectrice de l'utilisateur d'internet. En 2012, un nouveau projet de règlement relatif à la protection des données personnelles a été proposé en vue de modifier la directive européenne du 24 octobre 1995. Ce projet porte sur la notification des violations de traitements de données personnelles, les analyses d'impacts préalables pour les traitements les plus "risqués", le durcissement de la définition du consentement, la création de nouveaux droits concernant l'oubli et la portabilité des données ainsi que l'évolution de la fonction des CIL.
Le second niveau concernerait la modification des protocoles internet, laquelle permettrait à l'internaute d'envoyer moins d'informations à son insu. L'utilisation de différents outils d'anonymat répond à une stratégie de communication (quel récepteur à quel moment pour quel objectif ?). Il est logique et nécessaire pour l'internaute de compartimenter, c'est-à-dire d'avoir une identité numérique variable donnant accès, en fonction de ses interlocuteurs, à tout ou partie de ses informations. Le recours à un pseudonyme peut être une option pour retrouver l'anonymat : il permet de créer une identité temporaire et masquée. Le recours au chiffrement peut aussi apporter une sécurité mais il limite l'accès à l'information.
Enfin, la sensibilisation au numérique et aux droits individuels devrait s'intégrer à toutes les étapes de la formation. Il importe de développer l'éducation au discernement numérique et à la notion de consentement. Ces enseignements sont seulement les garants de la protection individuelle mais aussi de la liberté de communication, c'est-à-dire du droit à l'information tel que défini par l'article 19 de la Déclaration universelle des droits de l'homme.

B5 - Panorama des stratégies étatiques

Intervenants :

Denis FORTIER, Directeur de la rédaction, AEF Sécurité Globale
Professeur XU LONGDI, China Institute of International Studies ;
M. Oleg DEMIDOV, Program Director, International Information Security and Global Internet Governance, PIR Center ;
M. David N.SENTY, Director, Cyber Operations, MITRE .
Mme Frederick DOUZET, Titulaire de la Chaire Castex de Cyberstratégie (IHEDN/Cassidian Cybersecurity) – Directrice adjointe de l'Institut Français de Géopolitique de l'Université Paris 8.

Résumé des interventions :

Les stratégies suivies par les États diffèrent en fonction de leurs objectifs et ambitions. La Chine, immense réservoir d'utilisateurs d'Internet et acteur croissant dans les nouvelles technologies, rattrape à marche forcée les acteurs occidentaux et asiatiques historiques, adaptant progressivement sa politique de sécurité et la qualité de ses réseaux. La Russie met en place sa propre approche de la sécurité numérique sans y associer encore pleinement les acteurs privés. Les Etats-Unis, quant à eux, se sont focalisés sur la protection des systèmes, délaissant un peu une approche anticipative.

I. La politique chinoise en matière de cybersécurité

A la fin de l'année 2013, la Chine comptait 618 millions de « citoyens du net » et 81% des Chinois disposaient d'un accès à Internet. L'e-commerce connaît une croissance exponentielle portée par l'avènement des smartphones et autres moyens mobiles. La façon de consommer évolue et de nombreuses entreprises ont fait du marketing en ligne leur priorité pour augmenter leur chiffre d'affaires.

Pour le gouvernement chinois, l'Internet est un vecteur de modernité économique et d'ouverture au monde. Il a donc très vite pris une série de mesures visant à promouvoir cette modernisation sociale. Ainsi, en 1993, le pays a accueilli la Conférence conjointe sur l'informatisation économique pour marquer sa volonté de prendre une part active dans la gestion du réseau informatique de communication. Par ailleurs, le gouvernement a investi 4300 milliards de Yen dans les infrastructures Internet entre 1997 et 2009, notamment dans l'extension du réseau de fibres optiques sur la totalité du pays (longueur totale de 8267 millions de kilomètres dont 840000 km de câbles longue distance). Il mise également sur la recherche et développement pour promouvoir un Internet de nouvelle génération et un réseau plus fiable. La Chine doit néanmoins faire face à de nombreux problèmes notamment liés aux disparités économiques entre ses régions orientales et occidentales.

Depuis 1994, la Chine a promulgué une série de lois visant à réguler le réseau à la suite des décisions du Comité Permanent de l'Assemblée Nationale Populaire (NPC) relatives à la sécurité au sein du cyberespace, la gouvernance de l'Internet, le piratage, les signatures électroniques...etc.

La Chine a été, ces dernières années, la cible favorite des cyberattaques. Même si les progrès dans le domaine des technologies de l'information et de la communication sont indéniables, la Chine reste un pays qui accuse un retard par rapport aux pays occidentaux. La Chine se trouve, pour cette raison, dans un état de « cyber insécurité ». Réduire cette dernière constitue l'un des défis du gouvernement Chinois. La Chine compte aujourd'hui le plus grand nombre de netizens (citoyens du net) mais la plupart ne sont pas conscients des menaces qui pèsent sur le cyberespace et ne prennent pas ou peu de précautions, notamment les utilisateurs de smartphones. La Chine doit également faire face à la pression exercée par les autres pays développés dans la lutte contre la cyber insécurité. Ces trois dernières années, beaucoup de pays, et plus particulièrement les États Unis, ont renforcé la protection de leur cyberespace. Pour promouvoir les dialogues bilatéraux et une cyber coopération internationale, la Chine et les Etats-Unis ont déjà mis en place un groupe de travail (SED : Strategic and Economic Dialogue) et ont participé au WSIS (World Summit on the Information Society) cette année. Des forums les ont réunis à six reprises (quatre fois avec le Royaume Uni)

depuis 2007. Des échanges ont lieu également avec l'Union Européenne, la France, l'Allemagne et la Corée du Sud mais aussi Interpol.
En matière de coopération internationale, le CNCERT/CC représente la plate-forme majeure pour les différents centres d'alerte et de réaction aux attaques informatiques (CERT – Computer Emergency Response Team). Cette plate-forme permet une coopération technique transfrontalière en matière de cyber sécurité. D'autres organismes techniques tels que l'ISC (Internet Society of China) ou le CNNIC (China Internet Network Information Center) s'impliquent également dans les échanges internationaux.

II. Le rôle et le projet du Pir Center de Moscou

Organisme indépendant non gouvernemental fondé en avril 1994, le PIR Center est le principal institut d'expertise et de recherche russe dans le domaine de la sécurité internationale, du contrôle et de la non-prolifération des armes nucléaires et de destruction massive. Il joue aussi le rôle d'intermédiaire entre le gouvernement russe et les experts internationaux. Son objectif est de contribuer à une coopération internationale plus efficace. Ce centre va bientôt publier le premier Livre Blanc sur la cybersécurité et la gouvernance mondiale de l'Internet.
Il n'existe cependant pas d'organisme ou d'agence de coordination pour les problèmes liés à la cybersécurité. Les analyses réalisées par les instituts non gouvernementaux ne sont pas systématiquement prises en compte lorsqu'il s'agit de prendre des mesures dans ce domaine. On peut toutefois constater quelques avancées significatives comme, par exemple, l'initiative personnelle du sénateur Gattarov qui, fin 2012, a élaboré, avec l'aide d'experts, un projet de concept de stratégie nationale en matière de cybersécurité. Celui-ci a fait l'objet de discussions au parlement russe en novembre 2013 et ses grandes lignes ont été approuvées mais, à ce jour, aucune loi précise n'a été votée.
Pourtant, le gouvernement russe est conscient des enjeux et a pu identifier quatre types de menaces à la sécurité de l'information : les menaces militaires, politiques, le cyberterrorisme et les atteintes à la sécurité intérieure et la souveraineté de l'État. Sur le plan international, les Russes adhèrent au code de déontologie international sur la sécurité de l'information et ont fait, depuis 2011, des propositions pour réglementer le cyberespace, diversifier le système de fibres optiques (y compris les câbles intercontinentaux) et contrer les différents types de menaces. Leur attention se porte prioritairement aujourd'hui sur le management du système DNS (Système des noms de domaines) et de la distribution des adresses IP.

III. L'approche américaine

Les Américains ont porté prioritairement leurs efforts sur la protection des systèmes plus que sur l'anticipation des problèmes. Les systèmes de sécurité semblent aller moins vite que les multiples virus pirates et ne peu-

vent contrer efficacement ces menaces en perpétuelle augmentation. Face à cette vulnérabilité constante, il semble impératif que les utilisateurs de l'Internet deviennent des acteurs à part entière en matière de cybersécurité, voire de « cyber intelligence » et communiquent sur les diverses attaques qu'ils subissent. Une typologie de menaces existantes par secteur peut alors être établie. Grâce à ce « threat sharing model » (système de partage d'informations sur les menaces) et au « crowdsourcing » (collecte de données grâce à la coopération d'un maximum d'internautes), au lieu de parler aujourd'hui de « hackers » individuels, on peut identifier plusieurs groupes qui ciblent des secteurs précis (la propriété intellectuelle, les finances...). Les différents secteurs peuvent alors élaborer des typologies de menaces précises et permettre aux utilisateurs de protéger leurs données en connaissance de cause. Les systèmes d'échanges standardisés sont par exemple Cybox (Cyber observable Expression)et Stix (Structured threat Information Expression).

B6 – Logiciel libre et cybersécurité

Intervenants :
- Nicolas BARRETO-DIAZ, responsable des systèmes d'information, FIDH

Animateurs :
- Thomas GIRARD, directeur du département conseil&SSI, CS communication&systèmes
- Thibault KOECHLIN, head of consulting, NBS System
- Éric LEBLOND, hacktiviste, OISF
- Jérôme NOTIN, président de la société NOV-IT , chef de file du projet DAVFI,
- Luc RENOUIL, Hexatrust

Résumé des interventions :

La France est reconnue pour son excellence dans l'implémentation des logiciels libres. Mais le logiciel libre constitue-t-il la panacée ? Quelle est sa valeur ajoutée en termes de cybersécurité ? Existe-t-il une souveraineté du logiciel libre ? Autant de questions qui montrent l'acuité de cette problématique qui a animé les débats de la table ronde. Compte rendu de séance sous forme de questions-réponses.

« Quand vous êtes en position de domination commerciale et stratégique, ce serait trop tentant de ne pas utiliser cette suprématie ; c'est donc un problème de souveraineté ». C'est cette citation d'Eric FILLIOL va servir de fil rouge aux échanges de cette table-ronde abordant l'implémentation du logiciel libre les obstacles, le financement, le recrutement, la valeur ajoutée...

Il y a antagonisme entre le logiciel privateur (éditeur) et le logiciel libre. « On ne peut pas se protéger quand on utilise les outils de l'adversaire. Rappelons que la quasi-totalité de nos systèmes d'information sont équipés de produits américains... » souligne Éric Filliol pour qui « il faut une révolution en profondeur qui aboutisse à imposer, comme les États-Unis le font chez eux, une exception sur les produits de sécurité et de technologie ».

I. Le recours aux logiciels libres. Expérience et avis.

Il est nécessaire, en liminaire, de différencier l'open source (avantageux pour les éditeurs de logiciels qui, à partir d'un code source, peuvent le modifier et le revendre) du logiciel libre (dont la licence est libre et qui permet, à ce titre, à l'utilisateur de s'appuyer sur un socle de quatre droits intangibles : exécuter, étudier, redistribuer et modifier le logiciel, mais chaque modification reste elle aussi libre). On bénéficie dans un premier temps de l'apport des autres personnes et on restitue à la communauté par sa propre contribution le fruit de son travail.
Les avis sont divergents en ce qui concerne le modèle d'entreprise ou le modèle d'affaires. Pour les uns, la vente du seul service autour d'un logiciel libre ne suffit pas. Il faut y rajouter de l'intégration dans les systèmes d'information, de la main-d'œuvre, du suivi tout en reconnaissant que le recours à une version open source reste une solution pertinente pour les phases de test et de formation. Les autres, malgré la difficulté de trouver un modèle commercial au niveau de l'open source, sont convaincus qu'on peut arriver à en vivre en vendant du service.
La difficulté, sur des sujets sensibles, à réussir face à une administration française régulatrice qui se montre très tatillonne à faire propager ce type de solutions est mise en exergue. De même, sur la question financière de l'implémentation, il subsiste une différence d'approche en matière de coût complet entre les entreprises, où il est bien maîtrisé, et les administrations où sa mise en œuvre se révèle plus complexe.

II. Le financement en France est-il suffisant ?

Il existe des solutions, notamment au travers du programme gouvernemental « investissements d'avenir » qui financent l'innovation en France. Mais la constitution des dossiers exige bien souvent de s'associer avec un grand groupe car le rapport de forces n'est

pas en faveur de PME modestes, notamment dans le monde de la Défense.
Un des autres avantages à avoir recours à l'open source, c'est la capacité de disposer de tests fiables réalisés par des tiers. Alors qu'il est coûteux et difficile de faire évaluer par des sociétés spécialisées l'insécurité d'un logiciel, avec parfois à la clef des résultats incertains ou dépassés, il est beaucoup plus facile de faire un appel à la communauté du libre pour procéder à ces tests.
Il y a aussi une forme de bienveillance de certains éditeurs qui laissent volontairement un logiciel en mode ouvert pour des projets open source. Cette fraternité de la communauté du logiciel libre permet de donner à des structures - indépendamment de leur taille - les moyens d'accéder à des outils qui sont aujourd'hui réservés à des groupes puissants.
Une alternative au financement consiste à avoir recours à certaines Fondations qui soutiennent des initiatives permettant de développer des logiciels dans des domaines ciblés.

III. La communauté du libre est un acteur essentiel pour auditer le code. Comment arrive-t-on à manager cette communauté pour qu'elle ne constitue pas un frein ?

Dans une communauté qu'on ne contrôle pas, il peut de prime abord s'avérer difficile de faire interagir les membres pour en tirer des effets toujours constructifs. Mais la communauté a tendance à se piloter elle-même et on voit se développer rapidement, dès que l'attrait du produit est perçu, un esprit communautaire se caractérisant par des retours d'audits exhaustifs, une capacité à monter des challenges, voire une propension à créer des communautés encore plus importantes afin de mettre le logiciel à l'épreuve et de l'analyser sous toutes ses coutures.
L'open source permet ainsi de s'approprier le travail des autres et de le valoriser. Après, il faut jouer le jeu et redistribuer à ces communautés le fruit de ses propres avancées.
La communauté suppose une confiance. Si son action n'exclut pas le côté sympathique de la chose, elle doit cependant être soustendue, comme dans le monde industriel, par la recherche de l'efficacité. Il convient de structurer la communauté pour faire en sorte que les outils soient connus de tous et il faut vraiment faire preuve davantage de clarté sur les modes de pilotage afin d'avoir une dynamique plus efficace.
En matière de cybersécurité, le logiciel libre apporte une certaine assurance du fait de la communauté qui y travaille et l'open source est un levier important pour avoir des modes de confiance et démontrer la sécurité du système.

IV. En termes de recrutement, le logiciel libre est-il une valeur ajoutée pour un candidat ?

On trouve en France des produits d'excellente facture développés par des personnes com-

pétentes. Dans le domaine de la sécurité, la connaissance et la pratique de l'open source sont des atouts indéniables dans les profils recherchés. On reste très sensible à la personnalité du candidat qui dispose d'une expérience open source.
Tout le challenge réside ensuite à favoriser l'intégration harmonieuse de ces personnes douées dans des organisations de type industriel auxquelles elles ne sont pas forcément préparées. Il faut des gens qui réussissent à s'intégrer dans une grande équipe, fassent preuve de maturité et soient capables de résister au stress d'encadrement, au nouvel environnement de développement qui peut être assez sensible et montrent des facultés d'adaptation aux contraintes management-projet.
L'open source constitue un vivier de compétences vers lequel on se tourne régulièrement pour détecter des personnes aux qualifications avérées, notamment dans le secteur complexe de la sécurité offensive pour lequel on sait qu'il y a des lacunes de compétences techniques en France. Avoir une expérience open source contribue à l'accélération de la professionnalisation car le candidat, souvent jeune, va rapidement être confronté à l'exploitation de documentation, au chiffrement, au recours à plusieurs langues et donc la participation à des projets open source va lui permettre de se « séniориser » plus rapidement que s'il suivait une filière technique classique dans un établissement scolaire.
En outre, les communautés détectent rapidement les aptitudes de ceux qui peuvent y faire leurs premières armes.

V. L'audit et la relecture de codes sont-ils organisés de manière systématique ? Existe-t-il des phases de test ?

Il n'existe pas de règle stricte, mais c'est le phénomène de la loi des plus grands nombres qui s'applique. Plus il y a de personnes qui testent, plus le niveau de sécurité du logiciel sera élevé. En ce sens, l'open source garantit une qualité de code, surtout si on a une communauté avec plusieurs développeurs qui ne partagent pas les mêmes intérêts. La confrontation est dès lors source de richesses.
Maintenant, il faut convenir que le niveau de maturité n'est pas optimal et que des progrès doivent être réalisés, notamment pour les projets sensibles, en mettant par exemple en œuvre un schéma directeur fixant des objectifs et répertoriant les bonnes pratiques. Pour sa part, l'ANSSI pourrait apporter sa contribution en stimulant l'audit de codes qui reste une étape toujours laborieuse.

VI. Comment proposer l'utilisation de logiciels libres dans son entreprise ?

Dans le logiciel propriétaire, il faut parfois avoir de la chance car on peut se retrouver confronté à des volumes de codes et d'obscurité complexes qui sont tels qu'il suffit de

mettre le doigt au mauvais endroit pour que tout s'effondre. Dans le logiciel libre, plusieurs personnes se sont au préalable posé la question avant de le mettre en production, de telle sorte qu'il existe une interaction entre le monde du logiciel libre et celui des sociétés d'édition. Par ailleurs, le marché de l'exploitation d'un logiciel propriétaire est plus long que pour un logiciel libre. Enfin, il est souvent plus facile d'apporter un correctif à une vulnérabilité dans un logiciel libre que dans un logiciel propriétaire.

VII. Peut-on avoir une technologie nationale ?

La France accuse un retard trop conséquent pour espérer rattraper le temps perdu et l'ampleur de certains chantiers (en hardware notamment) nécessite une conjugaison de moyens financiers et techniques qui dépasse les capacités d'un seul pays. Face à ses concurrents, l'Europe a tout intérêt à développer un domaine de souveraineté notamment sur les logiciels de sécurité.
Avoir confiance dans le produit et conscience de sa qualité et de ses limites, être capable de garantir l'absence de mainmise de la part d'un État ou d'un organisme, le faire évoluer et l'intégrer dans sa structure critique sans devoir craindre que la ressource technologique et la ressource des évolutions ne soient coupées sont au cœur même de la philosophie du logiciel libre. Ces libertés sont essentielles pour les enjeux individuels des utilisateurs, mais pas uniquement, et prennent encore plus d'importance à mesure que notre culture et nos activités quotidiennes se numérisent.

VIII. Les besoins opérationnels sont-ils suffisamment pris en compte ?

Sur la partie produit de métier, il y a juste une adaptation à réaliser. La gendarmerie nationale a ouvert la voie et conçu en partant d'open office une suite bureautique libre correspondant à ses besoins. Le projet Eole de l'éducation nationale développe des produits clef en main déployés dans les écoles avec des services parfaitement adaptés au métier.

IX. En termes de marché, est-on en mesure de vendre et d'exporter notre savoir-faire au-delà de l'hexagone ?

Les marchés sont directement influencés par la géopolitique. Il y a d'indéniables progrès à faire pour surmonter les obstacles, en matière de certification notamment, qui ne doivent pas devenir pour les entreprises un facteur asséchant toutes les ressources avant export. Il faut se montrer coordonné, raisonner de manière intelligente et savoir saisir les opportunités avec un sens mesuré de l'anticipation même si le processus de certification n'est pas toujours complètement verrouillé. Il y a dans ce domaine de réelles opportunités sous réserve de bien travailler ensemble sur des cibles communes.
Au niveau des marchés publics français, il

existe de petits éditeurs compétents avec des moyens réduits et peu de financement. Il serait extrêmement judicieux de les soutenir et de s'assurer que, par capillarité, ces développeurs peuvent bénéficier de quelques subsides.

X. L'open source est-il destructeur de valeurs par rapport aux modèles existants ?

En tout cas, cela l'est assurément pour les patrons des entreprises propriétaires. Il y a une dichotomie entre le monde du logiciel libre et celui de l'argent. Il est vertueux de gagner de l'argent avec du logiciel libre, mais dans un juste équilibre. Il faut opérer un rééquilibrage dans ce système car certains éditeurs génèrent des milliards d'euros en France.

Alors que les conditions de signature de l'accord-cadre dit « open bar » Microsoft - ministère de la Défense de 2013 et ses conséquences (sécurité des logiciels de la Défense et souveraineté nationale) continuent d'alimenter les commentaires du monde du logiciel libre, il est instamment souhaité de pouvoir bénéficier d'un schéma directeur du ministère de la Défense afin d'ouvrir à des communautés les besoins non sensibles des utilisateurs du ministère et de permettre de sortir ainsi de l'addiction collective et économique. Les participants de la table ronde soulignent que cet accord-cadre n'est aucunement créateur de valeurs pour la société française, mais assurément très intéressant pour tous les actionnaires de Microsoft et certains intégrateurs du ministère qui font du lobbying. Ils conviennent pourtant que les problèmes opérationnels - implémentations et contraintes terrain principalement - doivent être mieux appréhendés par la communauté libre.

Un auditeur rappelle que les armées disposent de systèmes d'information et d'armes interopérables. Il souligne que la transition vers le logiciel n'est pas chose aisée quand il s'agit souvent de systèmes qui protègent les hommes sur des périmètres critiques. Sans pour autant renier les impératifs de souveraineté technologique, il en appelle à la raison du terrain et par conséquent à une transition nécessaire saine mais maîtrisée pour éviter tout dommage collatéral.

B7 – Souveraineté et coopération : quelle frontière ?

Intervenants :

- Valéry MARCHIVE : Journaliste, Le Mag IT,
- IGA Guillaume POUPARD : Responsable du pôle Sécurité des Systèmes d'Information, Direction Générale de l'Armement, Ministère de la Défense,
- Wolfgang ROEHRIG : Program Manager cyberdefense, European Defense Agency,
- Serge TAPIA : Security Services Director, Alcatel-Lucent

Résumé des interventions :

Les États sont demandeurs d'une plus grande coopération, mais souhaitent également qu'aucune atteinte ne soit portée à leur souveraineté. Il importe donc de savoir où se situe la frontière entre ces deux notions clés, frontière devenue très floue lorsque l'on agit dans le cyberespace. Il n'est pas question de remettre en cause la souveraineté nationale. Celle-ci se justifie par des intérêts étatiques, militaires ou encore économiques. Cependant, la coopération n'implique pas forcément la fin de la souveraineté. Elle peut même la renforcer. Ainsi, par exemple, une coopération technologique dans le domaine de la cryptographie permet une coopération dans le renseignement et la nouvelle capacité qui en résulte augmente de fait la souveraineté nationale. La notion de confiance doit également être abordée, même si, pour certains, « la confiance est un échec pour un cryptographe ».

Aucun pays n'est aujourd'hui en mesure de maîtriser toute la chaîne informatique, depuis le premier composant électronique jusqu'au logiciel. De la même façon, notre sécurité dépend de celle de nos voisins. Des coopérations internationales et des échanges d'informations sont donc indispensables. Pour autant, il est nécessaire de bien définir la sphère englobée par la souveraineté nationale et de fixer clairement les règles à adopter en matière d'échanges d'informations.

I. La souveraineté du cyberespace

Actuellement, la tendance mondiale s'agissant des États consiste à reprendre autant que possible le contrôle du cyberespace. En effet, ce dernier s'est développé sans contraintes sous l'influence et l'impulsion d'acteurs privés, entreprises ou particuliers. Mais les nouvelles problématiques qui émergent rendent nécessaire la notion de souveraineté du cyberespace, qu'il s'agisse d'attaques informatiques subies par certains États ou encore de la guerre économique en cours sur Internet.

Il existe deux degrés de souveraineté pour un État dans le cyberespace. Le premier est d'ordre militaire. On peut à ce sujet citer l'exemple de l'US Cyber Command aux États-Unis. Cet organisme est chargé de la sécurité de l'information pour l'armée américaine. Le deuxième aspect est étatique. La souveraineté est alors perçue comme essentielle car elle protège les intérêts de la Nation. Il s'agit de conserver des informations confidentielles pour préserver une autonomie d'action, ou encore pour se préparer contre d'éventuelles menaces provenant du cyberespace.

La souveraineté peut aussi concerner la cryptographie, considérée comme un outil technologique destiné à protéger les communications. En France, le choix a été fait d'être autonome sur ce point, ce qui ne correspond pas à un point de vue partagé au niveau international. Pour y parvenir, il faut une maîtrise des équipements utilisés, ce qui implique une relation de confiance avec les partenaires industriels. Pour illustrer cette relation, en France, on peut avancer l'exemple du téléphone portable Theorem de chez Thales. La confiance est notamment contrôlée par la Direction de la Protection et de la Sécurité de la Défense.

L'affaire Snowden est également mise en avant pour mieux modéliser cette notion de souveraineté nationale. Après avoir eu accès à certaines informations classifiées des États-Unis, cet Américain a publié des données sensibles, portant ainsi directement atteinte à la souveraineté des États-Unis. Cette fuite a eu des répercussions diplomatiques graves pour le Président Obama et éclairé d'une lumière un peu trop crue un pan entier du système de la sécurité nationale américaine. Cette affaire pointe bien les risques encourus si cette notion de souveraineté du cyberespace n'est pas sérieusement appréhendée. En France, l'Agence Nationale de la Sécurité des Systèmes de l'Information (ANSSI) est à ce titre chargée, notamment, de veiller à

l'intégrité de cette souveraineté. Elle préconise même une notion de souveraineté européenne numérique. Pour faire la comparaison avec les États-Unis, la National Security Agency a deux missions : la collecte de renseignements d'origine technique et la sécurité des systèmes d'information. Or, il a été constaté que ces deux missions peuvent avoir des exigences contradictoires. En France en revanche, le choix a été différent puisque l'ANSSI ne s'occupe que de la sécurité des systèmes d'information. Il n'existe ainsi aucune ambiguïté quant à ses missions précises. Il est important de souligner le rôle des agences étatiques ainsi que leur place dans cette lutte pour la souveraineté cyberspatiale.

II. Une frontière entre la souveraineté et la coopération

Cette nécessité de souveraineté n'exclut pas, en revanche, une possible coopération entre les États. Il est nécessaire pour la développer de pouvoir s'appuyer sur une relation de confiance entre les États concernés. Chacun doit être sûr que l'autre ne divulguera pas ses secrets. L'échange d'une information ne s'effectue que lorsque la certitude est acquise que le partenaire avec lequel on traite a la capacité de sauvegarder cette information comme si elle était sienne. Pour y parvenir, chaque État doit être souverain sur le cyberespace national.

La coopération entre les nations permet entre autres d'appréhender des technicités non maîtrisées, de mieux détecter les attaques ou encore d'accroître sa capacité de renseignement. Par exemple, au niveau européen, la European Defense Agency permet une coopération importante. Elle autorise les pays n'ayant pas un niveau national de développement suffisant à combler leurs lacunes dans certains domaines numériques. Il y a également un partage de renseignements au niveau européen.

Les concepts de souveraineté et de coopération peuvent, en première analyse, sembler s'opposer en raison de l'autonomie stratégique étatique ou encore de la maîtrise des technologies mises au point par des industries nationales (la compatibilité est difficile entre systèmes provenant de différents pays sauf dans le cas particulier d'une technologie interopérable). Il existe néanmoins deux raisons qui justifient la coopération au niveau international. En premier lieu, les menaces telles que le cyberterrorisme touchent indistinctement tous les pays. Par ailleurs, certaines infrastructures sont partagées entre plusieurs pays. S'agissant en particulier de l'interopérabilité, on peut souligner que les États travaillent entre eux sur des primitives cryptographiques afin de pouvoir partager des informations chiffrées de premier niveau. L'exemple européen s'impose une nouvelle fois. Certains pays de l'Union Européenne n'ont pas la capacité d'avoir une autonomie en cryptographie. Il est dès lors pertinent de développer une cryptographie européenne afin de développer la confiance entre les États membres et donc une meilleure coopération.

Le modèle de gestion des espaces maritimes, relevant à 90 % d'un statut international, constitue un exemple très parlant pour comprendre vers quel schéma les États peuvent tendre dans le domaine de la coopération en matière numérique. Internet pourrait relever de ce modèle. Chaque pays a la responsabilité de la résilience d'Internet sur son propre sol. On pourrait aussi concevoir de doter les données transitant par internet d'un insigne de nationalité qui permettrait de renforcer les actions de coopération.
Cette coopération doit s'appuyer sur la confiance. De l'avis des spécialistes, celle-ci se développe dans le temps. Il faut donc augmenter la capacité des États à se comprendre et faire en sorte que la relation créée soit le plus possible gagnant/gagnant.

L'opposition apparente entre coopération et souveraineté s'efface si l'on considère qu'il s'agit finalement non pas de garder un château fort hermétiquement clos mais plutôt de sécuriser un aéroport par lequel circulent des informations et des biens.

B8 - Usurpation d'identité sur internet : des modes opératoires de plus en plus complexes

Intervenants :

- Hadi El KHOURY, O'service 2
- Alexandre ARCOUTEIL, Responsable d'Activité Cerissim, Fia-Net
- Mamadou BA, Chef de Marché, Services d'Identité Numérique, Morpho
- Fabrice MATTATIA, Expert en confiance numérique, Ministère des Finances – conseil général de l'Économie
- Anne SOUVIRA, Commissaire Divisionnaire, Direction de la police judiciaire, chef de la BEFTI, Préfecture de police de Paris
- Chef d'escadron Vincent TERRASSE, chef de l'unité d'expertise fraude documentaire, Gendarmerie nationale

Résumé des interventions :

Les usurpations d'identité (UI) sont en constante augmentation mais les chiffres diffèrent en fonction du sens donné à ce terme. L'usurpation d'identité administrative apparaît comme la plus grave. Nous devons faire face désormais à un contentieux de masse avec des enjeux commerciaux. Des solutions diverses, souvent onéreuses, existent. Mais elles nécessitent d'arbitrer entre risque et profit et aucune n'apparaît d'ailleurs comme la « solution miracle ».

I. Un constat initial peu clair

Le phénomène des usurpations d'identité, indépendamment du facteur « en ligne », est généralement associé à des statistiques considérables qui tendent à démontrer qu'il s'agit d'un contentieux de masse. Pour autant, alors que des chiffres de 13 millions de faits pour l'année 2013 sont avancés pour les seuls Etats-Unis, un service spécialisé comme la BETFI de la Préfecture de police de Paris, dédié aux infractions commises sur internet, recense une soixantaine de cas pour cette même période. Cet écart s'explique surtout par l'élasticité de la notion d'usurpation d'identité. Une lecture plus attentive permet de constater que les cas rapportés par la préfecture de police de Paris le sont au titre du nouvel article 226-4-1 de 2011, spécifique à l'usurpation en ligne. A contrario, l'immense majorité des faits rapportés dans les autres études incluent des faits qui relèvent de l'escroquerie (85% de fraude documentaire) ou de l'utilisation de plaques d'immatriculation en doublette.

Il est nécessaire de bien cerner la menace en ne se focalisant pas uniquement sur les questions techniques. Durant la période des 12-18 derniers mois on a assisté à une augmentation et à une professionnalisation de la menace. L'identité est généralement associée à l'identité administrative ou état civil, qui semble seule présenter les garanties nécessaires d'individualisation correcte de la personne. Pour autant, le processus identitaire est avant tout un processus d'authentification : on compare l'individu à une représentation que l'on détient en mémoire (humaine ou digitalisée) en vue de lui accorder quelque chose. L'usurpation peut ainsi se voir accorder les droits afférents. Elle se commet en ligne lorsque lesdites informations circulent sur internet, ce qui pose la question de « l'identité numérique », concept, là encore, mal défini.

Toutes les entreprises détiennent dans leurs bases de données des éléments de l'identité directe ou indirecte. Toutes les données ou informations personnelles permettant d'identifier quelqu'un directement ou indirectement sont constitutives de l'identité. Ce dernier constat prouve que le concept prend corps, indépendamment de l'usage qui est fait de ces données.

Dans le cas spécifique de la sécurité on peut se demander si on ne déresponsabilise pas l'utilisateur et s'interroger sur la nature des mesures pouvant contribuer à sécuriser un peu plus les transactions.

Si l'on fait le parallèle avec certains objets d'utilisation courante, on pourrait presque envisager de rendre obligatoire la mention suivante « l'utilisation peut nuire à votre sécurité ». De fait se pose la question des actions concrètes qu'il est possible et souhaitable de mener auprès du Citoyen.

II. Des solutions difficiles à proposer

Selon l'Observatoire de la délinquance, les plaintes pour usurpations d'identité sont

passées en quatre ans de 300 à 1400. Sachant que chaque utilisateur possède en moyenne 16 comptes auprès d'une ou plusieurs banques et de sites d'e-commerce, on assiste à une progression très sensible des plaintes. À un moment ou à un autre, l'identité doit reposer sur deux choses : la nécessité de relier l'identité avec le monde physique et l'obligation que l'identité ne puisse pas être divulguée, d'où le besoin de la stocker dans un monde sécurisé.

La vision commerciale des choses est également importante : ce qui compte finalement pour le marchand, c'est que la transaction ait été réalisée sans préjudice, sans se soucier de savoir qui paie et qui obtient le produit. Dans un achat en ligne on essaye, par exemple, de reconnaître un agrégat de quatre composants : nom, prénom, identité postale et identité bancaire, cette dernière étant la plus liée au compte physique, dont on évalue la cohérence. Avec ces quatre paramètres on peut espérer avoir des indicateurs de compromission qui sont les alertes ou les signaux faibles qui vont alerter l'individu, le marchand ou l'établissement bancaire sur une usurpation d'identité.

La question est alors de savoir si le fait de lier nécessairement l'identité client à une identité administrative n'est pas générateur de risque. En effet, est-il absolument indispensable de fournir des renseignements d'état civil et un numéro de titre d'identité pour valider un achat sur internet sachant que ces données prennent alors une valeur commerciale et seront également stockées? L'exemple le plus frappant est celui des validations d'achat en ligne par l'envoi d'un scan de document d'identité. Ce processus est dangereux pour le client qui dévoile des données privées et produit une copie d'un document officiel. Quant au commerçant, amené à demander un document sécurisé dont il ne peut finalement vérifier au mieux que 80 à 90% des marques censées le légitimer, il voit ses démarches alourdies sans plus-value réelle en matière de sécurité. On peut y voir une forme de compromission de l'identité administrative par son usage commercial et il peut paraître utile d'envisager plusieurs déclinaisons de l'état civil selon l'usage. Cette dernière idée transparaissait avant son passage pour avis au Conseil constitutionnel.

Alors même que la menace n'est pas identifiée clairement, des solutions, forcement parcellaires et contingentées, apparaissent. Certaines reposent sur la confirmation du lien ou le passage par un tiers de confiance dans une optique de durcissement du système. Il s'agit soit de valider l'enrôlement dans le système par un contact avec la personne physique, soit de recoller l'information par un autre biais qu'internet, par exemple à l'aide d'une question de confiance par SMS. Pour autant, ces solutions induisent un surcoût que le consommateur n'est pas forcément prêt à accepter. D'autres méthodes extrêmement efficaces, quoique davantage orientées vers la lutte antifraude, reposent sur l'observation des comportements (pro-

filages) et la détection des anomalies. Ces procédés peuvent cependant se révéler rapidement invasifs en termes de vie privée, ce que surveille la CNIL avec attention. Il peut également être utile de proposer des systèmes d'identité autonomes, fonctionnant sur la reconnaissance au sein d'une communauté et ne mettant en jeu que la stricte quantité d'informations nécessaires à l'individualisation au sein de cette communauté.
Enfin, la seule solution globale semble reposer sur l'éducation, la pédagogie dès le plus jeune âge et la nécessaire intégration de ces nouveaux réflexes dans les comportements quotidiens.
Il n'y aura en effet jamais assez de moyens humains et financiers disponibles pour lutter contre un phénomène qui semble avoir toujours une longueur d'avance.
Quatre solutions sont donc proposées : celle d'une identité vérifiée, celle reposant avant tout sur l'éducation de l'utilisateur, celle consistant à trouver un compromis entre les informations requises et le but pour lequel elles sont utilisées et enfin la solution faisant appel à l'analyse comportementale.

B9 - L'assurance, outil de financement du cyber risque

Intervenants :

- José DIZ : Journaliste indépendant, Silicon.fr,
- Stanislas de MAUPÉOU, Directeur Conseil en Sécurité et Evaluation, Thales,
- Mathieu ESTRADE : Chief Technology Officer EMEA, Qualys,
- Jimaan SANE : Souscripteur Technologie, Média, Sociétés de Services, Beazley,
- Luc VIGNANCOUR : Directeur Adjoint Risques Financiers, Marsh.

Résumé des interventions :

Les cyberattaques, que les entreprises en aient conscience ou non, constituent un risque réel. Ces attaques ont un coût financier très important qui peut atteindre plusieurs milliards de dollars. Si le coût en termes de pertes de recette pour l'entreprise peut facilement s'estimer, d'autres répercussions financières, liées par exemple à la notoriété ou au facteur humain, quoique bien réelles, sont difficiles à évaluer. Les compagnies d'assurances et les courtiers tentent de prendre ces attaques informatiques en compte. Mais encore faut-il pouvoir évaluer par avance la valeur de l'ensemble des actifs de l'entreprise. Un dialogue de valorisation et d'évaluation du risque doit s'établir entre les compagnies d'assurances, les courtiers, les entreprises et enfin les industriels fournisseurs de plate-forme de sécurité. Il s'agit d'anticiper le risque pour minimiser et limiter la durée du sinistre, puis permettre une rapide reconstruction du système informatique.

Assurer des biens et des actifs réels est une démarche naturelle de la part des industriels. Assurer des données informatiques, des systèmes informatiques ou la notoriété de l'entreprise relève en revanche d'une démarche actuellement marginale. Pourtant, le cyberrisque, du fait de la circulation sans cesse croissante des informations et de la dématérialisation de plus en plus massive, n'épargne désormais aucune entreprise. L'assurance, comme elle le fait dans d'autres secteurs, peut agir contre les attaques informatiques. De la même manière que pour un bien matériel, une évaluation du risque doit être effectuée avec des outils ad hoc. La question qui se pose aux entreprises n'est pas de savoir si elles vont faire l'objet d'une attaque, mais plutôt de se demander quand celle-ci interviendra. Peut-être même a-t-elle déjà eu lieu à leur insu. Il est donc vital pour elles d'être capable de limiter le temps du sinistre de manière à redémarrer le plus rapidement possible leurs activités.

I. La nécessité d'évaluer les coûts

Les sociétés d'assurance, dans un contexte de dématérialisation croissante des données et d'une augmentation exponentielle de la circulation d'information, ont dû s'adapter aux risques que représentent les cyberattaques. Il s'agit pour l'entreprise d'assurer l'ensemble de ses données sensibles et son système informatique, mais également de trouver auprès de sa société d'assurance, une assistance financière et une assistance de gestion de crise. Chaque semaine, 343 entreprises dans plus de 200 pays seraient sujettes à une cyberattaque, engendrant plus de 7,5 milliards de dollars de sinistre. Ces agressions ne sont pas toujours immédiatement repérées : une société américaine mondialement connue comme TARGET a été victime de pirates alors que son système informatique était réputé le plus sûr au monde. Puisque le risque zéro n'existe pas, il s'agit d'externaliser dans la mesure du possible le facteur risque.

Comme pour tout dépôt de plainte, il est nécessaire d'évaluer financièrement le préjudice. Valoriser les conséquences d'une attaque informatique n'est pas une tâche aisée. Il convient de prendre en compte aussi bien les coûts qu'impliquent une cessation d'activité suite à une attaque du système informatique qu'une fuite de données qui porterait atteinte à la vie privée de salariés ou qui ternirait l'image et la notoriété d'une entreprise. Les courtiers d'assurance tentent de comprendre et d'analyser les risques encourus par leurs clients. Par la prise en compte de plusieurs facteurs, ils doivent anticiper lors d'un sinistre l'impact que la cyberattaque pourra avoir sur l'entreprise mais également ses conséquences éventuelles dans la durée. Ainsi, l'assureur doit notamment prendre en compte lors de sa valorisation les actifs qui peuvent être amenés à disparaître ou à être détournés, le système d'information qui permet à l'entreprise de fonctionner, les

coûts imposés par la réglementation (exemple : les coûts de notification), le droit de réclamation de l'entreprise en cas de préjudice.

II. Dispositif de protection et d'intervention face au sinistre

Dans un contexte d'économie mondialisée, toutes les entreprises sont potentiellement vulnérables à une cyberattaque. Les coûts et pertes induits par ces attaques étant potentiellement très élevés, il est nécessaire que les entreprises tentent de se prémunir contre ces risques. Des outils existent pour prévenir et apporter une protection à l'entreprise. Des plates-formes fournies par des opérateurs privés permettent aux entreprises d'avoir accès à une cartographie de leur système d'information. Ainsi par exemple certains dispositifs dits de « continuous monitoring » permettent à l'entreprise d'avoir un état permanent en termes de sécurité de leurs systèmes. Ces outils de qualité mettent en lumière les vulnérabilités de ces sociétés qui peuvent alors tenter de les pallier. Enfin, ces plates-formes autorisent une évaluation du risque pour les courtiers d'assurances et les assureurs.

Malgré les dispositifs de protection, le risque reste cependant réel et fortement probable. Dans certains cas, il est même difficile de comprendre pourquoi et comment l'entreprise a pu être attaquée. Des sociétés comme Thales proposent des prestations pour intervenir après la cyberattaque. Il s'agit alors, dans une optique de réduction des coûts financiers et des pertes de données, de limiter dans un premier temps la durée du sinistre par une analyse des causes de l'attaque, puis dans un deuxième temps de reconstruire rapidement le système d'information de la société attaquée.

III. Une analyse en amont et en aval du risque

Un véritable partenariat est nécessaire entre l'entreprise, les assureurs, les courtiers d'assurance et les sociétés prestataires en sécurité informatique. Il s'agit pour l'entreprise, en amont du sinistre, de mettre en œuvre les mesures de protection nécessaire que lui apportent les nouvelles technologies. Des labels de sécurité existent et permettent aux assureurs de vérifier si un suivi effectif de la sécurité est réalisé par l'entreprise. Certains « firewalls » suffisent et constituent pour les sociétés d'assurance la preuve qu'une protection est effectivement mise en place par l'assuré. Les courtiers, une fois leur évaluation effectuée, établissent le contrat d'assurance qui convient le mieux. Devant la difficulté à prévoir tous les risques dans un domaine connaissant sans cesse des évolutions rapides, ces contrats restent parfois volontairement flous de manière à pouvoir répondre à davantage de situations. En aval du risque, l'assureur doit apporter à l'assuré non plus seulement une indemnité mais un service. Il s'agit de lui permettre d'améliorer la détection des cyberattaques, puis de les comprendre et

de gérer au mieux la crise engendrée par ce sinistre.
Ainsi, de nouvelles technologies récemment apparues permettent aux entreprises de tenter de se prémunir contre les cyberattaques. Le monde de l'assurance a évolué également et s'adapte aux risques encourus. Si la difficulté d'estimer le cyber-risque reste réelle, seul un partenariat bien ciblé entre les différents acteurs peut permettre d'évaluer au mieux les conséquences de la cyber-attaque. Lors du sinistre, l'analyse de la situation par les différents acteurs est primordiale pour gagner du temps sur les dommages, car plus la réaction sera longue, plus les coûts seront élevés pour l'entreprise.

B10 - RSSI et CIL : quelles synergies ?

Intervenants :

- Bruno Rasle, Délégué Général, AFCDP
- Éric BarbRy, Avocat, Cabinet Bensoussan
- Hervé Schauer, Directeur, HSC
- Marie-Noëlle Séhabiague, Chargée de mission et CIL, Caisse nationale des Allocations familiales (CNAF)

Résumé des interventions :

Si le RSSI est l'expert technique en matière de sécurité de l'information, le CIL est à la fois conseiller juridique et observateur en matière de données personnelles. Chargés de rôles distincts mais largement complémentaires, ils doivent nécessairement coopérer pour garantir la sécurité des données personnelles et aider à protéger l'entreprise de l'impact majeur qu'aurait une fuite ou un vol de données.

I. Des métiers différents

RSSI et CIL sont deux métiers de la sphère de l'informatique que tout pourrait sembler opposer.

Le Correspondant Informatique et Libertés exerce dans un périmètre bien défini, régi par le décret n°2005-1309, dont on trouve l'équivalent dans tous les pays européens ayant érigé une législation protectrice des données personnelles, comme l'Allemagne depuis 1977. Le nombre et les noms des CIL en exercice sont connus. Plus de 10000 organismes dont près de 60 % de ceux composant le CAC 40 ont désigné un CIL. Ceux-ci, à 40 % des femmes, ont des profils assez diversifiés mais qui restent principalement juridiques. Ce dernier domaine correspond effectivement à 90 % de leur activité, le reste étant consacré à l'opérationnel. Confirmant cette prédominance du droit, le code ROME associé à la profession est celui de la défense et du conseil juridique.

La plupart du temps rattachés aux Directions générales ou entités assimilées, les CIL exercent en effet leur mission « directement auprès du responsable de traitement ». Pour cette fonction, ils sont indépendants et protégés de leur employeur du fait de leur exercice (articles 46 et 53 du décret), sauf à commettre des manquements graves. Agissant transversalement comme observateurs objectifs, ils peuvent en outre engager la responsabilité du responsable de traitement par saisine de la CNIL. Cette proximité de la direction permet au CIL de pouvoir soulever de manière assez audible les problèmes liés aux données personnelles, et au besoin d'obtenir les budgets nécessaires. Cependant, certains CIL peuvent ignorer jusqu'au fait qu'ils sont titulaires de cette fonction parce qu'ils ont été désignés par leurs employeurs sans en avoir été avisés. La désignation d'un CIL, même lorsqu'elle n'est pas suivie de réels effets, est néanmoins un signe de confiance, de respect de la loi et d'attachement à la protection des données personnelles.

À l'opposé du CIL, le responsable de la sécurité des systèmes d'information exerce un métier flou et hétérogène, dont aucun code ROME ne parvient à exprimer la complexité. Provenant majoritairement de professions proches, souvent informaticiens et pratiquement tous de sexe masculin, les RSSI s'adaptent aux habitudes de l'entreprise et, étant généralement employés par les Directions des systèmes d'information (DSI), font valider la politique de sécurité par la direction et sensibilisent la direction comme le personnel aux questions de sécurité de l'information. Plus facilement désigné que le CIL, en raison d'une part de l'impératif de sécurité de l'information nécessaire à la survie de l'organisme mais également parce qu'il ne bénéficie d'aucune indépendance dans son action et personnifie l'investissement dans la sécurité, le RSSI a généralement plus de poids qu'un CIL pour améliorer la sécurité et la protection des données de l'entreprise.

Un éloignement limité, un rapprochement nécessaire

Malgré leurs origines et leur positionnement différents, CIL et RSSI ont tout à gagner à un rapprochement et à une communication réciproque. Une synergie fondamentale entre eux est nécessaire pour dresser l'inventaire et la cartographie des informations personnelles détenues. De plus, lorsque l'arbitrage entre ces deux acteurs est correctement défini dans la gouvernance, leur coopération sécurise la gestion des données personnelles de l'organisme. Le CIL et le RSSI associent leurs compétences respectivement juridiques et techniques, chacun aidant l'autre à comprendre ses préoccupations et ses possibilités.

Ainsi par exemple, si chiffrer les données personnelles est une bonne solution pour les protéger d'un vol (ce qui relève d'une problématique au cœur des responsabilités du CIL), c'est avant tout une mesure technique qui devra être mise en place par la DSI, domaine par excellence de l'intervention du RSSI. Les deux responsables ne peuvent par conséquent pas être éloignés. Plus largement, la mise en place de nouveaux traitements de données à caractère personnel, que l'on peut considérer par une approche de risk manager, engendre un risque économique et légal pour l'entreprise par la sensibilité des données, leur éventuel transit hors de l'Union européenne ou encore leur stockage hors métropole. En cas d'incident, la perte de confiance des clients et la fuite d'informations vers un concurrent peuvent ainsi être fatales à l'organisme.

Ainsi, la gestion des données personnelles, parallèlement au souci de conformité légale du traitement, nécessite un point de vue technique spécialisé. Le RSSI apporte l'expertise technique tandis que le CIL rappelle les contraintes légales, notamment le respect de la finalité du traitement de données. Le CIL est finalement émetteur d'exigences sur le RSSI et peut lui faire décrocher les budgets : les deux doivent donc marcher dans le même sens et s'appuyer réciproquement.

Pour confirmer cette approche par le risque, la législation tend actuellement à évoluer vers une obligation de déclaration des incidents de sécurité concernant les données personnelles comme les failles du système d'information. Pour cette raison (et toutes celles évoquées ci-avant), la synergie entre le RSSI et le CIL apparaît donc impérative et capitale.


Advanced Cyber Security.
Be fully prepared for the future.
Soyez prêts pour le futur.
TRUST THE FUTURE / CONFIANT EN L'AVENIR
NETASQ
ARKOON
CASSIDIAN
CYBERSECURITY
WWW.CASSIDIANCYBERSECURITY.COM

B 11 – Quelle sécurité pour les usages et technologies de demain ?

Intervenants :

- Yann SERRA journaliste indépendant,
- Jean Marc RIETSCH président FedISA,
- Christophe AUBERGER SE Manager France & North Africa, Fortinet
- Isabelle DUMONT Directrice Marketing de la division Industrie, Palo Alto
- Bruno FORGIARINI Régional Sale Manager, FireEye
- Chebib GHARBI Directeur Général, Centre EuraRFID-CITC

Résumé des interventions :

La société évolue au gré des innovations technologiques. Objets communicants et partage d'information sur des serveurs distants feront partie de la vie quotidienne de chaque homme dans un futur proche. La cybercriminalité s'est organisée elle aussi pour tirer le meilleur parti des avancées technologiques importantes. Comment anticiper aujourd'hui la sécurité au sein d'une société en constante évolution technologique ?

I - Paiement sans contact et objet communicant

Les cartes de crédit sont depuis longtemps devenues un moyen de paiement incontournable. Pour permettre un délai de transaction toujours plus court, les ingénieurs ont développé la technologie des paiements sans contact. Il est cependant assez vite apparu que des pirates étaient en mesure de collecter les informations de ces cartes en activant à distance les puces RFID qui les équipent. Ils utilisent pour y parvenir des dispositifs techniques simples et des outils accessibles au grand public tels que des smartphones. La fiabilité et la sécurité de ces cartes semblent dès lors remises en question.
Certaines mesures de protection ont pu être proposées depuis que ces menaces ont été identifiées. Les ingénieurs parviennent à créer plus de sécurité, par exemple par le biais de cages de Faraday incorporées dans les portefeuilles ou par un chiffrement plus complexe des données.
Néanmoins, la tendance des industriels à rendre les moyens de paiement plus simples d'utilisation augmente les risques. Plus il y aura d'objets communicants au sein du réseau et plus les risques d'interception augmenteront. Il est par conséquent primordial que les industriels identifient les risques et proposent d'emblée des solutions permettant de les maîtriser. Avant même de se demander comment le consommateur s'appropriera les objets mis sur le marché (lunettes connectées, réfrigérateurs « intelligents », etc.), les services de recherche et développement devraient s'attacher à concevoir des produits en lesquels le consommateur pourra avoir confiance.

II- Stockage des données : devons nous être inquiets ?

Le Big Data (et son traitement) est considéré comme l'un des grands défis informatiques de la décennie 2010-2020. La masse des données disponibles devient tellement énorme qu'il devient difficile de travailler avec des outils classiques de gestion de base de données ou de gestion de l'information. Face à ces nouveaux ordres de grandeur, la capture, le stockage, la recherche, le partage, l'analyse et la visualisation des données doivent être redéfinis. L'enjeu réside dans le traitement et l'exploitation de l'information.
Il est légitime de s'interroger sur la confiance que l'on peut accorder au Big Data. Celle-ci s'appuie sur deux conditions. L'intégrité du document doit être préservée et l'identité de sa source garantie. Le support et le format des données ont aussi leur importance dans la sécurité des informations numériques. Les supports, sur le plan technologique, sont en pleine évolution dans le domaine des mémoires magnétiques, mais aussi avec l'optique et ses procédés holographiques. Des pistes commencent à être explorées en ce qui

concerne la gravure dans le quartz, facile à interpréter avec un microscope électronique et durable dans le temps. Cette nouvelle technologie présente une sécurité importante car elle supprime le doute quant à une éventuelle modification des données. De plus, des recherches portant sur l'ADN de synthèse se développent aux Etats-Unis et en Angleterre, avec des perspectives de capacité de stockage très importantes pour des volumes physiques très réduits.

III- Menaces d'aujourd'hui, que doit-on faire pour améliorer les défenses ?

Depuis 2006, la cybercriminalité génère un bénéfice plus élevé pour ses auteurs que le trafic de drogue, avec des risques bien moindres. Il est nécessaire de proposer aux acteurs économiques un niveau de sécurité important de leurs activités numériques pour faire face à cette menace avérée.
Le premier facteur de vulnérabilité de tous les systèmes est l'utilisateur qui doit prendre conscience de la réelle menace que constitue la cybercriminalité. Or, les technologies actuelles ne sont pas utilisées correctement. La plupart des gens ne changent pas leurs mots de passe. Sur beaucoup de configurations informatiques personnelles, les pare-feux ne sont pas installés et les mises à jour ne sont pas faites. Une véritable prise de conscience doit donc intervenir pour que la sécurité au niveau global évolue. Une réponse à l'échelle européenne doit être apportée dans le but de faire changer les comportements.
La prise en compte de la cybermenace dans ce contexte de flux grandissant d'informations passe nécessairement par une automatisation de la surveillance, seul moyen de détecter, au milieu de la masse, les comportements anormaux ou les flux suspects. Par ailleurs, la sécurité constitue souvent une contrainte pour les utilisateurs. Pour ne pas impacter la compétitivité des entreprises, il serait souhaitable qu'elle soit gérée de manière délocalisée et transparente pour l'utilisateur.

CONCLUSION

Le monde futur tel qu'il se dessine sera un monde connecté. Un flux d'information considérable sera échangé, notamment entre les objets, de manière automatisée et indépendante. Ce flux constitue une cible pour la cybercriminalité dont les intrusions et attaques auront encore plus d'impact qu'aujourd'hui. Il est temps de réagir à l'échelle européenne afin de sensibiliser la population à ce risque grandissant.
Les solutions, aussi élaborées et aussi pertinentes soient-elles, ne sont efficaces que si elles sont utilisées correctement. Technologie et travail collaboratif sont les points clefs pour parvenir à réduire l'écart entre les cyberpirates et les sociétés de sécurité logicielle.


MINISTÈRE DE L'INTÉRIEUR
PERMIS INTERNET
GENDARMERIE
PERMIS INTERNET

B12 - Détection et anticipation des menaces

Intervenants :

- Florence PUYBAREAU : journaliste indépendante
- Vincent LECLERC : Chef de l'équipe consulting d'avant vente Kaspersky
- Emmanuel BESSON : Directeur technique chez 6Cure, spécialisé dans le déni de service
- Yoann LE BORGNE : Responsable technique Sourcefire

Résumé des interventions :

Face à la sophistication croissante des menaces, les acteurs de la cybersécurité doivent dépasser les modes classiques de protection : de la détection en amont des menaces aux nouveaux modes de protection, quelles sont les solutions organisationnelles ou techniques que les acteurs de la sécurité proposent ?

I. État des lieux

L'époque où l'antivirus suffisait pour se prémunir des attaques informatiques est bien révolue. De nos jours, il faut absolument ajouter aux dispositifs techniques une approche des ressources humaines de l'entreprise si l'on veut progresser dans la prévention. Ce travail passe par la sensibilisation, voire la formation de l'utilisateur (formations, bulletins, sites Web,…).

Les entreprises, dans leur grande majorité, commencent à peine à prendre conscience de l'importance de la sécurité de leur système d'information. Ce constat est d'autant plus vrai s'agissant des risques internes à l'entreprise. Dans ce domaine, il n'y a que très peu de contrôle des données, de leur circulation et de leur stockage. L'utilisation d'un pare-feu ou d'un antivirus permet sans doute de se protéger de l'environnement extérieur mais ne garantit aucunement que l'entreprise est sécurisée sur le plan des systèmes d'information et de communication.

En matière de protection il ne faut pas hésiter à être proactif et à s'appuyer sur des partenaires spécialisés, tant pour des fonctions de veille, de formation ou d'audit que pour la mise en place de dispositifs de sécurité.

II. Comment gérer le risque ?

Tout protéger étant un objectif utopique, il faut définir, grâce à une analyse de risque, ce qui est essentiel et constitue « les bijoux de famille » de la société. Tout ce qui, en étant perdu ou volé, peut faire perdre de sa valeur à l'entreprise doit impérativement être mis en sécurité. En fonction de l'entreprise, l'analyse permettra de dégager les menaces qui la concernent principalement. Le cyber-hacktivisme (qui porte atteinte à l'image de l'entreprise), le cybercrime (qui porte atteinte généralement au profit de l'entreprise), le cyber-espionnage (qui vise à récupérer principalement des secrets industriels) constituent les principales menaces pour le monde économique.
Il faudrait donc penser différemment le choix de sa protection en se demandant par exemple, en cas de piratage, ce qui intéressait vraiment l'auteur de l'acte pour en déduire la manière dont on pourrait éviter une nouvelle attaque.

La définition et la mise en place des outils constituent les étapes qui forment la cartographie des risques. Pour ce faire, trois grands principes guident l'action du décideur. En premier lieu, il convient de veiller à définir correctement la politique de sécurité externe mais aussi interne en fonction des risques identifiés. Il est ensuite nécessaire de mixer les technologies pour utiliser le meilleur de chacune et compliquer la tâche des personnes malveillantes. Enfin, il est souhaitable que les différents outils communiquent entre eux pour éviter les effets silo, permettre une administration totale et homogène et autoriser, à un instant donné, la mobilisation de toutes

les ressources dans un objectif de sécurité globale.
Pour bien gérer le risque, il est nécessaire de garder à l'esprit qu'un outil reste un outil. Il est en effet primordial d'avoir derrière ces outils des spécialistes formés, qui apportent leur expertise et soient capables d'interpréter les signaux faibles comme de réagir à un acte hostile.
La problématique de sécurité se situe au cœur de l'entreprise, de la base jusqu'à son sommet. Il doit donc se créer une vraie communication interne (et même externe) à ce sujet afin que chacun se sente pleinement concerné et sache comment procéder en cas de besoin.

Il serait trompeur de croire que la diversification, l'ouverture vers l'extérieur, la mondialisation et la venue des objets connectés (réfrigérateurs, machines à café, smartphones,…) constituent en soi de nouveaux risques. Ces évolutions ne font finalement que créer de nouveaux points d'entrée au sein de l'entreprise, chacune de ces brèches nouvelles offrant la possibilité d'exploiter les faiblesses déjà existantes. Ceci étant dit, les fournisseurs d'objets connectés négligent trop souvent la question de la sécurité. Dans l'intérêt de tous, il serait préférable de s'en soucier dès la conception même de l'objet.

III. Et dans un futur proche ?

C'est l'anticipation et la détection en amont qui focalisent les efforts de recherche des professionnels de la sécurité des systèmes d'information. Ainsi, la société Kaspersky prête une attention toute particulière à l'environnement industriel. Elle étudie notamment les méthodes d'attaque silencieuses et ciblées afin de les détecter et de proposer à ses clients les moyens de s'en prémunir. La société 6Cure, quant à elle, s'est spécialisée dans les attaques de dénis de service, ce qui est un secteur très particulier. Ses recherches visent actuellement non plus à trouver les moyens de traiter ces attaques (elle dispose déjà d'une expertise dans ce domaine) mais à les anticiper. En détectant les prémices de ces attaques, elle pourra prendre les mesures nécessaires avant même que la crise ne se déclenche réellement. Les attaques étant de plus en plus ciblées et professionnelles, la société Sourcefire, enfin, travaille selon trois axes principaux. Le premier consiste à détecter au plus tôt afin de faire de la prévention efficace et ciblée. Le second axe concerne les attaques silencieuses et ciblées et particulièrement la détection des signaux faibles. Le dernier axe de recherche porte sur des systèmes de « boîte noire » permettant, si une attaque ne peut pas être déjouée, de comprendre et analyser a posteriori la faille utilisée, les moyens techniques mis en œuvre par l'agresseur et l'ampleur exacte des conséquences de l'attaque (les données auxquelles on a accédé, celles qui ont disparu et, éventuellement, la nature des modifications qui ont été apportées aux systèmes de l'entreprise).


GENDARMERIE
FIC

B13 - Portrait du citoyen numérique en 2020

Intervenants :

- Gérôme BILLOIS – Senior manager, Solucom
- Lazaro PEJSACHOWICZ – Président, CLUSIF,
- Christian-François VIALA – Dirigeant YesProfile,
- Sophie VULLIET-TAVERNIER – Directeur des études, de l'innovation et de la prospective, CNIL,
- Akim OURAL - Responsable systèmes d'information, Lille métropole communauté

Résumé des interventions :

La protection de la vie privée va se transformer d'ici 2020 à la faveur de l'avènement d'une société de plus en plus numérisée. Elle doit s'effectuer en toute sécurité et l'organisation des nouveaux usages doit répondre aux enjeux de la modification des comportements des citoyens numériques. La puissance publique a un rôle à jouer pour trouver un équilibre entre la protection des libertés individuelles, la sécurité et le développement de cet espace numérique.

I. Les usages, les comportements, les évolutions à l'horizon 2020

Des tendances se dessinent à l'horizon 2020 avec des évolutions liées au Big Data et à l'explosion des données. Cet énorme gisement d'informations numériques va faire l'objet d'exploitations multiples dans un manque de transparence manifeste. Les millions de données existantes peuvent en effet donner lieu à toutes sortes d'utilisations. Or, les captations automatiques de données vont se développer avec l'Internet des objets. La démocratisation des capteurs dans notre activité quotidienne a déjà commencé. La géolocalisation et le profilage connaîtront également une impulsion notamment à l'égard de la traçabilité dans le temps et l'espace des données ou métadonnées captées à notre insu. Enfin, la biométrie, au-delà de l'identification digitale, est une tendance lourde qui va s'amplifier avec le développement des dispositifs de reconnaissance faciale. L'Internet des objets générera entre 24 et 50 milliards d'objets connectés en 2020 avec potentiellement jusqu'à une centaine d'objets connectés autour d'un individu: lunettes, couches-culottes , réfrigérateurs... En 2020, à titre d'exemple, le réfrigérateur effectuera la commande des aliments et déclenchera la livraison.
Un paradoxe, le « privacy paradox », apparaît cependant entre le désir de dévoilement de soi et la préoccupation du respect de la vie privée et des libertés individuelles. Malgré l'exhibitionnisme numérique, la tendance actuelle réside dans la vérification des paramètres de confidentialité. L'individu, même s'il développe une propension à se mettre en avant sur les réseaux sociaux, souhaite effectivement conserver une part d'intimité qu'il va contrôler par la maîtrise de ses paramètres de confidentialité. Certains estiment qu'il faudrait davantage faire confiance à l'individu dans la gestion de ses données et de sa vie privée. En outre, le développement de l'espace numérique isole les citoyens. En effet, une des caractéristiques majeures résidera dans le fait qu'« *Internet en connaîtra beaucoup plus sur l'individu que l'individu lui-même* ». Dans le même temps, la confiance des citoyens dans tous les services nécessaires à leurs diverses activités risque d'être sérieusement mise à mal par les multiples menaces qui les touchent. Le défi, pour le gouvernement, consiste, d'ici 2020, à maintenir ou restaurer la confiance du public.
Une certaine passivité des citoyens a pu être observée face au plus grand scandale numérique de ces dernières années, à savoir l'affaire du programme PRISM. À terme, ne pas être connecté finira par devenir anormal. De même, la non-géolocalisation deviendra suspecte.

II. Les enjeux

Aux États-Unis, il n'existe pas de protection des données. En France, la protection de la vie privée n'est théoriquement pas un droit qui se monnaye, c'est un droit fondamental inscrit dans la Charte européenne des droits

de l'Homme. Or l'État n'a pas les moyens de préparer la population aux enjeux de respect de la vie privée et des libertés individuelles. C'est pourquoi il doit, en collaboration avec les collectivités territoriales, jouer un rôle de régulation pour créer, filtrer, anonymiser. Pour certains, cela devrait se traduire par le renforcement des pouvoirs de la CNIL. Diverses problématiques sont soulevées : opacité relative à l'usage des données, irrégularité de l'information numérique et déséquilibre des pouvoirs entre l'individu et les acteurs clés de l'Internet. L'essor des nouveaux usages nécessitera une préparation particulière pour répondre aux enjeux de modification des comportements des citoyens numériques et d'organisation entre les différentes collectivités. Le rôle de ces collectivités va résider dans l'élaboration des conditions de mise en œuvre de processus ou systèmes permettant l'adaptation numérique. Cette transformation comportementale des citoyens ne peut s'envisager que par l'encadrement numérique du territoire pour faciliter le développement d'un certain nombre de services liés à la mobilité, au maintien à domicile, à la culture, au tourisme, au développement économique... Cela doit s'effectuer en intégrant trois principes, à savoir l'interopérabilité des systèmes, la subsidiarité et la sécurité pour des usages cohérents en dehors des frontières des collectivités. Certaines collectivités le font déjà à travers un intergiciel. Le numérique décloisonne par nature la responsabilité et les compétences de ces collectivités.

Par ailleurs, le développement d'un « comportementalisme numérique » se dessine. En effet, on assiste à l'émergence d'une « gouvernementalité algorithmique » qui se manifeste par la prise automatique, par algorithme, de décisions à partir de l'exploitation de données. Cela pose un questionnement au regard des libertés publiques. Il y a un réel risque d'être formaté dans son opinion, dans sa liberté d'expression, dans sa liberté de déplacement. Cela se traduira par l'adaptation des comportements par rapport à l'exploitation des données et des traces que l'individu aura laissées.

La responsabilisation de l'individu devrait s'effectuer par l'éducation au numérique : la diffusion auprès de tous publics d'une véritable culture du numérique permettrait à chacun de disposer de moyens de compréhension de cet univers. Cela passerait également par l'éducation aux risques, notamment par la maîtrise de son propre risque. Pour certains, plus les personnes connectées seront éduquées, plus elles seront attentives aux pièges d'Internet. Des solutions doivent être trouvées pour résoudre les problèmes de comportements déstructurants sur les réseaux sociaux. Le permis Internet semble être un commencement de solution. La dotation de tablettes dans les écoles, évoquée il y a quelque temps, doit s'accompagner d'une formation pour être efficace. Des séances de codage pourraient être envisagées, l'éducation des moins jeunes pourrait se faire par les plus jeunes. Dans une optique positive, la CNIL essaie de trouver des solu-

tions et de faire prévaloir une pédagogie des usages. Il s'agit d'une régulation par la technique «privacy by design» : intégrer le plus en amont possible les applications informatiques et les solutions de sécurité. L'orientation donnée va dans ce sens, comme le montre la sanction prise contre Google pour son manque de confidentialité et de transparence.

Par ailleurs, on se dirige vers une responsabilisation plus grande des entreprises, avec un rôle plus actif par la promotion de nouveaux droits (portabilité des données, droit à l'effacement des données et droit à l'oubli). Une voie de réflexion concerne la taxation des entreprises numériques en fonction de leur comportement plus ou moins vertueux en matière de protection des données personnelles.

En conclusion, l'éducation numérique a une très grande importance mais elle ne doit pas constituer l'unique politique de protection des données personnelles. En effet la compréhension technique du fonctionnement d'une machine n'implique pas que l'on soit en sécurité. Par ailleurs, se pose la question du droit à rester seul, du droit à ne pas être connecté dans une société qui incite fortement à s'intégrer dans un univers numérique globalisé.

B14 - Représentation et cartographie du cyberespace.

Intervenants :

- Valery MARCHIVE, journaliste, le Mag IT,
- Lieutenant-colonel Stéphane DOSSE, Ministère de la Défense,
- Frédérick DOUZET, titulaire de la chaire Castex de cyberstratégie, directrice adjointe de l'institut français de géopolitique de l'université Paris 8,
- Bertrand de la CHAPELLE, ICANN.

Résumé des interventions :

Pour comprendre une situation complexe, un bon schéma vaut souvent mieux que des explications longues. La carte constitue un outil particulièrement utile et utilisé depuis très longtemps par les militaires et les décideurs politiques. Cartographier le cyberespace constitue à cet égard un double défi. D'une part il s'agit d'un sujet hautement stratégique avec des implications tant militaires qu'économiques et politiques, d'autre part cette démarche s'avère extrêmement complexe du fait de la nature même du cyberespace. Tout l'art du cartographe et des ingénieurs consiste par conséquent à concilier sur un espace en deux dimensions des concepts et un système conçu en couches multiples.

I. Cartographier le virtuel ?

La cartographie utilisée depuis toujours par les militaires réunit sur le papier un terrain, un adversaire et les unités amies. Le Livre blanc de la défense et de la sécurité nationale rajoute cependant aux territoires traditionnels (terre, mer, air, espace) un nouvel espace de confrontation à part entière : le cyberespace. Établir une cartographie de cet espace soulève de nombreuses difficultés. Le cyberespace est composé de couches qui se superposent et sont reliées les unes aux autres (de la couche physique à la couche applicative). Par ailleurs, les données représentées peuvent avoir des durées de validité très courtes, rendant les cartes obsolètes, parfois en quelques heures. Aux cartes correspondent bien souvent des notions de souveraineté délimitées par les frontières tracées sur le papier. Dans le monde cyber, il serait plus judicieux d'adopter une logique floue. En effet, la souveraineté, telle qu'entendue au sens westphalien, s'applique sur un domaine, dans un territoire et sans influence sur les autres territoires où s'appliquent d'autres souverainetés. Force est de constater que, dans le cyberespace, il existe des espaces de souveraineté commune impliquant États, acteurs commerciaux, organisations internationales... Dès lors, l'enjeu majeur consiste à définir des règles de coopération entre ces acteurs.
La cartographie est un instrument de connaissance et les choix de représentation qui sont opérés ne sont jamais neutres. Une carte est le reflet d'une partie seulement de la réalité, elle ne peut pas être exhaustive. Lors de sa conception, il est indispensable de comprendre ce que l'on veut exprimer. L'exercice, déjà délicat pour des cartes de géographie, devient réellement complexe pour le cyberespace. Il s'agit d'un point essentiel car une carte mal pensée peut, tout en s'appuyant sur des données techniquement exactes, fausser la perception de la réalité.

II. Une démarche déjà initiée et en mutation

Des cartographes, associés à des informaticiens, produisent déjà des documents du plus grand intérêt. Une carte permet ainsi de visualiser les enjeux relatifs aux flux d'information. Illustrant la balance des flux entrants et sortants de certains pays (Etats-Unis, Chine, Brésil, Corée du Sud et France), elle met en relief une masse entrante considérable aux Etats-Unis, sans lien proportionnel avec la population américaine. La carte démontre ainsi que le nombre de serveurs installés dans le pays ainsi que les conditions tarifaires associées aiguillent de fait une bonne partie des flux d'information vers ce territoire, ce qui donne évidemment des possibilités accrues d'interception de données aux autorités américaines.
Une autre analyse cartographique permet de distinguer les politiques de souveraineté nationale mises en place par certains États. Ainsi, les offres spécifiques et globales (réseau, moteur de recherche, langue, alphabet, outils d'e-commerce) de la Russie lui permettent

de se créer sur internet une sorte d'espace alternatif, identitaire, au sein duquel évoluent les internautes concernés sans lien avec le reste du cyberespace. Certains pays ex-satellites soviétiques prennent d'ailleurs bien soin d'utiliser la langue anglaise pour se détacher de cette nouvelle forme de tutelle. Une étude historique de l'URSS devenue ensuite Russie permet par ailleurs de noter comment l'État est intervenu, dans son territoire, sur la sphère des télécommunications (y compris cyber), parfois de manière physique en coupant les réseaux comme en 1991. Dans ce pays, il est par ailleurs notable que la couche physique d'internet (les serveurs, les câbles) suit presque exactement la dorsale transsibérienne.
Les données étant très mouvantes, notamment dans les couches logicielles et cognitives, il est vraisemblable que les cartographes essaient de plus en plus d'utiliser des représentations dynamiques, en 3D, remises à jour en permanence, lesquelles permettront de bénéficier d'une vision juste à un moment donné mais également de percevoir les variations dans le temps (évolution des flux quant aux cheminements suivis par exemple). Quoi qu'il en soit, la cartographie ne prétend aucunement donner seule une vision juste des choses. D'autres approches sont nécessaires pour donner aux décideurs une panoplie d'outils d'évaluation des situations.

La question de la cartographie du monde cyber pose très nettement celle de la souveraineté dans ce nouvel univers. L'affaire de la NSA et les révélations de Snowden posent la question de l'extension extraterritoriale de la notion de souveraineté par effet de levier sur les opérateurs et la couche physique du réseau. La politique américaine de surveillance des flux mise en lumière à cette occasion n'est finalement possible que parce que les grands opérateurs sont américains (donc soumis à la législation du pays) et parce qu'une grande quantité de serveurs sont physiquement situés aux Etats-Unis.


CECyF
Une Convergence
institutionnelle, académique et industrielle,

B15 - Le pouvoir de la perturbation massive sur Internet

Intervenants :

- Damien BANCAL, Zataz.com.
- Fabien LORCH', Université de Versailles Saint Quentin.
- Jean-Christophe GATUINGT, Co-fondateur, Visibrain.
- Hubert SZAFARCZYK, Section veille numérique CAE DGGN.

Résumé des interventions :

Phénomène encore peu étudié, la perturbation massive sur Internet correspond à une forme d'utilisation du Web. Elle consiste à diffuser et à propager des messages et des informations, qu'elles soient avérées ou fausses, soit dans l'intention de mobiliser ou de réaliser de grands rassemblements, soit de manière spontanée, en réaction immédiate à des événements. Elle implique pour les États un risque de trouble à l'ordre public. Cependant, aucune mobilisation n'a pour unique source Internet ni ne doit son éventuelle efficacité qu'aux seules actions virtuelles. Internet agit surtout comme une caisse de résonance qui amplifie et accélère un phénomène.

I. Anticiper le risque de perturbation massive

Le premier risque de perturbation massive est l'utilisation d'Internet comme un prolongement de l'action citoyenne ou militante dans le monde réel. Les réseaux sont alors mis à contribution afin de faciliter et de renforcer la mobilisation : ils constituent un moyen complémentaire parmi d'autres (pétitions, manifestations physiques) au service d'un mouvement social ou politique. La démocratisation des outils d'accès à Internet et les caractéristiques du Web (immédiateté et viralité) permettent en effet de communiquer et de diffuser des informations très rapidement à de très nombreuses personnes.

La notion de perturbation massive recouvre plusieurs réalités très différentes les unes des autres. En effet, elle se manifeste à plusieurs échelles. Elle implique plus ou moins d'individus, peut avoir un impact sur le plan local, national ou international et sur une durée variable : de la simple mobilisation citoyenne, sous forme de pétition en ligne, aux manifestations et aux grèves jusqu'au soulèvement des foules, à la lutte contre les dictatures ou à la révélation de faits et de documents visant à ébranler et à remettre en cause le fonctionnement ou la souveraineté d'un État. Dans tous les cas, les acteurs s'appuient sur la capillarité d'Internet et sur les réseaux sociaux.

Les campagnes actives sur Internet ont démontré dans certains cas leur efficacité et leur capacité à influer sur les situations dans le monde réel. À titre d'exemples, on peut citer le Printemps arabe, la « Révolution verte » iranienne, le Mouvement des Indignés, le mouvement Occupy Wall Street, les affaires Snowden et Julian Assange, le soulèvement contre le régime syrien, les manifestations hostiles à l'Acta (accord contre la contrefaçon – Anti-Counterfeiting Trade Agreement). Dans chacun de ces cas, les protagonistes ont activement mis à profit Internet. Cependant, il faut aussi relativiser les effets réels de ces mobilisations numériques. Pour être efficaces, les agissements sur le Web doivent nécessairement se doubler d'actions sur le terrain et il est indispensable de les resituer dans un contexte politique et dans le cadre d'un rapport de force. La mobilisation sur le Web ne constitue pas une fin en soi. Les oppositions qui se manifestent par le biais d'Internet ne sont pas nouvelles mais le cyberespace leur offre une nouvelle dimension.

Dans les démocraties, il est important de suivre les possibilités de contestation, d'identifier sur la Toile les prémices de rassemblements massifs pour prévenir les troubles à l'ordre public dans une démarche non pas répressive mais d'anticipation. À cette fin, la gendarmerie nationale a mis en place une cellule de veille sur des sources numériques ouvertes.

Les éléments collectés sur Internet, croisés impérativement avec les données remontées du terrain, lui permettent d'adapter au mieux ses dispositifs à la situation. Effectivement, une distorsion peut apparaître entre la virulence des propos tenus sur Internet, les intentions exprimées, l'affichage en termes de mobilisation et la réalité : ce fut le cas par exemple des Bonnets rouges à Lille et des militants contre le projet d'aéroport Notre-Dame-des-Landes, très présents, incisifs sur les réseaux sociaux, semblant bien préparés, mais dont les actions sont restées comparativement limitées et n'ont pas été massivement suivies. A contrario, les forces de l'ordre peuvent être confrontées à des individus violents appartenant à des réseaux sans lien avec ceux formés sur le Web. Ainsi, Internet n'offre parfois qu'un reflet partiel ou déformant de la réalité et de la société.

Il s'agit de suivre également les réactions à l'actualité sur le Web afin d'anticiper d'éventuels dérapages ou débordements. Ce fut le cas par exemple pour l'affaire Dieudonné : tenter de déterminer à partir du contenu des commentaires diffusés sur le Net et de leur niveau de propagation l'éventualité d'actions collectives concrètes. Il n'est pas toujours évident d'identifier, dans la masse des données échangées chaque jour, les informations réellement pertinentes. L'idéal serait bien sûr de parvenir à percevoir les signaux faibles et ce travail est en cours de formalisation par la gendarmerie. Il est nécessaire à cette fin de procéder à un tri des informations et de faire preuve de discernement dans l'analyse des données.

L'organisation en ligne d'apéritifs géants ou de soirées « projet-X » (en référence au film du même nom réalisé en 2012) fait également l'objet d'une vigilance particulière par les forces de l'ordre, en raison du risque potentiel d'alcoolisation massive et de désordres multiples.

Une autre problématique de la perturbation massive provoquée par Internet réside dans la gestion de la propagation des rumeurs lors d'événements dramatiques (catastrophes climatiques…), de crises publiques (telles que les émeutes de Londres ou les attentats de Boston) ou même de manifestations physiques (telles que le « Jour de colère » le 26 janvier 2014, durant lequel circulaient de fausses informations, notamment sur le nombre de manifestants et sur les agissements des forces de l'ordre). Tous ces événements sont aujourd'hui commentés en direct et relayés très rapidement par les populations grâce à l'Internet mobile, via les ordinateurs, tablettes ou smartphones. Contagion de la panique, saturation des lignes d'urgence et des voies de communication, augmentation des accidents de la circulation sont des risques qu'il est nécessaire de prendre en compte et de maîtriser. Il est donc primordial que les institutions soient présentes sur les réseaux

sociaux afin de pouvoir réagir très vite par les mêmes canaux. Il s'agit de tuer dans l'œuf la rumeur en formation par des messages qui rétablissent officiellement la réalité des faits et qui, par le même phénomène de contagion, atteindront un large public. L'objectif est d'éviter qu'Internet impose, via les réseaux sociaux, un dévoiement de la réalité.

II. Les acteurs de la perturbation massive

Les leaders qui mobilisent pour une quelconque cause sur Internet, qui diffusent leur propagande ou mettent en place des stratégies d'agitation, mettent à profit les liens qu'ils ont tissés sur la Toile, très souvent fondés sur l'affect et sur la confiance. Leur force tient à ces communautés d'opinions et de centres d'intérêt partagés qui se sont créées selon un mécanisme d'universalisme du moi. Ils fréquentent les mêmes sites Web, s'intéressent aux mêmes sujets, et conformément à la théorie des agrégats, issue de la psychologie sociale, constituent ainsi une communauté. Ils ont la capacité d'activer leur réseau pour défendre une cause commune. Unis dans un mouvement de protestation ou de revendication, ils sont pourtant animés par une morale individualiste. Ils cherchent dans l'autre un miroir d'eux-mêmes, une confirmation de leurs idées, de leurs goûts, de leurs valeurs, une forme de reconnaissance. Les leaders les plus avisés utilisent plusieurs réseaux sociaux, afin d'atteindre des cibles et des publics différents et d'augmenter le nombre de leurs suiveurs.

Il existe deux niveaux de mobilisation : l'un visible et l'autre chiffré/masqué. Le premier concerne des individus pragmatiques se servant des qualités d'Internet pour diffuser massivement des messages. Le deuxième niveau concerne les hacktivistes ou cybermilitants les plus expérimentés, les mieux organisés et équipés, qui bénéficient de compétences techniques pour évoluer dans le « Darknet ». L'anonymat leur permet d'échapper à la surveillance et de préparer leurs actions en toute confidentialité. Cependant, cette couche invisible de l'Internet n'est pas accessible à tous ; et l'objectif étant de mobiliser le plus grand nombre et de se faire connaître, agir dans un espace clos, fermé et secret ne semble pas le moyen le plus approprié.

Les acteurs de la perturbation massive ont cependant la possibilité de se dissimuler derrière une identité virtuelle, notamment grâce à un pseudonyme. L'anonymat pose un problème aux services de l'État, pas aux internautes qui considèrent quant à eux qu'ils ont des identités multiples et que celle dite « virtuelle » n'est pas moins importante que celle dite « réelle ».

Si la capacité de mobilisation sur Internet est indéniable, il faut néanmoins considérer que le comportement des individus varie dans l'espace virtuel et dans l'espace réel. Manifester sur le Web ne signifie pas

systématiquement descendre dans la rue. Toutefois, le « slacktivisme » n'est pas à sous-estimer. Ce terme désigne les individus participant à un mouvement collectif virtuel sans s'engager concrètement. Pourtant, ils peuvent, au gré des circonstances, s'impliquer plus activement. D'abord passifs, se contentant de cliquer sur un « like », ils sont toujours susceptibles d'intensifier ou même de radicaliser leur mode de contestation. Même sans un basculement dans un mode d'action plus affirmé, il ne faut pas négliger ce que l'on peut appeler « l'importance du dérisoire ».

La perturbation massive est à la portée de tous, les relations étant caractérisées par leur horizontalité et chacun pouvant intervenir sur la Toile. Certes, la puissance de propagation d'un message demeure aléatoire et n'est pas totalement maîtrisée : elle dépend de facteurs qu'il n'est pas toujours aisé de cerner. Un élément, selon le moment, pourra être ou non relayé, sans que l'on sache vraiment pourquoi. Il n'en demeure pas moins qu'Internet constitue un outil de lutte pour la société civile, qui n'a plus besoin du relais des institutions et des organes officiels, tels que les partis politiques.


03

B 16 – Cyberdéfense : Vers une vision plus dynamique de la cybersécurité ?

Intervenants :

- Marc OLANIE, CNIS-Mag' (Computer, Network & Information Security),
- Garance MATHIAS, Avocat à la Cour, Cabinet d'Avocats Mathias
- Lieutenant-colonel William DUPUY, CALID,
- Yves LE FLOCH, directeur développement de la cybersécurité, Sogeti,
- Franck ROUSEE, responsable du segment Critical-IT, Orange Business Services,
- Dan SOLOMON, Directeur, Cyber Security Services, Optimal Risk Management Ltd.

Résumé des interventions :

Dans le domaine cyber comme dans le domaine purement militaire, la posture défensive peut se concevoir de manière statique (des défenses sont élevées derrière lesquelles on envisage de contenir l'agresseur) ou de manière dynamique (il s'agit alors d'ajouter aux obstacles fixes des manœuvres de déception voire de contre-attaques destinées à faire échouer l'agresseur avant qu'il n'arrive aux « remparts »). Il est cependant difficile d'envisager la légitime défense dans le cadre d'attaques cyber d'installations non classées OIV. Par ailleurs, les entreprises n'ont pas toutes les moyens de rémunérer une société spécialisée dans la cybersécurité. Toute la difficulté consiste donc à trouver une solution de sécurité adaptée aux ressources disponibles et à la sensibilité de l'entreprise.

I. Défense statique – défense dynamique

La mise en sécurité d'un système informatique et des données qui y circulent ou y sont stockées peut être conçue de façon statique ou dynamique. Dans le premier cas, il s'agit d'élever des défenses correspondant à la puissance estimée des attaques pouvant toucher le système. Ces défenses sont censées être suffisantes pour empêcher les intrusions et les dégâts qui en résulteraient. Cette conception donne au propriétaire du réseau l'espoir que le système survivra en cas de coup dur. On est là dans une démarche de sécurité des systèmes informatiques très basique. La cyberdéfense va évidemment plus loin. Elle englobe une phase préparatoire, qui consiste à analyser le système, identifier ses faiblesses et effectuer des tests. Suivent une phase pré-active, correspondant à la préparation des moyens de riposte, et enfin une phase active durant laquelle sont menées contre l'agresseur les actions de contre-attaque mises au point pendant la phase précédente. La cyberdéfense implique par conséquent l'existence d'une doctrine d'emploi des moyens de défense existants et la conception d'une manœuvre destinée à déjouer les attaques. Elle se conçoit dans la profondeur et de manière dynamique.

Le ministère de la Défense s'est doté, avec le CALID, d'un outil opérationnel mis à la disposition du chef militaire. Le CALID considère que l'adversaire a une capacité de réaction et d'apprentissage face aux actions de défense qui lui sont opposées. Il étudie également les attaques sous des angles différents : quelle est la finalité de l'agresseur, quels sont les effets qu'il recherche (dégâts physiques, acquisition d'informations, altération de e-réputation...) et selon quels critères temporels a-t-il conçu et lancé son attaque (on suppose qu'il choisit le moment de manière à amplifier les effets de son attaque).

L'approche militaire des cybermenaces et le vocabulaire qui y est associé ont, non sans raison, tendance à déteindre sur l'approche qu'ont les entrepreneurs de ces questions. En effet, le concept de cybersécurité active est parfaitement adapté aux entreprises. Ces dernières ne se demandent plus si une crise peut intervenir mais quand elle se produira. Elles doivent donc impérativement se préparer à gérer ces épisodes critiques.

Pour autant, tout n'est pas possible en matière de cyberdéfense. Le droit n'appréhende pas le risque mais prend en compte les préjudices réels. Dans le système juridique français, la légitime défense ne se conçoit que de manière proportionnée et concomitante, nul ne pouvant par ailleurs se faire justice lui-même. La rétorsion reste du domaine exclusif de l'État. La France s'est cependant dotée en 2013 de textes forts avec le Livre blanc sur la défense et la sécurité nationale et la loi de programmation militaire.

L'Union européenne, de son côté, a inscrit de longue date la lutte contre la cybercriminalité dans la liste de ses objectifs en termes de délinquance. L'UE marque d'ailleurs, depuis un an, sa volonté en la matière en renforçant Europol et la coopération policière et judiciaire internationale ainsi qu'en affichant son objectif de mettre en place des outils communs au sein des États Membres.

II – Des choix difficiles pour les entreprises

Face à une menace protéiforme et en constante évolution, le choix d'une politique de défense s'avère difficile pour les entreprises. Des facteurs d'ordre économique entrent d'abord en ligne de compte : les dispositifs ont un coût que toutes les entreprises ne peuvent pas supporter. Ainsi, la mise en place d'un SOC ne peut être envisagée que par une entreprise disposant de moyens financiers importants. On pourra cependant objecter que le coût supporté sera moindre que celui des conséquences d'une attaque à laquelle on n'a pas été préparé. D'autre part, dans un contexte économique difficile, le prestataire de services doit s'attacher à rendre plus performant le dispositif existant en commençant impérativement par ce qui contribuera immédiatement à améliorer la vie de l'entreprise. Lorsque l'expertise interne n'est pas envisageable, il est possible de se tourner vers un prestataire externe.

S'agissant des structures, les nombreuses interconnexions entre systèmes contribuent à la vulnérabilité des entreprises et invitent à penser la SSI de manière plus large. La question d'une gouvernance d'ensemble portant, par exemple, sur les opérateurs réseaux est posée. Dans le cas des OIV, l'État a d'ores et déjà pris des mesures.

La ressource en spécialistes constitue un autre élément limitatif pour les entreprises. Actuellement, il n'y a pas suffisamment d'experts pour armer l'ensemble des clients potentiels. Le ministère de la Défense, pour des raisons d'ordre stratégique, conserve en son sein une capacité propre qui lui permet de rester indépendant dans le domaine.

S'agissant enfin des modes d'action proposés aux entrepreneurs par les spécialistes de la sécurité informatique, ils couvrent une palette assez large. Tout en haut de la gamme, les tests grandeur nature sont complexes à mettre en œuvre. Ils nécessitent une grande confiance de l'entreprise vis-à-vis de l'opérateur qui effectue la tentative d'intrusion, une information des clients (au risque de les effrayer), des autorisations délivrées aux testeurs qui accéderont peut-être à certaines bases de données... Les exercices d'intrusion de type « red team » sont destinés à se rapprocher des conditions d'une attaque réelle. Ils sont d'une durée plus longue et touchent un périmètre élargi (incluant en particulier du social

engeneering destiné à capter auprès des collaborateurs des informations de nature à faciliter l'entrée dans le système visé). Ils restent cependant assez peu fréquents. Les mesures adoptées par les entreprises sont davantage liées à la préparation de la gestion d'une crise. Quant aux mesures de réponse actives (les contre-attaques), elles sont, pour les raisons juridiques exposées précédemment, très difficiles à envisager. La mise en œuvre de moyens de déception constitue une alternative qui ne doit pas être négligée. Il s'agit d'identifier ce qui, au sein du système à défendre, peut constituer l'objet de la convoitise potentielle d'un tiers puis de créer une sorte de double ne renfermant aucune donnée essentielle et qui détournera l'attention de l'agresseur de sa véritable cible. Nécessitant moins de moyens, ce mode de défense est fiable et permet a minima de gagner du temps en cas d'agression.

B17 - Rôle du RSSI dans la dématérialisation.

Intervenants :

- Gérôme BILLOIS : Senior Manager, Solucom
- Isabelle RENARD : FEDISA, avocat,
- Alexandre BARBOT : Responsable commercial Sécurité intérieure, SOPRA Group,
- Vincent JAMIN : Directeur dématérialisation, Docapost,
- François VERGEZ : Directeur, Deloitte,

Résumé des interventions :

La dématérialisation est un choix d'entreprise qui nécessite un engagement au plus haut niveau afin d'assurer un pilotage du projet qui tienne compte de la gestion du risque et de son environnement juridique. Elle place le RSSI dans un rôle de facilitateur et de conseil. Intégré dès le début dans la gestion du projet avec le CIL, les fonctionnels et les informaticiens, ce dernier concourt à la résilience de l'entreprise et à des processus fiabilisés dès la conception donc techniquement et commercialement viables.

I. La dématérialisation : un choix stratégique

La dématérialisation correspond à une démarche ambitieuse qui touche tous les processus de l'entreprise. Elle provoque des changements des modes de travail. Elle nécessite que le plus haut niveau hiérarchique de l'organisation s'implique. Cela se manifeste par des directives, des comités de pilotage, une politique promotionnelle et la mise de sens dans la démarche.

Les décideurs sont généralement convaincus de la nécessité de s'engager dans une dématérialisation ou de l'accroître notamment en termes d'efficacité des services et de réduction de leur coût. Au sein des administrations, l'augmentation de la qualité du service auprès du citoyen passe par plus de dématérialisation et plus de mobilité. La dématérialisation pose toutefois la question de la modernisation des habitudes de l'entreprise. Une des difficultés essentielles rencontrées, tant au sein de l'entreprise qu'au sein de l'administration, est de déterminer en interne une conduite du projet acceptable, de concevoir une communication sur chacune de ses étapes et d'associer les acteurs à la définition des processus nouveaux.

Les processus doivent être simples à mettre en œuvre pour être facilement acceptés ou apporter une plus-value significative. Deux exemples concrets : consulter un double électronique des factures ou, pour un opérateur intervenant sur une panne, obtenir le plan d'une propriété à partir d'un dossier client.

Les clients attendent de la dématérialisation une efficacité au travers de deux piliers, à savoir la conformité et la sécurité. Il faut donc apporter des garanties en termes de sécurité, de la performance, une réactivité, une productivité (gestion des documents, des factures, etc.) et un gain en trésorerie. Un accompagnement des clients doit permettre de déterminer les modalités de la transition en termes d'organisation. Il comporte une dimension supplémentaire par rapport aux objets connectés et aux applicatifs déployés sur les smartphones dont le niveau de sécurisation est perfectible.

II. La problématique de l'identification

Il ressort des évaluations, dans l'état de l'art, une forte capacité technique en termes de fiabilité, hormis la problématique de l'identification et de la confiance. Celle-ci concerne notamment les grands acteurs (banques, assurances…) qui hésitent parce qu'ils ont du mal à évaluer le risque.

Les systèmes ont un niveau de fiabilité satisfaisant mais il subsiste une inquiétude quant à l'intégrité du document dématérialisé par rapport au document original ; d'où l'importance de la signature électronique ou d'un certificat reconnu. La dématérialisation du processus papier doit

être accompagnée juridiquement pour établir une équivalence des documents numériques par rapport à leurs équivalents « papier » (signature électronique, personne qualifiée). Si on prend le cas du vote électronique, on note une grande facilité à contourner ce processus qui obère sa pertinence.

Les analyses montrent également les dangers de la prise de contrôle du site externe, hébergeur de ses données ou de ses applicatifs, par un tiers. Il faut donc vérifier le niveau de sécurité du site prestataire. La problématique essentielle repose sur le coût de l'authentification et de la gestion de l'usurpation de l'identité. Il y a pléthore de solutions techniques d'une mise en œuvre assez simple tout en se prémunissant de produits récents relevant du gadget. Cela reste plus compliqué avec des opérateurs distants qui appliquent leurs propres procédures Web. Il y a alors deux cas de figure « B to C» : soit on reste derrière le site Web du client et on adhère de fait à son système de protection, soit il faut procéder à une authentification interne. À titre d'exemple, DOCAPOST authentifie la transaction par mot de passe et un login avec complément par SMS. Cette technique simple se révèle efficace. Si l'identité avec une remise « face à face » est facile à déployer, on peut se poser, selon les transactions, la question de l'utilité de s'assurer de l'identité de la personne. Un processus d'identification avec étoiles dans un « face à face » plus ou moins formel, selon la transaction, peut satisfaire le RSSI et le client.

On peut estimer que la fourniture de l'identité du futur relève d'une prérogative régalienne qui évolue dans l'état de l'art au détriment d'acteurs externes comme Facebook qui sont dans une démarche de consumérisation en diversifiant l'identité et en la diluant selon les activités de l'internaute. En effet, les pratiques montrent l'apparition de nouvelles personnalités juridiques qui doivent être gérées dans un cadre institutionnel fiable. Ce devrait être un domaine régalien mais les projets de gestion d'identité se sont montrés difficiles à mener. La carte nationale d'identité électronique pouvait être utilisée à des fins différentes (identification lors de transactions commerciales) mais elle a été abandonnée. Une dimension culturelle doit être prise en compte car une forte opposition subsiste quant au fichage de masse et un consensus se dégage au niveau européen quant à la protection des libertés. Le danger essentiel, tel qu'il est ressenti en termes de limite sociologique, est la mise en œuvre d'un système de croisement de bases de données qui puisse dévoiler un individu dans toutes les composantes de sa personnalité.

III. L'accompagnement juridique de la dématérialisation

La problématique est d'inclure la sécurité en amont. La tendance actuelle est

l'externalisation stratégique. Cela veut dire que l'on supporte le risque des sous-traitants. Il faut donc instaurer des instruments de contrôle et rédiger des contrats qui comprennent la gestion du risque.
Juridiquement tout peut être dématérialisé sauf pour de rares actes définis par la commission européenne. Les directives concernées ont d'ailleurs fait l'objet en France d'une transposition assez libérale. Ces exceptions concernent essentiellement le droit de la famille et des sûretés ou garanties sur les personnes physiques. Ces dispositions peuvent être un frein à la dématérialisation par une sur-garantie. On peut donner en exemple les bulletins de salaire dont la dématérialisation a dû passer par une mention dans le code du travail. Plus récemment, on peut citer la problématique des recommandés dans la gestion de la copropriété.

IV. Le rôle du RSSI dans la dématérialisation

Penser la sécurité dès le départ n'est pas complexe si la démarche est pluridisciplinaire et prend en compte le fonctionnel (qui initie le processus), l'informatique, la sécurité et l'accompagnement juridique. Le rôle du RSSI, gardien du secret de l'information, dépend du type de processus et de domaine traité par rapport à la gestion du risque. Il est particulièrement sensible si le domaine traité a une incidence réglementaire ou légale fluctuante ou concerne un domaine purement opérationnel. La gestion du risque est le domaine essentiel du RSSI.
Un questionnement subsiste dans la pratique quant à l'insertion du RSSI dans le projet. Certaines sociétés disposent d'un Comité de sécurité où est intégré le RSSI. Un intervenant précise que sa société a investi massivement sur la sécurité en 2013. Le but de cet effort est une forte amélioration de toutes les procédures. Aucun projet n'y est mené sans sécurité.
En termes d'administration de l'État ou des collectivités, la présence du RSSI est bien ancrée. La dématérialisation, notamment en matière de service aux usagers, fait que la dimension de sécurité est présente. Aucun projet n'est avalisé si sa sécurité n'est pas prise en compte.
Le RSSI n'est pas monolithique et sa position sera différente selon la maturité de l'entreprise. Des témoignages montrent que le RSSI n'est pas toujours intégré dans les projets. Pour certains, son rôle n'est pas encore entièrement reconnu et il subsiste un problème de définition du poste au sein de l'entreprise. Pour d'autres, il est vu par le fonctionnel comme un fournisseur de contraintes notamment quand des délais très réduits doivent être tenus. On note également une application de règles de sécurité sans explication qui conduisent à des blocages. Ainsi, au sein de l'entreprise, une politique trop restrictive des fichiers en

format PDF finit par conduire à une limitation de la communication interne. En réalité, le RSSI est un facilitateur qui propose des solutions. Il a un rôle de conseil sur la sécurité du système d'information ou du processus. Il existe des enjeux de métiers ou de business qui font qu'on doit passer par la dématérialisation. Le RSSI joue un rôle dans le projet, que cela soit en interne ou dans la gestion des attentes du client. La bonne pratique est qu'il soit intégré dès le départ du processus afin qu'il puisse traiter avec les administrateurs centraux et fixer l'exigence en fonction du risque. S'il n'intervient pas directement, il faut qu'il donne son aval et qu'il ait vu les documents. Si le projet est initié par un fonctionnel, il faut mettre en face un RSSI qui sait poser les questions et dialoguer.

On peut également évoquer le rôle du CIL (Correspondant informatique et libertés) dans l'organisation de l'entreprise. Il est important qu'il soit impliqué lors de la mise en œuvre de méthodes d'identifications ou de certifications comportant de fortes contraintes réglementaires, typiquement lors de la réalisation de signatures par tablettes ou d'enregistrements locaux pour renforcer l'autorisation selon les préconisations de la CNIL. C'est un frein à la mise en œuvre du processus, donc il doit être consulté très tôt pour éviter un blocage légal. Sa place dans l'organisation et sa relation avec le RSSI doivent éviter qu'il soit mis devant le fait accompli.


- Encrypted calls
- Encrypted Emails
- Encrypted SMS
- Controlled communication ports
- Biometric authentication
The integrally secured smartphone
hoox
BULL
POWERED BY
CRYPTOSMART
marque appartenant à ERCOM

B 18 – Sécurité des moyens de paiement et innovations technologiques

Intervenants :

- Animateur –. Benjamin MARECHAL, Manager – FIDS, EY
- Catherine Rosalie JOLY, avocat, Cabinet Ulys
- Philippe LE PAPE, directeur commercial Europe, Moyen-Orient, Afrique, MORPHO
- Bernard SCHRAMBACH, expert SI et moyens de paiement, Société Générale
- Thomas SOUVIGNET, capitaine de gendarmerie, IRCGN
- Annabelle TRAVERS-VIAUD, consultante cybersécurité senior, Bull

Résumé des interventions :

L'apparition de nouveaux moyens de paiement a entraîné une double évolution. D'une part, les modes de paiement à distance, désormais entrés dans les mœurs, sont utilisés pour un nombre croissant de transactions et impliquent un renforcement des modes d'authentification des utilisateurs. D'autre part, le droit a dû évoluer pour garantir la protection du consommateur et des paiements.

Pour autant, le sujet n'est pas clos. La sécurité déploie aujourd'hui des moyens qui réduisent l'ergonomie des outils ou qui conduisent à l'utilisation de données personnelles, telle la biométrie. Au final, il semble nécessaire de retenir un principe de proportionnalité, selon l'importance du paiement effectué.

L'article L311-3 du Code monétaire et financier définit comme moyen de paiement « tous les instruments qui permettent à toute personne de transférer des fonds, quel que soit le support ou le procédé technique utilisé. ». On y trouve les moyens de paiement traditionnels, tels que le chèque, le virement, la carte bancaire. Cependant, ces dernières années ont connu d'importantes évolutions technologiques, induisant des modifications du comportement des consommateurs. Il en résulte une adaptation du droit tandis que les principes de sécurité se renforcent.

I - Une évolution technologique rapide mais un droit qui s'adapte

À l'origine, le droit ne connaissait que quelques moyens de paiement : chèque, virement et cartes bancaires. Le cadre réglementaire correspondait à un mode de fonctionnement en « face à face », sécurisé par la production de pièces d'identités et la comparaison entre celles-ci et leur porteur. Puis se sont développés la vente à distance et le paiement sur internet.

Il était important de maintenir la confiance dans les dispositifs de paiement d'autant que toute une série de services de paiement se sont exonérés du monopole bancaire : retrait et dépôt en espèces, prélèvements, paiements par carte, transfert de fonds, facturations électroniques (par les opérateurs téléphoniques par exemple). De nouveaux moyens de paiement sont apparus, comme le téléphone mobile. Le droit a évolué en deux temps. La protection du consommateur en matière de paiement par carte à distance a été renforcée, en prévoyant des cas d'irresponsabilité ou d'obligation de remboursement, avec prise en charge du risque par la banque. Puis de nouvelles solutions de paiement se sont développées dans le domaine de la monnaie électronique et le prépayé. Les textes législatifs se sont succédé à un rythme annuel. Ce sont soit des directives de l'Union Européenne sur la monnaie électronique en 2002 puis 2009 ou les services de paiement en 2007, 2009 ou 2013, soit des transcriptions du droit européen dans le Code monétaire et financier. Aujourd'hui, c'est l'opération de paiement et non l'instrument utilisé qui détermine le droit, les recours et la protection. L'usager bénéficie de la même protection, des mêmes recours et des mêmes obligations en termes de délais d'exécution.

II - Une innovation technologique qui se heurte aux contraintes de la sécurité

Aujourd'hui, une opération d'achat sur internet est à peine plus simple qu'il y a 20 ans. C'est pourquoi le nombre de transactions reste encore limité aux alentours de 10% du marché, cette faible volumétrie engendrant un montant de fraude encore acceptable. Cependant, les solutions de paiement qui se développent actuellement, les « wallets »,

simplifient ces transactions, ce qui va développer l'e-commerce mais aussi la fraude. De plus, ces nouveaux modes de paiement à distance – avec un téléphone par exemple – s'étendent également au commerce de proximité et laissent penser que la fraude pourra devenir très importante.
A ce jour, il existe un grand nombre de solutions pour authentifier le propriétaire de l'instrument de paiement. Pour les petits montants, les mots de passe sont simples, voire inexistants (par cartes sans contact notamment). D'autres solutions proposent des moyens d'authentification rigoureux : biométrie, mot de passe avec double facteur. L'Union Européenne encourage l'authentification forte pour les paiements à distance. C'est possible aujourd'hui grâce à l'évolution des technologies qui permettent d'avoir accès beaucoup plus facilement à la biométrie par exemple. L'idéal, même si ce n'est pas la seule solution, est d'arriver à une authentification à double facteur - « out of bank » - qui offre une opération de paiement clairement sécurisée.

III - La recherche du juste équilibre entre ergonomie, sécurité et respect de la vie privée

La sécurité se heurte à l'ergonomie. Imposer un code PIN à 8 ou 10 chiffres semble impossible. Le système 3DS exige la saisie d'un code reçu par SMS, ce qui peut sembler lourd pour le consommateur. Et si le taux de fraude baisse sensiblement, les commerçants s'en méfient parfois en raison du frein qu'il constitue aux e-achats. Les « wallets » comme Paylib utilisent une solution dite « out of bank ». L'achat commence sur le site commerçant et se termine par la validation sur une application bancaire sur téléphone mobile. La biométrie offre également une possibilité forte de sécurisation, en combinant de plus des éléments très authentifiant comme la reconnaissance vocale, faciale ou du réseau veineux.
Cependant, le respect de la vie privée et la Loi «informatique et liberté» exigent que les niveaux de protection soient proportionnés à la nature de l'opération. La biométrie doit être encadrée, notamment pour celui qui conserve la donnée. Il faut éviter de recouper les fichiers. Le positionnement du curseur est très large, entre ergonomie, sécurité et respect de la vie privée. On n'opérera pas les mêmes choix pour des paiements de petit montant faits par un particulier, et pour les gros virements ou prélèvements, faits par des entreprises. Pour les particuliers la sécurisation a commencé par des mots de passe, puis de l'out of bank,. Pour les trésoriers d'entreprises susceptibles d'agir sur de gros volumes, la biométrie est concevable.
Enfin, il convient de se souvenir que la délinquance est très adaptable. S'il y a trop de « portes blindées », les criminels s'attaqueront alors au maillon faible, l'homme. On voit ainsi se développer les méthodes dites « d'ingénierie sociale », qui coûteraient 200 millions par an aux entreprises françaises (la plus connue de ces méthodes est celle dite « au

faux patron », l'escroc se faisant passer pour le chef d'entreprise auprès d'un employé soigneusement choisi afin d'obtenir un virement sous un motif hautement confidentiel). La réponse ici n'est plus technologique mais organisationnelle.

B19: Les réserves Cyber : quels dispositifs mettre en œuvre ?

Intervenants :

- Lieutenant-colonel Stéphane DOSSE (Ministère de la Défense - France)
- Sébastien BOMBAL, Responsable sécurité opérationnelle et des systèmes industriels, AREVA
- Hans FOLMER (Commander Task Force Cyber, Ministère de la Défense des Pays-Bas)
- Lieutenant-colonel Philipe MIRABAUD (Chargé de mission cybersécurité et numérique auprès du directeur général de la gendarmerie nationale)
- Andrus PADAR (Ministère de la Défense Estonien)

Résumé des interventions :

Si le risque « cyber » est désormais un truisme, les approches internationales et surtout nationales des « cyberréserves » méritent une attention et un examen particulier.
À cet égard, les intervenants font le point exhaustif des réalités des postures de cyberdéfense et de cybersécurité et permettent d'établir un parallèle utile entre trois politiques : celles de la France, des Pays-Bas et de l'Estonie.
Si la logique public/privé emporte globalement l'adhésion et permet de souligner le caractère interdisciplinaire et interministériel de cette réserve (en France notamment), l'exemple des Pays-Bas et de l'Estonie révèle clairement les contraintes des « petits pays »

I. La réserve cyber/ citoyenne française, une logique de prévention par un partenariat public/privé

Constituée de personnalités extrêmement diverses, tant publiques que privées, la réserve cybercitoyenne française, sorte de melting pot de bonnes volontés n'ayant pour but que le service altruiste du pays, condense un très large panorama de compétences et offre une véritable perspective interministérielle pour la réflexion stratégique ou de plus court terme.

L'ensemble de ses membres travaille bénévolement sur les problèmes cyber et ce réseau soutient la posture nationale de cybersécurité.

Magistrats, militaires, acteurs de sociétés privées et des opérateurs d'importance vitale se réunissent au sein de groupes de travail, y partagent des expériences et des points de vue et fédèrent les compétences interdisciplinaires (scientifiques, sciences humaines, langues, droit, etc.).

Cependant, le réseau jusque-là limité à son creuset de naissance parisien, demande désormais à s'étendre davantage vers l'ensemble des régions. Certaines d'entre elles ont cependant d'ores et déjà constitué localement un réseau étoffé.

Le schéma de fonctionnement reste campé sur ses socles fondateurs. Ainsi, six thèmes réunissent en groupes de travail les réservistes citoyens, en fonction de leurs compétences et domaines d'excellence. Les groupes ainsi définis ont pour thème: élus et journalistes, les jeunes et la formation, les think tanks, les PME/PMI, les grandes entreprises, et enfin les réservistes citoyen cyber (RCC).

II. Les exemples étrangers ; une approche par « l'essentiel »

Les Pays-Bas et l'Estonie ont une taille et des moyens humains plus contraignants qui invitent naturellement, et en toute logique, à adopter une démarche très ciblée.

Aux Pays-Bas, la problématique majeure est celle des moyens humains. En effet, le nombre des experts et le spectre de leurs compétences sont assez réduits et limite d'emblée les ambitions. D'autre part on assiste à un engagement limité des entreprises dans cette démarche en raison des contraintes de résultats immédiats et constants qui pèsent sur elles.

C'est pourquoi l'idée du volontariat s'est rapidement imposée. Une véritable task force a été constituée sur la base de volontaires pressentis par les autorités en raison de leurs compétences bien identifiées dans des domaines intéressant la Défense.

Des problèmes subsistent cependant, notamment s'agissant des questions liées au domaine cyber. Celui-ci embrasse de multiples secteurs et oblige à prendre en compte toute une mosaïque de cas particuliers et à définir en amont des listes de « compétences ». C'est pourquoi la logique hollandaise embrasse deux types d'entités à vocation dédiée. La première regroupe des conseillers et a une visée préventive tandis que la

seconde, à objectif curatif, rassemble plutôt des techniciens.

Le gouvernement estonien, pour sa part, a délibérément opté pour la plus grande flexibilité. Il peut tirer profit de la loi de 2010 sur le service national qui autorise l'objection de conscience. Les objecteurs de conscience, à défaut de porter les armes, sont a minima invités à se montrer actifs au profit de la cyberdéfense, nonobstant le but final identique de défense de la patrie.
En Estonie sont définis deux niveaux de compétences en matière de sécurité des réseaux et des informations. Ainsi distingue-t-on un réseau d'hyper-spécialistes, et un second groupe composé de techniciens qui sont des relais, au sein des entreprises, pour le développement d'une culture SSI performante.
Une question demeure cependant sans réponse satisfaisante aux yeux des praticiens : comment et par quel truchement faire participer le maximum de citoyens au nécessaire développement de la prévention du risque cyber?
Une solution par défaut a pour l'instant été retenue. Il s'agit d'établir et de réaliser un grand nombre d'entraînements communs avec l'armée et de garantir ainsi une véritable interopérabilité s'appuyant sur une bonne connaissance réciproque des sociétés privées et des agents de l'État. Il s'agit également, par ce biais, d'encourager au sein des entreprises une politique active de mise en sécurité des réseaux et du patrimoine d'information qu'elles détiennent.

B 20 – Neutralité du Net : un mythe ?

Intervenants :

- Stéphane BORTZMEYER, AFNIC
- Bertrand de LA CHAPELLE, Membre du Conseil d'administration, ICANN ; Directeur du projet Internet et Juridiction, Académie diplomatique internationale
- Gérard PELIKS, président de l'Atelier sécurité,Forum ATENA
- Robin WILTON, Internet society

Résumé des interventions :

Véritable mythe fondateur, le principe de neutralité du Net désigne un Internet libre et ouvert dont le contenu ne devrait être altéré sous aucun prétexte.

Le débat sur la neutralité du Net est impacté par la nature même de celui-ci. En effet, le cyberespace relève d'abord d'une gestion structurelle avec les aménagements des infrastructures et les producteurs de protocoles et de logiciels. Dans l'absolu, cette neutralité entend défendre la libre circulation de l'information par tout le monde et pour tout le monde. Pourtant, des rapports de force s'exercent dans cet espace, notamment sur le plan financier. En effet, la mise en œuvre de la neutralité du Net repose sur des réseaux performants, rapides et sécurisés, ce qui implique des investissements dans une économie de marché et de droit.

Mais le débat ne peut s'affranchir du véritable enjeu sociétal du droit à l'information et à la liberté d'expression dans le respect des lois nationales et des conventions internationales. La neutralité du Net doit être considérée comme un facteur de développement économique et culturel. La question n'est donc pas de savoir si la neutralité du Net est un mythe ou pas mais plutôt dans quelles conditions on peut y parvenir.

I – Les enjeux

La notion de neutralité consiste à transmettre, sans modifications, un paquet d'informations d'un point A vers un point B, quels qu'ils soient. L'ensemble du « *trafic internet doit être traité de façon égale, sans discrimination ni altération, sans traitement préférentiel ou suppression, indépendamment de l'expéditeur, du destinataire, du type, du contenu, de l'appareil, du service ou de l'application* ». Le principe de neutralité vise à garantir une utilisation d'Internet transparente et égalitaire, sans discrimination de contenus ou d'utilisateurs.

Le processus de diffusion est un système constitué de trois couches imbriquées. La première concerne les infrastructures, c'est-à-dire les installations physiques qui favorisent la diffusion. Ce sont les « tuyaux », les câbles, la fibre optique, les satellites. À partir du moment où l'utilisateur attend que son paquet d'information circule librement quel que soit le chemin emprunté, il entend n'être limité ni dans son libre accès aux réseaux ni dans le choix de ses propres ressources du Net. Les protocoles et applications, qui constituent la seconde couche, gèrent et hiérarchisent la diffusion des types de paquets. Le traitement discriminé des services rendus, pour des raisons techniques ou commerciales, est contre-productif au regard de la neutralité du Net.

Enfin, la troisième couche est la plus complexe. C'est celle de la sémantique, du sens de l'information. L'information, sur le plan technique, n'est qu'une suite de 1 de 0. L'intrusion d'informations malveillantes (virus...) ou commerciales est clairement identifiable et condamnable. Le niveau d'intervention pour se protéger de ces intrusions détermine le niveau de neutralité. Soit l'intervention se situe au niveau du réseau, soit l'utilisateur seul accepte ou bloque les éléments qui arrivent sur son ordinateur. Le niveau de capacité à se préserver est donc un élément quantifiable et objectif. En revanche, le sens, la sémantique, ne sont pas des notions neutres. Le contrôle du contenu de l'information, sa diffusion libre ou réduite, sa censure ou l'interdiction d'y accéder constituent des indicateurs du niveau de liberté et de neutralité du Net à un endroit donné.

Les trois niveaux impactent l'accessibilité au Net et sa neutralité. Paradoxalement, la notion éthique de la libre circulation grâce à la neutralité du Net s'efface au profit de la logique économique. Mais le débat ne se réduit pas à une lutte d'influence, car les acteurs ont intérêt à s'entendre. La question de la neutralité du Net ne peut donc se réduire à une sémantique manichéenne, pour ou contre, mais doit donner lieu à en une reformulation nuancée de la gestion complémentaire des trois couches.

II – La neutralité du Net en question ou en construction ?

La neutralité en termes de capacités technologiques des fournisseurs d'infrastructures, de gestion des producteurs de services et de contenus et enfin d'accès libre et non discriminatoire des utilisateurs, n'est pas un mythe mais un objectif. Le marché des communications électroniques est au cœur de l'économie numérique. Pour permettre d'exploiter pleinement ce potentiel du marché unique numérique en matière de croissance, de compétitivité et d'emploi, il convient de renforcer le rôle joué par les télécommunications en faveur de l'innovation et de la connectivité dans tous les secteurs de l'économie. Mais si les fournisseurs de réseaux sont amenés à respecter l'égalité des droits d'accès, la protection des droits individuels passe par une réglementation nationale et internationale. En protégeant la sphère privée et l'utilisateur, la neutralité de la diffusion des données du Net favorisera le développement et la protection des avantages sociaux et économiques.

La régulation d'Internet s'effectue à deux niveaux. Elle se fait a priori par les opérateurs qui permettent la diffusion matérielle de l'information. En effet, pour que le Net soit accessible à tous, il faut que les réseaux soient performants et sécurisés. En revanche, la régulation entre les opérateurs en termes d'infrastructures et de protocole est nécessaire afin de limiter les abus économiques au détriment des utilisateurs et de limiter la fracture numérique.
En amont, la régulation s'effectue a posteriori et revêt une forme judiciaire. L'internet doit être libre de toute censure gouvernementale mais également respecter la loi. L'impunité de l'internaute ne peut être justifiable. Le respect des droits en matière de confidentialité des communications ainsi que la protection de la vie privée et des données à caractère personnel sont les éléments essentiels qui permettent aux utilisateurs d'avoir confiance dans les communications électroniques. Les utilisateurs finaux doivent avoir l'assurance que ces droits sont respectés à chaque fois qu'ils ont recours aux services et réseaux de communication électronique. Ils doivent aussi avoir la certitude que toute interférence avec ces droits est proportionnée et nécessaire, et qu'elle répond à un objectif légitime clairement spécifié.

En définitive, la neutralité du Net apparaît comme un bien commun. Cette notion, en droit international, est bien spécifique. Elle implique en matière de régulation des coopérations et des relations inter-étatiques. Dans la sphère de l'Internet la régulation et la gouvernance passent aussi par les trois acteurs déjà énoncés, les infrastructures, les protocoles et les utilisateurs. Le modèle actuel est fortement ancré dans un système de lobbying auprès des institutions nationales et internationales, dans une opacité totale. Il serait opportun de passer à une gouvernance collaborative qui limite l'appropriation du

système par certains intermédiaires et favorise les capacités d'innovations des internautes. L'Internet offre un potentiel énorme de développement social et économique. Dans ce contexte, le caractère libre et ouvert de ce média, la capacité du réseau à fonctionner et à fournir des services ainsi que le caractère inclusif de l'architecture du réseau, garantissant à tous les groupes de population et opérateurs du marché un accès sans discrimination à tous les contenus et des possibilités de participation active, revêtent une importance essentielle. La protection juridique de la neutralité de l'Internet constitue une condition préalable à la pleine exploitation de ce potentiel et à la sauvegarde de la diversité et du pluralisme. En raison de son caractère ouvert et non discriminatoire, l'Internet s'est révélé être un moteur d'innovation pour le développement social et économique. Sa neutralité révèle la capacité des acteurs à négocier pour un objectif réalisable et non pour une utopie.

B 21 – UE/OTAN : Quelles complémentarités ?

Intervenants :
- Axel DYEVRE, directeur du bureau européen CEIS
- Monsieur Detlef PUHL, OTAN
- Madame Heli TIIRMAA-KLAAR conseillère en politique de cyber-sécurité, UE
- Lieutenant-colonel Patrice TROMPARENT, Ministère de la défense

Résumé des interventions :
Dans la lutte contre les risques et menaces du cyber, l'Union Européenne et l'OTAN n'en sont qu'au début d'une collaboration pour trouver des complémentarités. Cette collaboration ne peut prendre la place des politiques et choix des États membres qui restent souverains en matière de défense et de sécurité.

I. Les avancées des deux organisations.

L'OTAN, dans sa stratégie de cyberdéfense, cherche avant tout à protéger ses propres réseaux en s'appuyant sur :
- la modernisation des outils et processus,
- la mise en place d'une politique cyber au sein des structures militaires,
- l'identification des besoins critiques des systèmes et réseaux des pays membres,
- le développement de la prise de conscience des enjeux du cyber,
- une coopération adaptée aux partenaires : pays tiers, privé, autres organisations internationales.

L'Union Européenne, quant à elle, place l'État membre au centre du dispositif de la cybersécurité. Bruxelles ne peut donner que des directives. La lutte contre les menaces sur les réseaux numériques doit également tenir compte de la forte prédominance du secteur privé dans ce domaine.
L'Union Européenne a proposé en 2013 une stratégie en matière de cybersécurité qui se décline en cinq objectifs :
- renforcer la capacité de cyberdéfense,
- développer la résilience cyber au niveau de l'ensemble de l'Union Européenne,
- lutter contre la cyberdélinquance,
- renforcer les capacités technologiques pour faire face aux nouvelles menaces,
- préparer les réunions internationales sur le cyberespace et la cyberdéfense.

Les deux organisations internationales développent des outils et stratégies avec la conscience que les États membres demeurent des acteurs clés de la lutte contre les cyberattaques. C'est une mission fondamentale des États membres, cette responsabilité ne peut en effet se partager au sein d'une organisation internationale.

On note que les deux organisations s'inscrivent avec raison dans la nécessité de collaborer et de développer des complémentarités dans ce domaine.

II. Les possibilités d'actions complémentaires

Les deux organisations sont favorables à des rapprochements afin de lutter contre la menace que le cyber peut faire peser sur elles.
Pour autant, la nature même du cyberespace peut rendre difficile la définition du rôle de chacune des organisations dans une collaboration. Cette situation est parfaitement illustrée par le concept du continuum sécurité/défense qu'a présenté le général d'Armée Watin-Augouard.

Pour l'OTAN, il est possible de déterminer trois complémentarités entre les organisations. Il s'agit d'éviter des doublons en matière de défense, de partager des infrastructures de formation et d'échanger sur les retours d'expérience en matière de gestion de crise.

Du côté de l'UE, la collaboration commence à se matérialiser au travers de rencontres afin d'envisager le développement de capacités d'actions communes et de développer des techniques standards entre les deux organisations. Il est évident qu'il s'agit de se tenir informés des actions des uns et des autres dans ce domaine et de partager les expériences. L'UE convient également d'éviter de créer des doublons et d'associer les forces des deux organisations.

Les contraintes

Cette réelle volonté de développer des complémentarités entre les deux organisations ne doit pas cacher certaines réalités.
La première d'entre elles est la place que tiennent les États membres dans chacune des organisations. En matière de protection des réseaux numériques, chacun des États conserve sa souveraineté. La politique d'entraide qui prévaut au sein de chacune de ces organisations présente des limites pour les États membres qui ne peuvent pas uniquement s'en remettre à ces organisations. On toucherait aux principes même de souveraineté des États. Cela sous-tend donc que les complémentarités présentent certaines limites.
Une autre contrainte est celle de la nature même des deux organisations. L'OTAN est une alliance militaire. L'Union Européenne dispose quant à elle de sa propre politique et de ses moyens de défense, elle ne peut les sacrifier au motif du risque de la création de doublons avec l'OTAN qui disposerait dans ce domaine de plus d'expériences pour faire face à des attaques.

Pour conclure, il est possible de souligner que l'Union Européenne est dans son rôle quand elle protège ses infrastructures et quand elle appuie le développement de l'industrie en cyber sécurité. L'OTAN de son côté est en avance dans le domaine de la cyberdéfense et devrait partager ses procédures et standards.
Il est possible d'envisager de développer et bâtir des systèmes d'alerte communs, de partager l'information et de créer un système de reporting sur les incidents cyber. De même, les exercices communs sur ce domaine doivent être automatiques..

FIC 2015

Cybersécurité
et Transformation Numérique

7ème Forum International de la Cybersécurité

CO-FINANCÉ PAR

RÉGION NORD-PAS DE CALAIS

ORGANISÉ PAR

Sogeti est l'un des leaders des services informatiques et d'ingénierie de proximité, spécialisé dans la gestion des applicatifs et des infrastructures (*application and infrastructure management*), le conseil en technologies (*high-tech engineering*). Sogeti propose des solutions innovantes autour du Testing, du Business Intelligence Management, de la Mobilité, du Cloud et de la Cybersécurité, s'appuyant sur sa méthodologie et son modèle mondial de prestations de services Rightshore®.

Présente dans 15 pays avec plus de 100 implantations en Europe, aux Etats-Unis et en Inde, la société réunit plus de 20 000 professionnels. Sogeti est une filiale à 100% de Cap Gemini S.A., coté à la Bourse de Paris.

Plus d'informations sur : www.fr.sogeti.com
Suivez nous sur Twitter : @sogeti_fr.

SOGETI