TELECOM
REVUE DE L'ASSOCIATION TELECOM PARISTECH ALUMNI

TELECOM ParisTech
ALUMNI

N°174 - OCTOBRE 2014

Notre ADN, le bon sens

CO

www.comexans.fr

CYBERSÉCURITÉ

LE PROCHAIN NUMÉRO SERA CONSACRÉ
À L'E-SANTÉ ET AUX START-UP

TÉLÉCOM n°174 - Octobre 2014
est édité par l'Association Télécom ParisTech alumni.
Dépôt légal à parution.

Directeur de la publication : Dominique Jean (1973)
Directrice de la rédaction : Agnès Maître (1983)
Secrétaire de rédaction : Amélie Pageard

Rédacteur en chef dossier Cybersécurité :
David Fayon (1993)
Rédacteur en chef dossier Mobilité :
Paul Jolivet (1995)
Comité de rédaction : Marylin Arndt (1981), Céline Beillouin (2011), Gérard Cambillau (1973), Christine Chardon (1995), Michel Cochet (1973), David Fayon (1993), Ayoub Figuigui (2011), Louis-Aimé de Fouquières (1982), Grégoire Galievsky (2000), Philippe Hilsz (1980), Paul Jolivet (1995).
Ont contribué à ce numéro :
Jean-Claude Merlin (1962)

Maquettiste : DHTL - pao@dhtl.fr
Couverture : réalisée par Valérie Mounier - www.ikkomoon.com
Illustrations : Gédéon
Banque d'image : Thinkstock

Rédaction & Abonnements :
46 rue Barrault 75634 Paris Cedex 13
Tél. 01 45 81 74 77
Courriel : revue@télécom-paristech.org
Site : www.télécom-paristech.org

Régie publicitaire : EM-COM
11, rue Chevreul - 94100 SAINT MAUR DES FOSSES
Tél. : 01 43 97 40 82
contact@em-com.fr - www.em-com.fr

Imprimé en france

Abonnements annuels 2014 : 53 € TTC
Prix au numéro : 21 € TTC
ISSN 0040-2478

TELECOM Evolution

Institut Mines-Télécom

TELECOM ParisTech

Certificat d'Études Spécialisées

ARCHITECTE D'APPLICATIONS MOBILES POUR L'ENTREPRISE

NOUVEAUTÉ 2015

- Développez et certifiez les compétences recherchées par les entreprises dans leur démarche centrée sur la mobilité
- Appréhendez les facettes techniques, sécuritaires, légales et organisationnelles dans la création d'applications mobiles
- Maîtrisez les architectures multi-plateformes orientées mobilité et l'urbanisation technique associée
- Étudiez, définissez et proposez des applications mobiles dans le respect de contraintes métier et des objectifs stratégiques de l'entreprise
- Déployez des solutions de mobilité à coût maitrisé et gérez leur mise en œuvre

Renseignements / candidature

Site web : *www.telecom-paristech.fr/ces*

Contact : *cesappmob@telecom-paristech.fr*

Télécom ParisTech - 37/39 rue Dareau 75014 - Paris

N°Vert 0800 880 915

MOBILITÉ

NOTRE RÉSEAU

CYBERSÉCURITÉ

Editorial

Par David FAYON (1993)
et Jean-Pierre DARDAYROL (1977)

David FAYON (1993), est Consultant Web dans la Silicon Valley. Auteur de plusieurs ouvrages dont *Géopolitique d'Internet*, Economica, il intervient pour des conférences notamment sur le Web 2.0 et la stratégie numérique et anime le site www.davidfayon.fr.

Jean-Pierre DARDAYROL (1977) est ingénieur général des mines au Conseil Général de l'Economie, ministère de l'économie. Ses activités porte principalement sur les ruptures que connaît le monde de l'Internet et les systèmes critiques - crises de la confiance, renouveau de la propriété intellectuelle, cloud, analytics, objets connectés, ... Il est le référent cybersécurité au CGE. Ancien directeur de l'ATICA et ancien Président de l'AFNIC, il est membre du CSPLA.

Cybersécurité, l'assurance vie de notre société numérique

Les menaces qui existaient dans le monde du système d'information se sont accrues avec la révolution Internet. Le Web 2.0 avec notamment les réseaux sociaux et la mobilité et désormais le 3.0 avec l'Internet des objets qui pointe son nez sont la source de nouvelles opportunités de services et d'usages avec entre autres la géolocalisation, la personnalisation, ... mais aussi de nouveaux risques, de nouvelles menaces. La valeur se situant désormais dans les données – avec une complexité liée à l'infobésité et son corollaire le big data – il est naturel que celles-ci soient l'objet de convoitise.

Les menaces concernent chacun de nous tant dans sa vie professionnelle que personnelle avec des frontières qui s'estompent. Chaque internaute peut de surcroît devenir complice d'une cyberattaque « à l'insu de son plein gré » avec son PC ou son smartphone. Celui-ci pouvant en effet servir de relais à un groupe criminel, un réseau terroriste en devenant un botnet pour une attaque allant au-delà des classiques spams, virus informatiques via la messagerie et les liens frauduleux.

Les risques, conjonctions des menaces et des vulnérabilités – importantes sur les smartphones et tablettes insuffisamment sécurisées s'agissant des mots de passe et de l'accès direct aux Apps – sont légions. On pourrait citer les malwares, le phishing, les possibles détournements de fonds avec les monnaies virtuelles de type bitcoin alimentant des mafias en tout genre qui défient des États avec des risques d'apparition de « small brothers » dangereuses pour les citoyens. Sur le plan international, on peut relever les cyberattaques de l'Estonie par la Russie en 2007 ou encore les vers Stuxnet en 2010 visant les systèmes iraniens et Flame en 2012 pour le cyberespionnage. Les révélations d'Edward Snowden à partir du 6 juin 2013 ont constitué l'événement déclencheur d'une prise de conscience de l'opinion publique par rapport aux risques d'écoute sur Internet et à l'intelligence économique dans la société de l'information. Toutefois, il n'existe pas, du moins officiellement, à ce jour, de cyberguerre ayant fait des morts. Qu'en serait-il par exemple si des paquets IP étaient bloqués ou modifiés à grande échelle par rapport à des centrales nucléaires, des Google cars, etc. ?

En France, le rapport du sénateur Bockel le 18 juillet 2012 a par exemple mis en exergue les écoutes potentielles sur des routeurs chinois. Le Livre blanc pour la défense et la sécurité nationale de 2013 a fait de la cybersécurité l'une des priorités nationales. La loi du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale en est la concrétisation sur le plan juridique. La question de la cybersécurité est désormais intégrée au plus haut niveau de l'État avec par exemple le renforcement des moyens de l'ANSSI.

Des solutions existent néanmoins tant techniques (chiffrement, authentification forte, etc.) qu'humaine (formation et prévention, politique de sécurité au sein des organisations) complétées par des réponses juridiques avec notamment une harmonisation du cadre européen. Et en entreprise, le rôle du RSSI est appelé à évoluer avec l'utilisation plus systématique d'un cadre méthodologique, la mise en place d'audits et le développement de l'intelligence économique.

Les sujets sont nombreux, ce numéro de la revue TELECOM nous permet de faire le point sur l'état de l'art et les perspectives en matière de cybersécurité.

Le facteur humain dans les cyberattaques touchant les messageries des entreprises

Par Ismet GERI et Laura PEYTAVIN (1990)

Cliquer sur un lien malveillant ? Qui, quand, où et pourquoi ? Les techniques de Big Data au service de l'analyse du facteur humain, maillon faible en matière de sécurité.

S'il y a un facteur déterminant en matière de protection contre les cyberattaques, c'est bien le facteur humain, considéré comme un maillon faible parce qu'il ne se résout pas par des solutions d'ordre purement techniques, et aussi parce qu'il se prête peu à des études précises et détaillées.

Le média le plus utilisé par les cyberattaquants est la messagerie et il est aujourd'hui possible pour des acteurs majeurs en cybersécurité de faire des analyses statistiques de grande valeur sur les menaces et les attaques. Encore faut-il pouvoir cartographier, analyser et corréler jusqu'aux gestes de ceux qui cliquent effectivement sur les liens malveillants dans les messages. C'est ce que peut faire la société Proofpoint grâce aux volumes importants de données obtenus lors de l'utilisation de sa solution Targeted Attack Protection™, en conditions réelles, par ses clients au travers le monde.

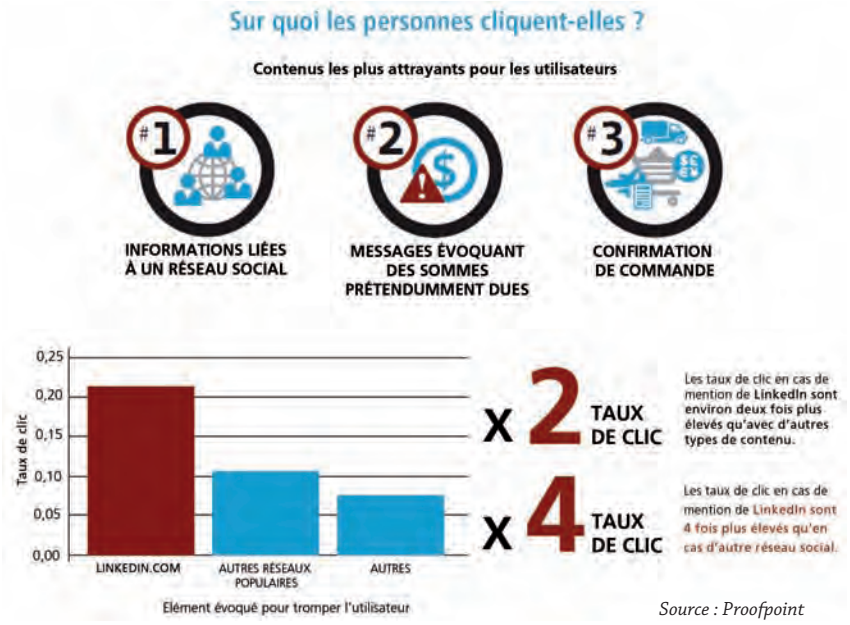
Voici ce que l'analyse nous raconte de nos comportements.

Quelles sont les personnes qui cliquent sur les URL ?

Chaque entreprise est concernée. En moyenne, 10 % des employés sont à l'origine de tous les clics pouvant occasionner des problèmes sérieux. Même les entreprises leader sont concernées : le pourcentage excède là 1 %.

Certaines entreprises investissent de réels efforts pour organiser des formations ayant pour but de sensibiliser le personnel, et pour mettre en place divers procédés de sécurité, dernier cri et traditionnels. Les sommes et efforts induits débouchent sans conteste sur du positif. Cependant comme il n'est pas possible de savoir précisément comment un utilisateur se comportera, et comme la donne change constamment, certains programmes parviendront toujours à passer entre les mailles du filet et à trouver un employé pour cliquer sur une URL. D'après les données recueillies, aucune entreprise n'est épargnée par cela.

Source : Proofpoint



Source : Proofpoint

Tout le monde fait des erreurs. Bien que les personnes cliquant de façon répétée sur des liens dangereux soient responsables de la majorité des situations, 40 % des clics sont également dus à des personnes qui auront cliqué une seule fois.

On pense généralement que, pour réduire les risques, il est surtout nécessaire de s'intéresser aux personnes qui cliqueront de manière répétée. Cela ne permet pas de remédier aux 40 % restants.

Dans la mesure où le nombre de personnes qui ne cliqueront qu'une seule fois peut varier et induire un risque non négligeable, il est donc fondamental de disposer de solutions permettant de prédire et de détecter, dès que possible, les menaces.

Tout le monde est concerné. Les employés non cadres sont ciblés deux fois plus que les cadres, et 1,3 fois plus que le personnel dirigeant. De plus, les employés non cadres sont deux fois plus enclins à cliquer sur des URL douteuses.

Les attaques de phishing perpétrées à l'encontre du personnel dirigeant sont particulièrement intéressantes pour les hackers.dans la mesure où celles-ci profitent de l'accès le plus large aux données de l'entreprise. Toutefois, dans la mesure où les hackers peuvent infiltrer les systèmes mis en place depuis n'importe quel endroit, puis ensuite se diriger où ils le souhaitent, ceux-ci préfèrent s'attaquer aux employés non cadres car ils savent ainsi qu'ils ont plus de chance que les URL soient consultées.

Les attaques sont dirigées vers tous les secteurs. Bien que les industries les plus ciblées soient celles du secteur pharmaceutique, hospitalier et des assurances, même celles présentant un intérêt plus réduit ont été victimes d'un nombre élevé d'attaques.

Généralement, on estime que le secteur financier et le secteur de la santé sont les plus touchés. Cependant, les recherches que nous avons effectuées révèlent qu'en termes de volume, les autres industries semblent également faire l'expérience d'un nombre élevé d'attaques. L'écart comparatif est minimal lorsque la taille de l'entreprise est prise en compte. En particulier, le fait que l'entreprise soit plus grande n'implique pas obligatoirement un nombre d'attaques plus élevé.

Sur quoi les personnes cliquent-elles ?

La connectivité sociale est un bon appât. Les courriers électroniques se rapportant aux réseaux sociaux, à des commandes, ou mettant les utilisateurs en garde contre des sommes d'argent prétendument dues, se révèlent particulièrement attrayants. LinkedIn décroche la palme avec 2 fois plus de clics induits lorsque celui-ci est mentionné dans de fausses invitations à se connecter.

Les utilisateurs sont généralement capables de distinguer un courrier électronique douteux d'un message légitime. Cependant, il devient de plus en plus difficile pour eux de le faire maintenant que des services populaires sont utilisés comme prétexte, comme par exemple les réseaux sociaux. C'est notamment le cas de LinkedIn, qui est fréquemment évoqué dans les courriers électroniques qui encouragent les utilisateurs à cliquer sur les URL, car celui-ci est considéré comme digne de confiance.

Quand les personnes cliquent-elles ?

La plupart des messages dangereux sont envoyés pendant les heures de travail. En outre, un utilisateur sur 15 clique sur une URL douteuse plus d'un mois après la réception du message.

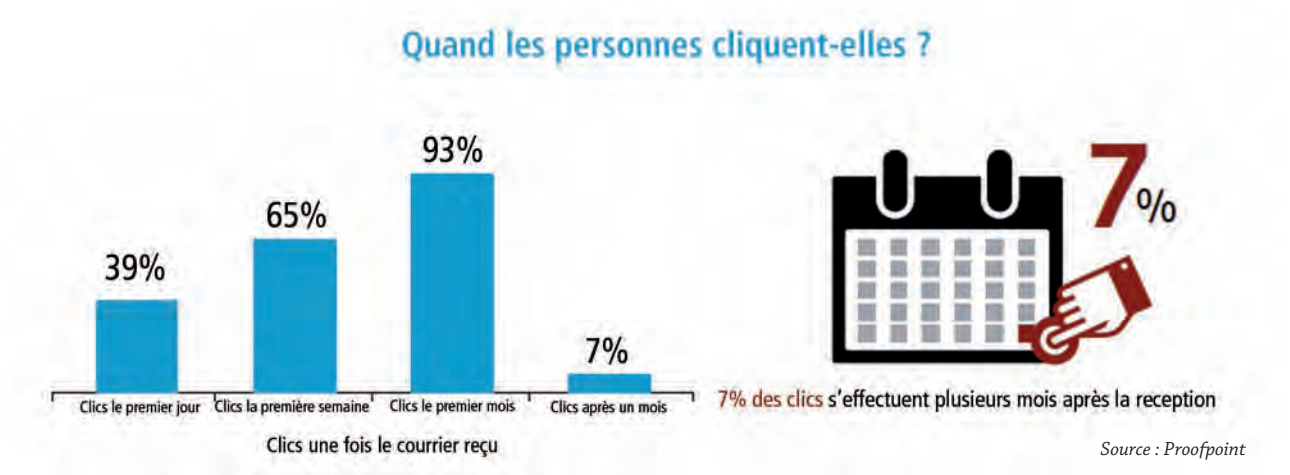
On pense généralement que les hackers effectuent leurs opérations à des moments bien précis, comme tard le soir, juste avant le week-end, voire même pendant. En effet, les utilisateurs sont alors censés être moins vigilants, ou consulteront plus probablement leurs messages alors qu'ils ne seront plus protégés par les outils de sécurité de leur entreprise. Le résultat de l'analyse démontre toutefois le contraire : les attaques sont perpétrées à tout moment pendant les heures de travail. À cela s'ajoute l'aspect latent des risques, dans la mesure où les employés peuvent encore cliquer sur les URL plus de 30 jours après réception du message concerné.

Depuis quel endroit les personnes cliquent-elles ?

Bien que la mobilité soit une notion centrale aujourd'hui, les appareils mobiles ne sont pas nécessairement concernés. 90 % des clics sur des URL dangereuses ont été effectués depuis un ordinateur (non protégé par le pare-feu de l'entreprise dans 20 % des cas). Seuls 10 % le sont sur des appareils mobiles.

D'après de récentes estimations, 65 % des courriers électroniques sont consultés d'abord sur un appareil mobile. On suppose donc que les clics se produiront en grand nombre sur ces derniers également. Mais cela ne semble toutefois pas se vérifier dans les entreprises. De plus, le risque encouru par les utilisateurs d'appareils mobiles est bien moindre en comparaison, à l'heure actuelle.

Enfin, 1 clic sur 5 se produisant sur des équipements situés hors de réseaux VPN, le casse-tête se révèle encore plus ardu.



Source : Proofpoint

Pourquoi les personnes cliquent-elles ?

Le volume de courriers électroniques a une importance pour les utilisateurs. Le fait de recevoir peu de courriers douteux est aussi dangereux que le fait d'en recevoir en grand nombre. Une fois 100 messages dangereux reçus, la probabilité de cliquer sur des URL se stabilise à un niveau de 60%.

Les équipes informatiques partent du principe que les employés reproduisent toujours certaines erreurs : les mauvaises habitudes ont la vie dure. Cependant, les données recueillies révèlent qu'il existe en réalité un lien clair entre le nombre de messages dangereux reçus par un utilisateur et le nombre d'URL qui seront effectivement consultées.

Le facteur humain face aux nouvelles menaces

Au cours des 12 derniers mois, 76 % des employés en charge de la sécurité et des opérations informatiques ont indiqué que leur entreprise avait été victime de logiciels malveillants, logiciels qui n'ont pas pu être bloqués par les solutions déjà à leur portée (entre autres, les anti-virus). Selon les données d'un autre rapport, 95 % des attaques ciblées et de type APT (« Advanced Persistent Threat) ont été perpétrées via l'envoi de courriers électroniques de phishing à des entreprises. Le nombre de ces mêmes attaques, sophistiquées et très courantes en cette ère d'ingénierie sociale, n'a de cesse d'augmenter.

Les attaques les plus avancées tirent parti aussi bien des failles humaines que des failles système. Celles-ci réussissent parce que le personnel clique sur les URL douteuses, et que les équipes en charge de la sécurité ne disposent généralement pas de suffisamment de temps pour déterminer clairement qui est ciblé, ni de quelle manière. Pour cette raison, il leur est impossible d'implémenter des procédés de protection de niveau suffisant au sein de l'entreprise. Un certain pourcentage de ces attaques seront contrecarrées grâce à des passerelles, au sandboxing[1] et à d'autres technologies. Cependant, grâce à leur précision et à leur profusion, certaines techniques modernes (comme les attaques de type « longlining[2] ») qui sont relayées par des réseaux d'objets connectés piratés « thing bots » (par exemple les frigidaires ou les télévisions) parviennent à porter leurs fruits. Être familier de tous les rouages induits par les logiciels malveillants ne suffit toutefois pas à protéger une entreprise.

En cas d'attaque de type « longlining », il est crucial de savoir qui est réellement ciblé, qui clique sur les URL et quelles sont ces dernières, et à quelle fréquence. Ce qui permet le développement de stratégies de protection particulièrement puissantes.

LES AUTEURS

Ismet GERI, est directeur Europe du sud chez Proofpoint depuis septembre 2009. Diplômé de l'Ecole Supérieur d'Ingénieurs en Génie Electrique puis Doctorant à l'Université de Rouen. Ismet a été directeur Europe du Sud chez Infoblox, et a auparavant exercé des fonctions commerciales pour Netscreen Technologies, Juniper Networks et Ascend (Lucent).

Laura PEYTAVIN (1990), est Senior Technical Support Engineer chez Proofpoint en charge du support niveau 2 sur tous les produits et solutions de sécurité sur site ou dans le cloud.
Diplômée de Télécom ParisTech en 1990, Laura a exercé plusieurs métiers en développement, avant vente et support technique pour des grands acteurs de la communication numérique (EADS, Alcatel Lucent) comme des startups américaines ou françaises innovantes (Streamezzo, Sendmail, ...)

1/ Mécanisme qui permet l'exécution de logiciel(s) avec moins de risques pour le système d'exploitation. Ces derniers sont souvent utilisés pour exécuter du code non testé ou de provenance douteuse.

2/ Ce terme de pêche industrielle (palangre en français) désigne une pratique consistant à déployer des lignes de pêche de plusieurs kilomètres de long équipées de milliers d'hameçons pour piéger le poisson. En cybersécurité, ce sont des attaques de type phishing qui se distinguent par de forts volumes globaux d'envoi de mail, mais discrets pour chaque cible attaquée, avec une personnalisation de masse du contenu par rotation rapides des IP, inclusion de divers sujets et corps de texte ainsi que des dizaines d'URL uniques – ce qui ne facilite pas leur repérage, alors que les URLs amènent à des charges utiles virales non encore identifiées.

Cybersécurité : quelles réponses juridiques ?

Par Myriam QUÉMÉNER

Le Livre blanc pour la défense et la sécurité nationale de 2013 fait de la cybersécurité l'une des priorités nationales pour la France. Le constat d'une dépendance accrue de la Nation aux systèmes d'information, ainsi qu'une vulnérabilité aigüe des appareils d'État et des entreprises[1] laissant craindre des cyberattaques majeures sur les infrastructures et les réseaux numériques, ont justifié la mise en place d'une véritable stratégie de cybersécurité. La loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale[2] en est la concrétisation sur le plan juridique.
Les dispositions normatives en faveur du renforcement de la cybersécurité réforme le cadre juridique du renseignement de la cyberdéfense[3], de la protection des sites et impose de nouvelles obligations aux Organismes d'Importance Vitales (OIV).

Cybersécurité et accès aux données[4]

Le législateur a adapté les procédures d'encadrement des pratiques de surveillance administrative au contexte numérique, en y incluant notamment la surveillance sur l'Internet et l'accès aux données de géolocalisation en temps réel[5] : Avec ces nouvelles dispositions, les services de l'État français sont désormais dotés des mêmes moyens d'actions que leurs homologues étrangers en matière de cybersécurité. Les autorités compétentes pour accéder aux données sont « *les agents individuellement désignés et dûment habilités des services relevant des ministres chargés de la Sécurité intérieure, de la Défense, de l'Économie et du Budget, chargés de missions prévues à l'article L. 241-2* » du Code de la sécurité intérieure, à savoir la recherche des « *renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous de combat et de milice privés* ».
Le fait d'inclure dans le champ d'application des formulations aussi génériques que la « *prévention de la criminalité* » ou de la « *délinquance organisée* » permettra désormais aux agents compétents d'accéder aux données dans le cadre des enquêtes relevant de la lutte contre la contrefaçon ou contre la fraude fiscale.

On relève ainsi la tendance à vouloir faire traiter en priorité les affaires relatives à la cybersécurité dans le cadre administratif plutôt que judiciaire.

Les données de connexion

Les autorisations pour récupérer les données de connexion a posteriori seront désormais données par une personnalité qualifiée, placée auprès du Premier ministre, sous le contrôle de la Commission Nationale de Contrôle des Interceptions de Sécurité (CNCIS). Les fadettes rentrent ainsi dans le droit commun plus protecteur de la loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques, alors qu'elles faisaient, jusqu'à présent, l'objet d'un dispositif spécifique dans la loi antiterroriste du 23 janvier 2006[6], qui sera caduc le 31 décembre 2015. L'accès aux données prévu par ce nouveau texte a pour particularité d'être réalisé sous le contrôle d'un juge en invoquant la sécurité nationale.

1/ M. Quéméner , J-P Pinte « Cybersécurité des acteurs économiques » : réponses stratégiques et juridiques « 2012 Ed. Hermès Lavoisier »
2/ JORF n°0294 du 19 décembre 2013 page 20570
3/ M. Quéméner » La cyberdéfense au regard du livre blanc 2013 sur la défense et la sécurité nationale, https://www.cdse.fr/la-cyberdefense-au-regard-du-livre.html
4/ articles L. 246-1 à L. 246-5du Code de la sécurité intérieure
5/ article 20 de cette loi
6/Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers

Les données de géolocalisation

Les données de surveillance en temps réel sont visées par le nouvel article L 246-3 du Code de la sécurité intérieure ; celles-ci sont recueillies « *sur sollicitation du réseau et transmis en temps réel par les opérateurs* » aux agents individuellement désignés. Le rôle de la Commission Nationale de Contrôle des Interceptions de Sécurité (CNCIS) est restreint dès lors que l'autorisation du recueil se fait uniquement par le Premier ministre sur une demande écrite et motivée des ministres de la Sécurité intérieure, de la Défense, de l'Économie et du Budget ou des personnes spécialement désignées par eux. La CNCIS est simplement informée de la décision du Premier Ministre et elle dispose d'un accès permanent au dispositif de recueil concerné pour procéder à des contrôles de sa légalité (CSI, art. L. 246-4). Elle pourrait considérer que le recueil de données a été autorisé en méconnaissance des présentes dispositions, mais son seul moyen d'action consistera à adresser une recommandation au Premier ministre tendant à ce qu'il y soit mis fin, mesure cependant non contraignante.

Le nouveau dispositif sera ainsi plus protecteur des libertés avec l'accroissement du contrôle effectué par la CNCIS et en raison de la motivation des demandes de géolocalisation par le ministre et non plus uniquement des personnes désignées et habilitées. En outre, le nouveau régime apparaît également plus adapté aux besoins opérationnels des services, car ouvert à tous les services de renseignement, et pour des motifs plus larges. La durée des autorisations de géolocalisation a été fixée à 30 jours. Notons néanmoins que la durée des autorisations en matière d'interception de sécurité, pourtant estimée plus intrusive dans la vie privée, est de quatre mois.

Cybersécurité et protection des organismes d'importance vitale (OIV)

Concernant les Opérateurs d'Importance Vitale[7] (OIV), désormais, selon l'article 22 de la loi de programmation militaire (LPM), le Premier ministre « *fixe les règles de sécurité nécessaires à la protection de [leurs] systèmes d'informations* ». L'objectif de ces dispositions est de protéger de manière particulière les systèmes pour lesquels « *l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation* » .

En conséquence, le Gouvernement peut ordonner tout type de mesure pour répondre aux crises majeures menaçant ou affectant la sécurité desdits systèmes d'information. Le fait de ne pas se conformer à ces obligations[8] est passible d'une amende de 150 000 €[9]. Il peut être exigé des opérateurs d'importance vitale, à leurs frais, qu'ils mettent en oeuvre « *des systèmes qualifiés de détection des événements susceptibles d'affecter la sécurité de leurs systèmes d'informations*[10] ».

D'autres mesures liées spécifiquement à la sécurité des systèmes, telles que la coupure d'un serveur, le routage de données vers des réseaux spécifiques, ou même la participation à des contre-attaques peuvent potentiellement être visées par cette disposition. Les OIV doivent soumettre leurs systèmes d'information à des contrôles par les services du Premier ministre destinés à vérifier leur niveau de sécurité et le respect de règles de sécurité. Ces contrôles seront diligentés par l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI[11]) ou par des prestataires de services qu'elle qualifie.

En outre, un régime spécial de la notification d'incident est créé[12] à destination des Opérateurs d'Importance Vitale (OIV) qui sont désormais tenus d'informer sans délai le Premier ministre des « *incidents affectant le fonctionnement ou la sécurité des systèmes d'information* », en pratique l'ANSSI. Un décret en Conseil d'État doit intervenir afin de préciser les conditions et limites d'application de l'ensemble de ces nouvelles dispositions. On voit apparaître en raison du renforcement de ces contraintes qui inquiètent certains secteurs économiques, notamment le secteur bancaire, une volonté de développement de l'assurance des cyber-risques[13].

Pour compléter ce système de notification, l'article 24 de la loi de programmation instaure le nouvel article L.2321-3 au Code de la défense en permettant à ce que l'ANSSI obtienne des opérateurs de communications électroniques « *l'identité, l'adresse postale et l'adresse électronique d'utilisateurs ou de détenteurs de systèmes d'information vulnérables, menacés ou attaqués, afin de les alerter sur la vulnérabilité ou la compromission de leur système* ». Désormais, l'ANSSI peut donc obtenir les coordonnées de tout abonné, hébergeur ou éditeur de site Internet, si l'agence estime que son système informatique est ou peut être sujet à des attaques. Mais la disposition ne réserve pas cette faculté qu'aux seules fins d'information des personnes concernées, l'article 24 modifie également l'article L. 34-1 du Code des postes et des communications électroniques pour donner à l'ANSSI la possibilité de se faire communiquer des données d'abonnés « *pour les besoins de la prévention des atteintes aux systèmes de traitement automatisés* ».

La stratégie française s'inscrit plus largement dans une démarche coordonnée au niveau européen dans une stratégie européenne du cyberespace. La France contribue activement à la formulation de cette stratégie qui doit permettre d'assurer une meilleure cybersécurité dans les institutions européennes et dans les Etats membres, mais aussi de faire de l'Union un des acteurs majeurs du cyberespace au niveau mondial. ▮

7/ Article R1332-3 du Code de la Défense
8/ C. défense, art. L. 1332-6-1 à L. 1332-6-4
6/ C. défense, art. L. 1332-6-6.
10/ C. défense, art. L. 1332-6-1
11/www.ssi.gouv.fr
12/ article L. 1332-6-2 du Code de la défense
13/ J-L Santoni, Loi de programmation militaire, Contribution de l'assurance des cyberrisques : Expertises, avr. 2014, p. 135 à 140).

L'AUTEUR

Myriam QUÉMÉNER, magistrat, ancien auditrice de l'IHEDN, actuellement avocat général près la Cour d'appel de Versailles est expert auprès du Conseil de l'Europe en matière de cybercriminalité.
Elle est l'auteur de nombreux ouvrages sur les problématiques liées au cyberespace, notamment « Cybercriminalité, droit pénal appliqué » (Economica), « Cybersécurité des acteurs économiques » , Hermès Lavoisier et « cybersociété, entre espoirs et risques » (Lharmattan).

Les missions de l'ANSSI

« L'ANSSI répond à une évolution des menaces et son champ d'action couvre à la fois des Réseaux de l'Etat et des réseaux privés »

Interview de Guillaume POUPARD, Directeur de l'ANSSI
Propos recueillis par David FAYON (1993)

Pourriez-vous nous présenter l'organisation actuelle de l'ANSSI qui a succédé à la DCSSI et ses missions ?
L'ANSSI (Agence nationale de la sécurité des systèmes d'information) est un service qui dépend du Premier ministre et qui a une vocation interministérielle. Elle s'inscrit historiquement dans une longue série, celle du « chiffre gouvernemental » suivie par la création du Service central de la sécurité des systèmes d'information (SCSSI) en 1986 puis de la Direction centrale de la sécurité des systèmes d'information (DCSSI) en 2001. L'ANSSI, en plus de la sécurité des systèmes d'information de l'État, possède désormais une mission de défense des systèmes d'information des administrations et des opérateurs d'importance vitale (OIV). Elle contribue également à la sécurité de la société de l'information, en participant notamment à la recherche, au développement des technologies de sécurité et à leur promotion.

L'ANSSI répond ainsi à une évolution des menaces et son champ d'action est plus vaste puisqu'il couvre à la fois des Réseaux de l'État et des réseaux privés, principalement d'OIV.

On peut distinguer quelques missions majeures :
- la connaissance et l'anticipation de la menace informatique. Il convient de bien connaître le risque pour s'en prémunir. Cela passe notamment par des laboratoires qui ont la volonté d'être à l'état de l'art technique pour comprendre les scénarios d'attaque ;
- la détection et la réaction aux attaques qui consistent notamment à déployer des sondes de détection au sein des ministères. Ces dernières permettent de détecter des comportements anormaux – par exemple des signatures d'attaque, des volumes de téléchargements anormaux à des heures inhabituelles. Cette mission de défense n'existait pas du temps de la DCSSI ;
- le soutien d'une politique industrielle pour disposer en France de solutions de sécurité de confiance. Cela nécessite de bien connaître le besoin pour y répondre (routeurs, équipements réseaux, solutions de chiffrement, smartphones sécurisés). Cela passe également par une animation et un financement de la recherche et du développement. Il s'agit notamment d'animer l'écosystème industriel pour ne pas être dépendant de solutions de sécurité qui ne seraient pas de confiance.
- la sensibilisation auprès de différents publics sur la nécessaire protection des environnements numériques en promouvant les bonnes pratiques de cybersécurité et en émettant des recommandations techniques.
- de nombreuses activités transverses de réglementation, de formation, de relations internationales, de communication.

Quel a été l'impact des révélations d'E. Snowden et de la Loi de Programmation Militaire (LPM) sur l'ANSSI, notamment en matière d'évolution de ses missions (intelligence économique) et de recrutement (passage de 350 à 500 personnes en 2015 alors même que les budgets de l'État ont peu de marge de manœuvre, ce qui montre le caractère stratégique de l'ANSSI et la prise de conscience par rapport à l'importance des données en particulier) ?
La prise de conscience remonte à 2008 avec le précédent Livre blanc de la défense et de la sécurité nationale. Celui-ci a clairement identifié la menace informatique pour l'État. C'est là qu'est née l'idée de créer une agence capable d'assurer la sécurité des systèmes d'information de l'Etat. Nous avions connu l'attaque contre l'Estonie en 2007. Le pouvoir politique français a donc bien compris qu'il s'agissait d'un sujet important. Pour cela, il a donné des moyens humains et financiers à l'ANSSI mais aussi à d'autres ministères. Entretemps, des attaques en France et à l'étranger ont confirmé l'existence de cette menace et l'importance des conséquences potentielles. Un nouveau Livre Blanc a été remis en 2013. Il a confirmé la priorité stratégique de mettre en œuvre une organisation pour répondre à cette menace au plus haut niveau et le besoin d'augmenter des ressources notamment humaines. Il en est de même chez nos partenaires étrangers.

Nous restons sur une cible de 500 personnes à l'ANSSI fin 2015. Il demeure indispensable de disposer de ces experts pour assurer convenablement les missions de l'ANSSI.

Finalement, les révélations d'E. Snowden n'auront pas été une surprise. En effet, elles n'ont fait que confirmer la réalité de la menace. Par ailleurs, depuis lors, notre mission de sensibilisation est plus facile à réaliser car nous n'avons plus besoin de convaincre de la réalité de la menace.

Autour de la cybersécurité, un dispositif global a été mis en place impliquant plusieurs ministères dont la Défense, l'Intérieur, l'Économie et les Finances, les Affaires étrangères. Tout un écosystème se développe au sein duquel l'ANSSI assure le rôle d'autorité nationale et coordonne les projets cyber en interministériel.

Le recrutement est un point clé pour l'ANSSI qui intervient à deux niveaux :

- la formation et l'enseignement de la sécurité informatique dans les établissements d'enseignement supérieur restent encore insuffisants;
- le recrutement massif de professionnels sur des postes essentiellement techniques. Nous observons l'apparition de nouveaux métiers, ce qui est passionnant pour de jeunes ingénieurs même si beaucoup ne sont pas initialement experts en cybersécurité.

La LPM constitue une actualisation du référentiel législatif. Elle vient corriger des régimes existants en introduisant pour les OIV quatre points majeurs : l'obligation de se sécuriser et de remonter à l'ANSSI les incidents, la faculté pour l'ANSSI de pouvoir demander des contrôles de sécurité si nécessaire, et la possibilité de donner des consignes en cas de crise majeure.
Cela répond au besoin de systématiser et d'être efficace en cas de crise. On développera des processus plus systématiques et opérationnels pour gérer les crises informatiques et s'y préparer. Il importe de protéger les acteurs qui sont d'une importance vitale pour la nation. Au-delà, il est important de protéger également les PME, cibles de nombreuses attaques, le monde de la recherche et plus généralement la société civile qui s'étend jusqu'au particulier.

Quelles comparaisons peut-on établir entre l'ANSSI et la NSA ?

Le choix français est de clairement séparer les missions offensives et défensives. L'ANSSI n'assure que la défense des systèmes d'information de l'État et des opérateurs d'importance vitale. La NSA a pour sa part les deux missions, l'attaque et la défense.

L'article 24 de la LPM introduit une évolution importante mais qui ne remet nullement en cause ce modèle. L'ANSSI pourra désormais contacter les victimes d'une attaque informatique identifiées grâce aux adresses IP. Jusqu'alors, on n'avait pas la possibilité d'interroger les opérateurs télécoms pour recueillir les coordonnées et alerter les victimes sur le sol national. Cela demeure beaucoup plus complexe toutefois pour l'étranger mais il est possible de coopérer et de s'échanger des signalements avec les pays partenaires.

Quelles sont les principales menaces en matière de cybersécurité pour les entreprises et de cyberdéfense pour notre pays ?

Classiquement, nous distinguons trois catégories de menaces :
La déstabilisation avec notamment le défacement de sites Internet, dont l'impact pour l'image de la structure visée n'est pas à sous-estimer. Elle se situe à la limite de la cyberpollution que l'on subit au quotidien sur Internet ;
L'espionnage informatique. Il n'y a probablement pas beaucoup de grosses entreprises qui n'aient pas déjà été victimes d'une attaque de ce type. Elles sont discrètes et visent à prendre connaissance, voire à dérober le patrimoine économique et scientifique de la structure visée ;
Le sabotage qui se produit heureusement peu pour le moment mais qui n'en est pas moins réel. On anticipe par ailleurs sa croissance. Il peut s'agir par exemple de la neutralisation, voir même de la destruction de systèmes industriels. De telles attaques sont donc par définition très visibles et donc logiquement réservées à des situations où elles ont un véritable intérêt pour l'attaquant. Nous avons des exemples qui se sont produits à l'étranger (par exemple Stuxnext, Flame), qui ont prouvé que ce type de menace pouvait perturber significativement l'industrie. En outre, les conséquences indirectes peuvent être tout aussi graves avec des effets induits difficiles à prévoir.

Enfin, quels messages souhaiteriez-vous apporter aux étudiants et anciens élèves de Télécom ParisTech ?

Objectivement, l'ANSSI propose des métiers pour des ingénieurs qui ont un goût pour la technique. Il ne faut pas avoir de complexe si on n'a pas fait de cryptographie ou reçu des enseignements en techniques algorithmiques poussées. On peut venir chez nous et apprendre la sécurité sur le tas. Les métiers sont passionnants tant en expertise technique qu'en opérationnel. Le prérequis est d'être bien « câblé » côté informatique, télécoms et mathématiques. Les offres de stage et d'emploi sont consultables sur le site Internet de l'ANSSI. ■

L'AUTEUR

Guillaume POUPARD est ancien élève de l'Ecole Polytechnique (1992). Ingénieur de l'armement en option recherche, il est titulaire d'une thèse de doctorat en cryptographie réalisée sous la direction de Jacques Stern à l'Ecole Normale Supérieure de Paris et soutenue en 2000. Il est également diplômé de l'enseignement supérieur en psychologie.
Il débute sa carrière comme expert puis chef du laboratoire de cryptographie de la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI), devenue en 2009 l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Il rejoint en 2006 le Ministère de la défense, toujours dans le domaine de la cryptographie gouvernementale puis de la cyberdéfense. En novembre 2010, il devient responsable du pôle « sécurité des systèmes d'information » au sein de la direction technique de la Direction Générale de l'Armement (DGA), responsable de l'expertise et de la politique technique dans le domaine de la cybersécurité. Le 27 mars 2014, il est nommé directeur général de l'Agence nationale de sécurité des systèmes d'information. Marié, il est père de trois enfants.

Transparence, confiance et contrôle des données par les utilisateurs : les nouveaux fondements d'un monde connecté.

Hervé Le Jouan - herve@privowny.com - www.privowny.com

Après les vagues de l'Internet et des mobiles de plus en plus intelligents, nous entrons aujourd'hui dans l'ère des objets connectés, source inépuisable de capteurs et de nouveaux services. Selon IDC, il pourrait y avoir plus de 50 milliards d'objets connectés en 2020 : en plus de nos PCs, tablettes et mobiles, notre maison et ses équipements, notre voiture, nos vêtements et d'autres objets de la vie courante seront connectés, collecteront des données en permanence, les enverront dans le Cloud, les analyseront et nous rendront de nombreux services. C'est d'abord une opportunité extraordinaire pour les citoyens d'être mieux entourés et servis, mais évidemment aussi pour les marques de mieux les comprendre, de personnaliser leurs services et de se différencier des concurrents. Tout cela dans un environnement technologique qui réunit tous les composants essentiels : le Cloud qui offre des capacités de stockage et de traitement à bas prix, des capteurs miniaturisés, des réseaux très hauts débits, des logiciels de traitement toujours plus puissants et des interfaces homme machine toujours plus efficaces et simples à la fois.

Cependant, cette révolution s'accompagne de risques majeurs : vol de données, fraude, usurpation d'identité, changements incontrôlés de comportement des objets, etc... Autant de dangers qui rendront les individus plus vulnérables, plus méfiants car se sentant tracés en permanence, et donc plus attentifs à la protection de leur vie privée et au contrôle sur toutes ces données. Les marques ont une énorme responsabilité et beaucoup à perdre si elles négligent ces aspects : réputation dégradée, procès, pouvoir accru des grands agrégateurs mondiaux qui pourront à leur tour développer une connaissance du marché d'une précision sans précédent.

Chez Privowny, nous sommes convaincus que face à ce double risque qui touche à la fois liberté personnelle et équilibre des relations avec les acteurs économiques et les Etats, les utilisateurs doivent reprendre visibilité et contrôle sur leurs données et ce qui en est fait. C'est ce que nous proposons à nos clients. L'enjeu est énorme, mais les solutions de demain sont disponibles dès aujourd'hui. Essayez-les !

ercom

CRYPTOSMART

Sécurisation forte de la voix, des données et des SMS

Fiabilité

Simplicité

Confiance
&
Indépendance

DEVENEZ PARTENAIRE

Complétez votre gamme de produits et de solutions pour protéger fortement vos clients

Proposez la mise en mobilité de systèmes d'informations sensibles

Ciblez les gouvernements et les opérateurs d'infrastructures vitales

PROTEGEZ VOS EQUIPES ET DIRIGEANTS

Fournissez une solution éprouvée aux VIP de votre entreprise pour protéger leurs conversations

Apportez une solution avec authentification forte aux opérationnels

Bénéficiez de certifications EAL5+, EAL4+ et de l'agrément Diffusion Restreinte de Cryptosmart

Nous recrutons, envoyez votre CV à l'adresse rh@ercom.fr

contact@ercom.fr www.ercom.fr 6 rue Dewoitine 78140 Vélizy-Villacoublay 01 39 46 50 50

L'Europe met en place un cadre juridique pour la cybersécurité

Par Fabrice MATTATIA[1] (1995)

L'obtention de la cybersécurité nécessite certes des outils techniques performants et des mesures organisationnelles pour les mettre en œuvre, mais elle ne peut se faire que dans un cadre juridique propice. La menace étant par nature internationale, il était logique que l'Union européenne harmonisât le droit applicable dans les Etats membres. L'Union souhaite ainsi promouvoir en amont l'utilisation d'outils et de services de confiance, qui font l'objet d'un règlement adopté en 2014. Elle a également adopté en 2013 une directive sur la lutte contre la cybercriminalité.

Le règlement sur les services de confiance

Le règlement, qui entrera en vigueur à partir de 2016, remplace et complète la directive européenne de 1999 sur la signature électronique, actuellement en vigueur. En effet, la Commission européenne a considéré que le manque de succès que l'on constate actuellement pour la signature électronique provient des différences nationales de transposition de cette directive. Le règlement crée donc des règles communes à tous les Etats membres pour l'identité numérique ainsi que pour la signature électronique des personnes physiques et (ce qui est nouveau) morales. En France, ce texte remplace la loi de 2000 sur la signature électronique, qui transposait la directive de 1999.

Qu'est-ce que l'identité numérique ?

L'identité numérique (ou électronique) est ici entendue comme un moyen de prouver sur internet sa véritable identité. Une telle démarche n'a aucune raison d'être systématique : l'internaute a parfaitement le droit de naviguer de manière anonyme ou en adoptant des pseudonymes. La preuve d'identité doit se limiter aux seuls services qui justifient cette exigence, comme par exemple l'accès à des dossiers personnels.

Concrètement, de nombreux Etats européens ont émis ces identités électroniques sous forme de certificats contenus dans les puces de cartes d'identité électroniques : Finlande, Estonie, Belgique, Espagne, Portugal, Suède, Allemagne, etc. En France, une disposition adoptée par le Parlement a été censurée en mars 2012 par le Conseil constitutionnel, qui estimait que la rédaction de l'article concernant l'identité numérique était maladroite.

Notons que les mêmes outils techniques permettent souvent de réaliser des signatures électroniques, c'est-à-dire d'apposer électroniquement son approbation sur un document.

La création d'un cadre européen d'interopérabilité

Le règlement crée les conditions selon lesquelles chaque Etat devra reconnaître et accepter les identités numériques émises par un autre Etat. Ainsi, chaque

1/ Auteur de Traitement des données personnelles, Eyrolles, 2013, et de Loi et internet, Eyrolles, 2014.

Etat pourra notifier à la Commission des systèmes d'identité numérique qui respectent les conditions suivantes :
a) Les identités numériques sont émises par cet Etat, pour son compte ou sous son contrôle ;
b) Elles servent au moins à accéder aux services d'administration électronique ;
c) L'Etat garantit l'identité du titulaire.

L'Etat garantit la disponibilité en ligne, 24/7 des éléments de vérification (comme les listes d'opposition). Il n'impose aucune spécification technique excessive pour utiliser l'identité électronique.
A partir de 2016 les Etats membres de l'Union devront reconnaître les identités électroniques émises par les autres Etats à partir du moment où elles sont inscrites sur la liste publiée par la Commission. Ils devront notamment les accepter pour leurs services d'administration électronique requérant une identité numérique avec un niveau de sécurité important.
Par ailleurs, si l'outil d'identité numérique permet de générer des signatures électroniques avec un degré suffisant de sécurité, alors cette signature électronique aura une validité juridique équivalente à celle d'une signature manuscrite, reconnue dans toute l'Union.
Il est important de souligner que ce texte ne crée aucune obligation pour un Etat de l'Union de délivrer ou de faire délivrer des identités numériques (avec ou sans outil de signature), ni de notifier à la Commission celles qu'il délivre ou fait délivrer.

On peut toutefois s'interroger sur la réalité du besoin, pour le grand public, de disposer d'une identité numérique reconnue dans un autre Etat membre. Les transactions électroniques avec notre propre administration nationale, nécessitant une identité de niveau de sécurité important ou une signature électronique, sont déjà très rares (cf. l'abandon de la signature électronique pour la télédéclaration des revenus…) ; les occasions de traiter avec une administration étrangère le sont encore plus, sauf cas particuliers (travailleurs transfrontaliers ou expatriés, par exemple).

L'identification électronique d'une personne morale

En l'état actuel du droit français et européen, seule la signature électronique d'une personne physique dispose d'une définition juridique, grâce à la directive de 1999. La notion de signature électronique d'une personne morale n'existe pas juridiquement.

Le règlement comble cette lacune. Tout d'abord, il définit l'identification d'une personne morale (entreprise, association…) de la même manière que celle d'une personne physique : l'identification doit permettre de désigner sans ambiguïté cette personne. L'utilisation de cette identité numérique des personnes morales servira par exemple à lutter contre le phishing, en garantissant l'authenticité des mails expédiés par les sociétés et des sites web auxquels l'internaute se connecte.

Afin de permettre une reconnaissance intereuropéenne de cette identité numérique des personnes morales, le texte prévoit le même mécanisme que celui prévu pour les personnes physiques : chaque Etat pourrait notifier à la Commission des systèmes d'identité numérique des personnes morales dans les mêmes conditions que pour les personnes physiques.

La signature électronique d'une personne morale

Le règlement innove également en créant la notion de signature électronique d'une personne morale, appelée « cachet électronique ». L'apposition d'un cachet électronique permet à une personne morale de garantir l'origine et l'intégrité de données. Par exemple, elle permet de lutter contre le phishing en garantissant l'identité de l'émetteur des mails, ou contre la modification frauduleuse d'un code logiciel, en garantissant l'absence de modification de ce code.

Par ailleurs, si le cachet électronique est généré avec un degré suffisant de sécurité, alors le document portant ce cachet bénéficiera d'une présomption légale d'authenticité et d'intégrité.

Les entreprises ont beaucoup à gagner à disposer d'une identité numérique qui soit à la fois reconnue au niveau juridique et valable dans toute l'Union européenne. Cette identité peut servir dans leurs échanges avec le public, comme cité plus haut, pour lutter contre le phishing ; elle peut également servir dans les échanges B2B (passation de commandes, signature de contrat, garantie d'intégrité d'un logiciel) ou B2A (dématérialisation des diverses déclarations et formalités, soumission aux marchés publics…).

La directive sur la lutte contre la cybercriminalité

Les législations des différents Etats de l'Union européenne visant à réprimer les attaques informatiques sont disparates et peu dissuasives. Alors qu'on constate une recrudescence des menaces, visant notamment les infrastructures critiques, l'Union souhaite harmoniser les sanctions pénales et mieux coordonner l'action des organismes nationaux et internationaux, comme Europol ou l'Agence européenne de la sécurité des réseaux et de l'information (ENISA). Les Etats membres ont jusqu'au 4 septembre 2015 pour transposer cette directive dans leur droit interne.

Des sanctions pénales minimales

La directive prévoit des sanctions pénales pour l'accès sans droit à un système d'information. Elle précise toutefois que les Etats doivent prévoir ces sanctions au moins « lorsque l'acte est commis en violation d'une mesure de sécurité », et « au moins lorsqu'il ne s'agit pas de cas mineurs ». Il ne devrait pas être nécessaire de transposer cette disposition en droit français, puisque l'actuel article 323-1 du Code pénal prévoit déjà la répression des accès frauduleux, et ce dans tous les cas, qu'il y ait ou pas des mesures de sécurité et que le cas soit mineur ou pas.

Cette notion de « cas mineur », en revanche, constitue une nouveauté pour le droit français. La directive précise que les Etats peuvent, s'ils le souhaitent, ne pas sanctionner des infractions jugées mineures, la définition de ces dernières étant de leur ressort. La directive suggère que puissent être considérés comme mineurs les faits qui causent des dommages ou qui génèrent des risques « peu importants ».
La directive prévoit de même de sanctionner la « perturbation grave » d'un système, ainsi que l'altération frauduleuse de données, « lorsque l'acte est

commis de manière intentionnelle et sans droit, au moins lorsqu'il ne s'agit pas de cas mineurs ». A nouveau, le code pénal français actuel réprime déjà, de manière plus large, la perturbation volontaire (article 323-2) ou involontaire (lorsqu'elle résulte d'un accès frauduleux, article 323-1) d'un système informatique, ainsi que la modification frauduleuse de données (article 323-3).

La production, la vente, ou la diffusion de programmes de piratage informatique sont également visées par la directive, ainsi que la diffusion de mots de passe ou codes d'accès. Cela nécessitera peut-être un ajustement de la rédaction de l'actuel article 323-3-1 de notre Code pénal, qui ne vise que les « programmes ou données spécialement conçus ou adaptés » pour commettre des infractions : il est difficile de soutenir qu'un mot de passe ou un code d'accès entrerait dans cette définition.

La directive exige que les peines encourues soient au moins de deux ans de prison (sauf « cas mineurs »), et de trois ans lorsque l'infraction est intentionnelle et qu'un nombre important de systèmes d'information est atteint. La peine encourue doit être d'au moins cinq ans lorsque l'infraction est commise par une organisation criminelle, ou cause un préjudice grave, ou est commise à l'encontre d'un système ou d'une infrastructure critique. Il est à noter que l'article 323-1 français actuel ne prévoit que deux ans de prison pour les accès frauduleux et trois ans pour l'altération de données qui en résulte ; les articles 323-2 et 323-3 prévoyant déjà une peine de 5 ans de prison. La participation à une organisation criminelle en vue de commettre une de ces infractions est punie des mêmes peines (article 323-4).

La directive prévoit que l'usurpation des données personnelles d'une personne, en vue de gagner la confiance d'un tiers et causant un préjudice au propriétaire légitime de l'identité, constitue une circonstance aggravante.

La responsabilité des personnes morales

La directive prévoit que les personnes morales doivent être tenues responsables des infractions commises pour leur compte par leurs dirigeants. La personne morale est également responsable si son absence de surveillance a rendu l'infraction possible par ses salariés. Cela n'exclut pas les poursuites individuelles contre les personnes physiques en cause.

En droit français, l'actuel article 323-6 du Code pénal prévoit déjà la responsabilité des personnes morales.

Le renforcement de la coopération internationale

La directive prévoit que les Etats sont compétents pour les infractions commises sur leur territoire, ou par leurs ressortissants, ou lorsque l'infraction vise un système situé sur son territoire.

Des échanges d'informations sont mis en place entre les Etats, avec des points de contacts opérationnels 24h/24 et 7 jours sur 7.

La transposition de cette directive n'impactera que peu notre droit pénal national, qui prend en compte les attaques informatiques depuis la loi Godfrain de 1988. C'est dans l'amélioration de l'efficacité de la coopération contre la cybercriminalité que réside le principal espoir d'endiguer ce fléau.

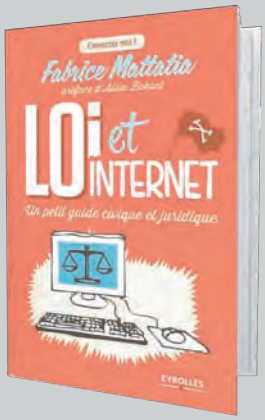
En conclusion, l'Union européenne se dote de deux outils juridiques pour lutter contre la cybercriminalité : l'un, préventif, vise à augmenter le niveau de sécurité des échanges ; l'autre, répressif, harmonise et augmente les sanctions infligées aux cybercriminels. ▮

L'AUTEUR

Fabrice MATTATIA, Polytechnicien, ingénieur Télécom ParisTech (1995) et docteur en droit, Fabrice Mattatia a été en 2009-2010 le conseiller de la secrétaire d'Etat à l'économie numérique. Il est expert en confiance numérique (identité numérique, données personnelles, droit du numérique) et a publié en 2013 chez Eyrolles Traitement des données personnelles : le guide juridique. Son nouvel ouvrage, Loi et Internet, vient de paraître chez le même éditeur.

Loi et internet *(Eyrolles, 2014, 230 pages)*

En sept chapitres consacrés à la liberté d'expression, aux données personnelles, à l'e-réputation, au droit d'auteur, aux transactions en ligne, à internet dans la vie professionnelle et à la cybercriminalité, vous découvrirez le cadre légal rendu clair et accessible, émaillé de définitions, de jurisprudences, de perspectives, d'élément à retenir, de résumés des débats en cours, de points de vue de spécialistes, ... Que vous surfiez pour votre vie privée ou pour votre travail, que vos soyez utilisateur ou responsable informatique, toutes les situations sont envisagées et illustrées d'exemples concrets.



La NSA et l'évolution des algorithmes de cryptage

Par Bernard ROUSSELY

Il y aura un avant et un après Snowden en matière de confiance numérique et un équilibre des pouvoirs entre espions, contre-espions et autorités de cyber-protection et de cyber-régulation est nécessaire pour que la croissance des activités liées au numérique se poursuive, sous peine d'une plus grande réserve des cybernautes quant à l'utilisation de services en ligne. Cependant si les quelques 1,7 millions de documents exfiltrés par Edward Snowden de SIPRnet1 révèlent l'ampleur ainsi que le caractère méthodique et systématique de l'espionnage de la NSA2 ainsi que ses tentatives d'affaiblissement des systèmes informatiques, des réseaux (par l'insertion d'implants spécifiques) et des protocoles cryptographiques, il est difficile d'être totalement surpris compte tenu du passif de cette agence en la matière.

Cet article reprend quelques épisodes, depuis le milieu des années 1970, qui montrent la constance de la NSA dans ses efforts pour assurer sa maîtrise de l'information et qui ont pour conséquence d'affaiblir la « confiance numérique » dans le cyber-espace.

Du DES à l'AES en passant par PGP

La NSA se fait connaître du public pour ses compétences en cryptographie au milieu des années 70. Le NIST[3], qui s'appelait alors le NBS, a besoin d'un algorithme de chiffrement pour protéger les informations sensibles[4] des entités fédérales. IBM est chargé de développer cet algorithme et propose Lucifer, dont les clés font 128 bits, ce qui a posteriori semble avant-gardiste pour l'époque. La NSA, en tant que conseiller technique du NBS, modifie profondément l'algorithme qui deviendra le Data Encryption Standard (DES). La taille des clés passe de 128 à 56 bits mais le changement le plus remarqué porte sur ce que l'on appelle les « boîtes »[5] de substitution dont les critères de choix ne sont pas rendus publics[6]. Dès lors, la NSA est soupçonnée d'avoir introduit une vulnérabilité dans le DES (une « backdoor ») lui permettant de retrouver facilement le clair à partir du chiffré.

En réalité, même s'il est indéniable que le DES est un algorithme aux propriétés parfois surprenantes et déroutantes, une autre théorie est possible. La NSA applique la loi de Moore et fait l'hypothèse qu'il faudra environ 10 ans pour que le DES soit largement utilisé par l'industrie. Elle détermine alors qu'une taille de clé de 56 bits est « acceptable » au regard des informations en sa possession et de son hypothèse sur le déploiement du DES. Comme un joueur d'échec, l'Agence a plusieurs coups d'avance et, au milieu des années 80, elle possède tous les outils nécessaires pour casser le DES de manière indus-

1/ Prononcer sipeurnet, un réseau classé secret du DoD américain.
2/ National Security Agency.
3/ National Institute of Standards and Technology : un organisme ayant compétence pour tous les standards fédéraux, bien au-delà du secteur de l'informatique et des télécoms.
4/ La NSA a la responsabilité des « standards » et des mesures de protection pour le domaine classifié.
5/ On parlerait plutôt de table ou de tableau en français. Ces tables servent à introduire de la « confusion » selon le terme de Shannon (cette confusion se traduit par un certain nombre de propriétés).
6/ Il faudra attendre 1994 pour que l'un des développeurs du DES, Don Coppersmith, les dévoile.

trielle. Cette capacité ne l'empêche pas de conduire d'autres actions pour faciliter son travail d'interception et l'export de produit à base de DES (ou d'autres algorithmes) est contrôlé. Les versions logicielles export du DES sont bridées avec des clés de 40 bits.

Suspicion aidant, de très nombreux chercheurs à travers le monde se lancent dans la cryptanalyse du DES et ouvrent ainsi une boîte de Pandore qui ne se refermera plus, pour le plus grand malheur des services de renseignement. En 1990, Adi Shamir, le 'S' de RSA, associé à Elie Biham « découvre »[7] la cryptanalyse différentielle avec une attaque, certes trop complexe à réaliser avec des moyens classiques de l'époque, qui affaiblit considérablement le DES. Ils sont suivis trois ans plus tard par Mitsuru Matsui qui « invente » la cryptanalyse différentielle, qui affaiblit encore plus le DES. Entretemps, des rumeurs sur la faiblesse du DES ont circulé, surtout en provenance du Royaume-Uni et du GCHQ[8], qui, comme par hasard, a une solution de remplacement pour l'industrie de défense avec (la famille) Rambutan.

Le contrôle voulu par la NSA (et le FBI) sur la cryptographie et les interceptions va prendre une mauvaise tournure avec plusieurs affaires. La première est révélée en 1988[9] par un journaliste britannique, Duncan Campbell. Il s'agit d'ECHELON, un nom de code désignant un réseau mondial d'interception mis en œuvre par ceux que l'on n'appelle pas encore les FIVE EYES et dont les agences techniques en charge du SIGINT[10] sont : la NSA pour les Etats-Unis, le GCHQ pour le Royaume-Uni, le CSE[11] pour le Canada, le DSD[12] pour l'Australie et le GCSB[13] pour la Nouvelle-Zélande[14,15].

La seconde est la tentative par la NSA et le FBI de contrôler les communications chiffrées sur le territoire américain : c'est le fiasco du Clipper Chip. L'idée de l'Agence est que chaque équipement de cryptophonie déployé sur le territoire soit équipé d'une puce, le Clipper Chip, répondant à ses spécifications, dont, entres autres, l'utilisation d'un algorithme classifié nommé SKIPJACK[16] pour le chiffrement du trafic, mais offrant la possibilité aux Agences (et surtout au FBI) d'avoir accès au trafic en clair. Cette initiative est très mal reçue par l'industrie et par les mouvements de défense des libertés individuelles, très actifs et influents aux Etats-Unis. Le Clipper Chip est mort-né mais les Agences se consolent avec le Communications Assistance for Law Enforcement Act (CALEA) qui oblige les opérateurs à leur fournir un accès aux centraux téléphoniques pour intercepter le trafic.

Sous le feu des critiques aux Etats-Unis, la NSA n'est pas la seule à devoir être blâmée pour des activités de renseignement faisant fi des droits individuels en matière de protection des données privées. Elle gagne aussi des batailles qu'elle n'a même pas à mener et, pour cela, elle peut compter sur son indéfectible alliée, sa sœur jumelle britannique : le GCHQ. Le GCHQ a des positions sur la libéralisation de la cryptographie qui sont souvent bien plus dures que celle de la NSA, sans doute parce qu'elle a beaucoup moins de moyens techniques[17]. Elle possède néanmoins des personnels très brillants souvent sortis d'Oxbridge et a compris très tôt que le recrutement ne devait plus se faire sur la base de la résolution des mots-croisés du Times, mais sur la base de très solides connaissances, en particulier dans le domaine mathématique[18]. Sa politique anti-prolifération cryptologique est bien affirmée et le GSM va lui donner l'occasion de montrer tout son talent, avec l'appui des « services » français, trop contents de l'aubaine. Le GSM a besoin d'un algorithme de chiffrement pour sécuriser les échanges entre le terminal et la station de base[19]. Ce sera l'A5 qui existera en plusieurs déclinaisons dans le temps. Le fonctionnement de l'A5 est secret et il faudra attendre la fin des années 90 pour qu'il soit rendu public après que Marc Briceno en ait fait la rétro-ingénierie en 1999[20]. La proposition initiale est que l'A5 soit utilisé avec une clé de 128 bits, ce qui au début des années 80 est toujours ambitieux mais pas nécessairement problématique en terme de performance compte tenu du temps qu'il va falloir avant d'arriver en production, fin des années 80. Cette taille de clé est purement inacceptable pour les « services » et le GCHQ, qui avance caché avec son entité appelée CESG[21], va user de toute son influence pour réduire cette taille à 54 bits, que l'on rapprochera de celle du DES. Cette valeur semble

7/ Les guillemets sur des mots comme « découvre » ou « invente » sont mis pour signaler que le terme est sans doute impropre et que la découverte ou l'invention était jusqu'alors classifiée et par conséquent pas dans le domaine public. Ça n'enlève strictement rien au travail, souvent brillant, effectué par les chercheurs qui n'avaient ni les moyens ni l'antériorité des services spécialisés.

8/ Government Communications Headquarters

9/ Sans aucun lien apparent mais la même année, Robert Tappan Morris lâche le ver qui portera son nom sur Internet. Pour l'anecdote, le père de Morris est un scientifique de la NSA.

10/ SIGnal INTelligence, renseignement d'origine électro-magnétique en français mais dont le spectre (!) est plus large chez les anglo-saxons.

11/ Communications Security Establishment.

12/ Defence Security Directorate.

13/ Government Communications Security Bureau.

14/ Certains organismes ont changé de nom depuis.

15/ La France rêvait de faire partie des FIVES EYES et elle se consolera en entrant dans les NINE EYES, un cercle d'amis plus proche que celui des FOURTEEN EYES.

16/ L'algorithme sera déclassifié en 1998 et cryptanalysé dans la foulée. A ce jour, aucune attaque ne remet en cause la force de l'algorithme dans sa version complète (80 bits de clé et 32 tours).

17/ Elle est pourtant aujourd'hui encore probablement toujours la deuxième agence de ce type par les moyens parmi celles des pays de l'OTAN, voire au niveau mondial compte tenu de sa co-gestion de certaines ressources avec la NSA.

18/ Elle réclame d'ailleurs le droit, controversé, d'invention de la cryptographie à clé publique.

19/ Chacun sait que les autres segments du réseau sont en clair, sans doute parce que les « services » avaient « anticipé » le CALEA et les lois similaires dans les pays de l'Union Européenne.

20/ L'algorithme sera alors cryptanalysé dans toutes ses versions et apparaîtra comme très faible.

21/ Communications Electronics Security Group, est une division du GCHQ comme l'Information Assurance Directorate (IAD) de la NSA. Ces services sont les homologues de l'ANSSI mais sont sous le même management que le SIGINT.

être un bon indicateur de la capacité des agences techniques à casser du code en temps réel ou quasi-réel au milieu des années 80[22]. Le GCHQ est soutenu par presque tous les services des autres états concernés par le développement du GSM, à l'exception de ceux de l'Allemagne, qui craint les interceptions des pays du pacte de Varsovie à sa frontière de l'Est. La France se montre très zélée dans cette affaire et sera active dans le « développement » de l'algorithme A5 malgré quelques turpitudes internes.

Echaudés par ces tentatives visant à faciliter les écoutes et les interceptions, des activistes décident de réagir pour « protéger les libertés individuelles » et notamment les communications privées. C'est la troisième affaire d'envergure en quelques années qui va mettre la politique de la NSA en lumière. Phil Zimmermann développe Pretty Good Privacy (PGP) et doit affronter le courroux des autorités américaines. PGP est devenu possible grâce à plusieurs facteurs et en particulier « l'invention » de la cryptographie asymétrique au milieu des années 70 par Whitfield Diffie et Martin Hellman puis sa mise en œuvre avec RSA, l'algorithme de Ronald Rivest, Adi Shamir et Leonard Adleman.

RSA est le cauchemar des Agences de sécurité car il a la fâcheuse propriété de pouvoir, selon le mode choisi, soit signer, soit chiffrer un message et fin des années 80, début des années 90, ces Agences n'ont pas nécessairement les compétences pour « casser » du RSA[23] et ses clés très longues[24]. Elles s'intéressent à la cryptographie symétrique pour d'évidentes raisons et les systèmes de distribution de clés (autre application possible de RSA) sont centralisés, hiérarchiques, archaïques pour certains (avec des bandes perforées) et n'utilisent surtout pas de cryptographie asymétrique. Zimmermann mène un long combat qui prend fin après plusieurs années difficiles pour lui. La NSA et les autres « agences à trois lettres » américaines ont perdu, PGP, même s'il existe alors des versions « US » et « internationales » prolifère. Pire encore, l'Administration Clinton prépare une directive qui va complètement libéraliser l'utilisation de la cryptographie à partir de l'année 2000.

Cette directive est devenue nécessaire pour satisfaire les besoins de l'industrie dans un monde où l'Internet prend de l'importance. La NSA a cette fois-ci l'intelligence de ne pas s'engager dans ce combat perdu d'avance. Si Bill Gates n'avait pas prévu l'explosion des services sur Internet dans son livre « Road to the future » en 1995[25], l'Agence l'a bien compris elle, avant tout le monde, et la *Toile* va devenir son nouvel Eldorado. Sans doute aidée par quelques visionnaires internes, elle tire les leçons du Clipper Chip et revoit complètement sa politique. La connaissance en matière de cryptologie est maintenant très répandue dans le monde et l'avance de l'Agence par rapport au domaine public diminue chaque année un peu plus. Elle la doit encore à son antériorité dans le domaine et à ses moyens incomparables.

Au début des années 90, Cray Research, le fabriquant de supercalculateurs a vendu environ 300 systèmes dans le monde allant de l'historique CRAY-1 jusqu'à la série YMP. Plus de 20% de ces systèmes sont installés dans des « services spéciaux »[26] et parmi ces derniers, 50% se trouvent à la NSA. Ces machines sont essentiellement dédiées à la recherche en cryptographie et à la production pour le SIGINT et les crypto-mathématiciens constituent alors la *noblesse* de la NSA. L'Agence ne refuse rien à ses experts et les ordinateurs les plus performants de l'époque[27] sont utilisés, voire conçus à la demande des ingénieurs[28]. Seulement, les temps changent et la NSA considère, au moins momentanément et partiellement, que la bataille des « codes » sous sa forme d'alors est perdue. Des algorithmes forts de chiffrement ont été publiés par des académiques et la compétition lancée par le NIST en 1997 pour remplacer le DES par ce qui sera l'AES apparaît comme « la fin de partie » pour les « casseurs de code ».

Du SIGINT revisité par TAO à l'invention du « big data »

Dès lors que le nouveau champ de bataille est identifié, par l'Internet et les réseaux qui y sont connectés, c'est à dire un sous-ensemble du cyber-espace, la NSA prend les mesures qui s'imposent. La priorité en matière de recrutement va passer des mathématiciens aux « geeks » qui formeront son armée de cyber-guerriers. Dès le milieu des années 90, l'Agence met en place un réseau au niveau national pour recruter ses nouveaux éléments. Elle noue des partenariats avec des universités prestigieuses, envoie ses cadres en stage dans l'industrie pour faire évoluer la culture de « l'entreprise NSA », du chiffre vers le cyber-espace, et entreprend sa mue technologique.

Plus tard, les documents de Snowden mettront en lumière un service particulier au sein de l'Agence : Tailored Access Operations (TAO), chargé de placer des implants dans des cibles afin d'en prendre le contrôle ou d'en intercepter le trafic, avec son « Advanced Network Technology (ANT[29]) catalogue », contenant les outils d'attaque, d'exploitation des vulnérabilités et les implants utilisés par TAO. On peut, sans grand risque de se tromper, déduire que TAO et ANT sont nés entre 1995 et 2000 et sont le résultat de la « vision » de la NSA a une époque où la plupart des administrations de la planète découvrait la bureautique et où l'industrie commençait seulement à s'intéresser à Internet.

22/ On appliquera utilement la loi de Moore aux processeurs et à la mémoire pour avoir une estimation basse de la capacité de ces mêmes services en 2014.
23/ En particulier, les services de contre-espionnage qui n'ont pour la plupart aucune capacité en matière de cryptanalyse, sont inquiets quant à la prolifération cryptographique.
24/ Cependant, RSA est aussi très lent par rapport aux algorithmes symétriques, ce qui va fortement réduire son utilisation pour le chiffrement des données. On se contentera de chiffrer des clés, ce qui permettra de les distribuer à grande échelle et de résoudre un problème vieux comme la cryptographie.
25/ Le livre sera corrigé juste avant sa parution.
26/ Selon la propre nomenclature de Cray.
27/ Il n'y a aucune raison objective pour que la situation soit différente en 2014.
28/ Le musée de la NSA permet de se faire une bonne idée des moyens de cette période avec un Cray-2 et une « connection machine » en exposition.
29/ [1] La signification exacte du sigle n'est pas confirmée et le fait qu'ANT soit une entité propre ou un simple nom de catalogue de produit n'est pas clair.

Avant d'en arriver là, la NSA doit d'abord régler un dernier problème, concernant l'AES, avec sa sœur jumelle. Le GCHQ, toujours aussi rigide sur la libéralisation de la cryptographie, prend mal la compétition lancée par le NIST pour remplacer de DES. Il craint un grand déballage, avec des avancées en cryptanalyse bien plus importantes que celles faites sur le DES. En cela, l'avenir montrera qu'il n'avait pas tort, tellement l'activité de recherche sera intense pendant la campagne sur l'AES. L'avance des services aura encore fondu à la fin de l'exercice[30]. La compétition démarre donc et une rencontre a lieu à Cheltenham, siège du GCHQ, pour tenter de trouver un terrain d'entente et limiter les dégâts à venir selon la perspective des Britanniques. La NSA est dans une situation inconfortable car elle est chargée de conseiller le NIST sur le choix du vainqueur final[31] et elle sait qu'elle sera sous les regards scrutateurs de la communauté internationale qui ne l'apprécie guère et qui n'a aucune confiance en elle. Elle a pourtant tenté de se concilier les faveurs d'académiques influents en sous-traitant des études comme celle sur IPsec faite par Bruce Schneier[32], mais elle n'y pas parvenue. Elle ne doit pas s'aliéner le GCHQ et se rend à Cheltenham en ayant préparé un stratagème pour rendre les Britanniques à la raison. Elle leur propose de soumettre BATON comme candidat à l'AES. BATON est un algorithme classifié co-développé par la NSA et le GCHQ. Il est utilisé dans de nombreux produits gouvernementaux américains et britanniques et « approuvé » par l'OTAN[33]. Il ne répond pas exactement aux spécifications du NIST mais peut subir les évolutions nécessaires. Cette proposition cause la stupeur et la colère du côté britannique. Elle est jugée totalement irrecevable et irresponsable pour de nombreuses raisons, à commencer pour des raisons opérationnelles. Le ton monte entre les participants et un Britannique va même jusqu'à qualifier son homologue de la NSA de traitre, dans une ambiance plus que tendue. Mais le stratagème a fonctionné, et, en contrepartie du « retrait » de BATON, le GCHQ laisse la NSA procéder comme elle l'entend sur l'AES.

Pour autant, il ne faut pas croire que la NSA ait renoncé à traiter les interceptions chiffrées : on ne renie pas son passé parce que le monde évolue. Si gouverner c'est prévoir, espionner l'est aussi. La NSA ne subira pas la troisième révolution industrielle imaginée par Rifkin : elle va tenter de la contrôler. Si on ne peut attaquer un chiffre parce qu'il est trop fort, alors il faut attaquer la source ou utiliser d'autres méthodes, comme affaiblir les standards ou les implémentations ou encore se procurer les clés par d'autres moyens[34]. Tous les groupes de travail où l'on traite de cryptographie vont être investis et surveillés par la NSA : IETF, IEEE, ISO pour ne citer que les plus en vue.

Les documents de Snowden permettront d'identifier le Dual Elliptic Curve Deterministic Random Bit Generator (Dual_EC_DRBG) comme ayant potentiellement été affaibli par l'Agence via des propriétés mathématiques indésirables et des analyses en cours pourraient révéler d'autres cas douteux.

TAO va implanter des cibles et le trafic, selon une vieille habitude de la maison datant de la guerre froide, sera stocké et traité dans des centres conçus pour héberger des octets en masse. La NSA passe au « big data » avant l'heure et construit des sites gigantesques dans l'Utah et au Texas.

Malgré sa toute-puissance constamment maintenue, l'Agence ne peut pas tout faire par elle-même. Elle va sous-traiter une partie des développements à l'industrie. La zone industrielle qui jouxte Fort Meade est séparée de l'Agence par le Baltimore-Washington Parkway mais les deux entités sont reliées par un pont dont l'accès est réservé au personnel de l'Agence et aux sous-traitants, les fameux « Beltway Bandits[35] » comme on les surnomme au Pentagone. Le développement d'implants passe à l'ère industrielle et un premier évènement observable en 2010 va rendre compte de la force de cyber-frappe de la NSA et de ses alliés.

Alors que les autorités américaines dénoncent quotidiennement l'espionnage chinois via Internet, Stuxnet échappe au contrôle de ses créateurs[36] et devient public quelque temps après avoir atteint son objectif : retarder le développement de la « bombe » en Iran. Les analyses de rétro-ingénierie qui s'ensuivent montre que l'opération a été conduite sur plusieurs années avec des moyens que seule une agence du type de la NSA possède. Stuxnet a été construit de manière professionnelle et il a sans doute été testé et amélioré sur une réplique des installations de Natanz, avant de pouvoir atteindre son objectif. Un deuxième évènement similaire se produit peu après, en 2012 : il s'agit de la découverte de Flame, un virus avec une forte présence en Iran et considéré comme extrêmement riche en fonctionnalité. Flame exploite notamment une vulnérabilité cryptographique d'une fonction de hachage appelée MD5 et semble porter, plus encore que Stuxnet, la signature de la NSA, car on ne voit pas qui d'autre aurait pu exploiter cette vulnérabilité[37] nécessitant une connaissance théorique et des moyens peu courants.

30/ C'est en tout cas ce qu'ils cherchent à faire croire à l'époque.

31/ Elle recommandera d'ailleurs Rijndael, développé par des anciens de l'université catholique de Louvain (la KUL, à ne pas confondre avec l'UCL de Louvain-la-Neuve, née de la scission en 1969), en Belgique.

32/ https://www.schneier.com/paper-ipsec.html, un rapport assez critique mais contenant d'intéressantes propositions.

33/ L'OTAN possède une agence d'évaluation appelée SECAN. Cette agence est entièrement financée par la NSA et se trouve dans ses locaux. Elle n'a que deux ou trois permanents et utilise des ressources de la NSA pour ses évaluations. Chargée de donner un avis sur le niveau de sécurité des équipements de chiffrement utilisés par l'Alliance, SECAN a un accès privilégié et unique à tous les équipements soumis par les Etats membres. L'OTAN « possède » une autre agence pour la gestion des clés de chiffrement : DACAN. DACAN est aussi entièrement financée par la NSA, qui a donc potentiellement accès à toutes les communications de l'OTAN, en clair.

34/ La NSA ne s'occupe que de moyens « techniques », d'autres moyens sont mis en œuvre par des agences dont c'est le métier.

35/ En référence au périphérique de Washington, autour duquel sont agglutinées ces sociétés.

36/ A priori la NSA et son homologue israélienne, l'Unité 8200.

37/ Cette action s'inscrirait dans le cadre d'un programme appelé « Olympic Games » lancé par l'Administration Bush et poursuivi par l'Administration Obama.

Avec les révélations d'Edward Snowden, la NSA est entrée dans une période trouble, plus trouble encore que celle qu'elle a pu connaître par le passé. Le cas de Snowden est sans doute révélateur d'une situation difficile à vivre pour certains employés. Les services de renseignements recrutent des personnes intègres et s'assurent de leur intégrité via des enquêtes sur leur vie privée et des passages réguliers au détecteur de mensonge, pour ce qui concerne les Etats-Unis. Il arrive donc que des personnes sélectionnées pour leur intégrité soient confrontées à des choix cornéliens dans des situations, où pour des raisons dites de « sécurité nationale », on leur demande de violer des principes qu'elles s'attachent à défendre, comme, par exemple, enfreindre la loi ou les règles du service de manière systématique. Elles peuvent alors soit être loyales envers leur service et exécuter les ordres, soit changer d'affectation ou quitter le service, soit « trahir ». Il est possible, voire probable que Snowden ait eu à faire ce choix après avoir constaté les violations multiples et répétées des droits de ses concitoyens et l'illégalité d'une partie des interceptions de la NSA (et d'autres agences).

Le général Alexander, maintenant ancien directeur de la NSA, a nié de manière constante les accusations concernant l'illégalité des interceptions. Il récemment reçu le soutien de l'amiral McConnell, directeur de la NSA de 1992 à 1996, qui a lui aussi nié toute activité illégale de l'Agence sur le territoire des Etats-Unis[38].

Malheureusement pour eux, les documents de Snowden semblent les contredire, et plutôt de manière convaincante. Pire encore, les révélations de Russell Tice[39], un autre lanceur d'alerte ayant travaillé pour la NSA pendant 20 ans, tendraient à démontrer que la NSA a espionné, pour son propre compte ou pour le pouvoir en place, nombre de personnalités politiques y compris Barack Obama, Hillary Clinton, Colin Powell ou encore le général Petraeus, un juge de la Cour Suprême, des ONG ou des entreprises.

Comble de l'ironie pour l'Agence, un prix Pulitzer, principale récompense décernée au travail de journalistes américains, a consacré le lundi 14 avril 2014, l'édition américaine du *Guardian* et du *Washington Post* sur les révélations de Snowden.

Pour conclure sur ces épisodes en partie mis à jour par Snowden, il ne faut pas se tromper sur la lecture des évènements : *fluctat nec mergitur*. Si le navire de la NSA tangue, il sait tenir la haute mer. Comme tous les services dignes de ce nom, la NSA possède au moins deux choses qui lui serviront à continuer d'occuper la place qui est la sienne, à savoir être l'Agence SIGINT la plus puissante du monde, et à poursuivre sa mission : l'excellence dans le savoir-faire, qui s'accompagne de résultats, et des dossiers. C'est en puisant dans ces derniers que l'Agence va très probablement calmer les ardeurs de ceux qui veulent restreindre ses activités par la loi. Il lui faut sans doute juste un peu de temps pour faire comprendre à ses interlocuteurs où est leur intérêt.

Les dommages collatéraux, pour reprendre le jargon militaire, sont très importants. Sur le plan opérationnel, seule la NSA peut les estimer[40], mais sur le plan de l'image de l'Agence et de la « confiance numérique » dans les produits informatiques et Internet, les dégâts sont très importants. Ses connexions avec l'industrie informatique américaine ont des répercussions dans le monde entier et il a sans doute des opportunités pour l'industrie européenne, malheureusement pas très bien armée, d'augmenter sa visibilité et ses parts de marché.

Il faut aussi mettre en perspective les agissements de la NSA avec d'autres problèmes qui sapent la confiance numérique : le premier est le faible niveau de la sécurité des systèmes d'informations qui constituent le « cyber-espace ». S'il est indéniable que la NSA fait beaucoup pour exploiter les vulnérabilités de ces systèmes, et elle est dans son rôle, sa tâche est largement facilitée par l'incurie de l'industrie comme le montrent les nombreuses failles découvertes chaque jour dans les produits et les protocoles. La saga de SSL est en cela exemplaire mais elle n'est que l'arbre qui cache la forêt. Le deuxième problème est le peu de considération en matière de protection de la part des entreprises pour les données qu'elles collectent via leur site Internet. La CNIL effectue régulièrement des rappels à l'ordre et va parfois jusqu'à prononcer des sanctions contre les plus négligentes, mais malgré un cadre réglementaire européen pourtant assez riche, la prise de conscience est lente[41].

Pour les citoyens, des questions assez basiques se posent : y-a-t-il des produits de confiance ou non-implantés par la NSA, le GCHQ, les Chinois, les Russes, les Israéliens ou d'autres pays plus discrets sur le sujet ? L'Internet est infesté de *botnets* contrôlés par des hackers mais aussi par les « services » : peut-on encore s'y risquer, ou bien, comme le pense Snowden, est-ce la fin de la vie privée ?

L'AUTEUR

Bernard ROUSSELY est ingénieur de l'armement. Il a occupé diverses fonctions techniques et de management pendant 20 ans au sein de l'Etat et d'agences internationales au sein de l'OTAN ou de l'UE, avant de fonder sa société de conseil en cybersécurité. Il se consacre maintenant au développement d'applications à base de cryptographie.
Cyberens
bernard.roussely@cyberens.com
www.cyberens.fr

38/ Le fait d'avouer les expose probablement à des poursuites judiciaires compte tenu du caractère illégal présumé de certaines activités.
39/ http://www.huffingtonpost.com/tag/russell-tice/
40/ Il y a fort à parier que de nombreuses cibles présumées de la NSA ont changé leurs habitudes de communication.
41/ Une étude réalisée en France, en Espagne, au Benelux, en Italie, au Royaume-Uni, au Japon, en Australie et aux Etats-Unis, par le cabinet Vanson Bourne montre que 20% des entreprises ne masquent ni ne protègent les données confidentielles en phase de de test.

Une solution LTE 400 MHz pour la sécurité publique en France

Face à la demande croissante des citoyens pour des applications PPDR (protection du public et secours en cas de catastrophe) plus efficaces, les gouvernements s'intéressent plus que jamais aux services de données mobiles hautes débit afin d'optimiser leurs opérations. Reste aujourd'hui la problématique de la fréquence. Airbus Defence and Space prend position pour le LTE 400 MHz en France.

Rencontre avec Nicole Lecca, Directrice Secure Land Communications au sein d'Airbus Defence and Space.

Pourquoi étendre le spectre PPDR dans la bande 400 MHz ?

En Europe, les réseaux de sécurité publique ont été mis en service sur la bande 380-400 MHz selon une stratégie et une couverture nationales. Lorsqu'il s'agit de sélectionner les technologies, la stratégie de déploiement et les modes opératoires pour les utilisateurs critiques, les gouvernements fondent leurs décisions en grande partie sur des motivations économiques. Il est donc essentiel d'intégrer, pour la mise en œuvre de futures communications, une stratégie de réutilisation des sites existants.

Par ailleurs, le groupe de travail FM49 de la CEPT (Conférence européenne des administrations des postes et télécommunications), a été mis en place en 2011 pour identifier du spectre supplémentaire pour les réseaux PPDR large bande. La bande des 400 MHz fait partie des options retenues pour accueillir des futurs réseaux PPDR large bande.

Tout converge donc vers le LTE 400 MHz. En termes de performances, on constate de meilleures caractéristiques de propagation sur la bande UHF basse (380-470 MHz) qui permettent de couvrir une zone donnée avec des cellules plus grandes et de réduire ainsi le nombre de stations de base. En combinant la bande 400 MHz avec des stations de base et des terminaux plus puissants, on obtient en bordure de cellule une capacité de transmission de données LTE suffisante en réutilisant les sites Tetra et Tetrapol déjà existants.

Des solutions concrètes

Afin de répondre aux futurs besoins opérationnels, Airbus Defence and Space et Alcatel-Lucent ont ainsi créé la solution EVERCOR, permettant l'évolution progressive des systèmes Tetra ou Tetrapol vers une solution à large bande pour les missions critiques.

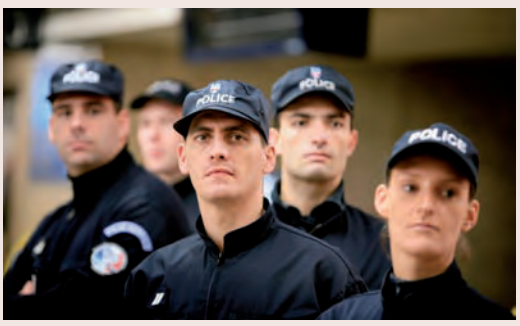
Cette évolution connaîtra plusieurs phases dont la prochaine est prévue pour répondre à la demande de services de données haut débit destinés aux organisations de sécurité publique, à l'horizon 2015. Les futures mises à jour introduiront ensuite des applications vocales critiques (push to talk) conformes aux efforts de standardisation associés.

Notre positionnement s'appuie par ailleurs sur des faits réels. Nous avons procédé avec succès à des essais terrains grâce à des réseaux pilotes LTE 400 MHz avec des clients potentiels dans plusieurs pays. Par ailleurs, nous avons livré les premières versions de notre solution LTE 400, l'an dernier, à nos principaux clients, qui souhaitaient l'intégrer à leurs systèmes Tetrapol et Tetra existants, ou encore l'utiliser pour des systèmes mobiles, notamment pour des applications militaires.

Quelle bande de fréquence pour la France ?

En France la décision finale de l'actuel Premier ministre, Manuel Valls, est attendue fin 2014. Parallèlement, le groupe de travail FM49 de la CEPT a été mis en place pour identifier un spectre supplémentaire pour les applications PPDR à large bande. L'Agence Nationale des Fréquences (ANFR) a publiquement demandé à ce groupe de travail d'étudier la bande 400 MHz pour ces applications.

Nous sommes convaincus qu'à court terme l'adaptation de la technologie LTE dans la bande 400 MHz constitue, d'un point de vue réglementaire, la solution la plus pragmatique pour la France, l'Europe et certains pays du Moyen-Orient et de la région Asie-Pacifique. Sur cette plage de fréquences, la technologie LTE offre de bonnes performances de transmission de données haut débit, optimisant ainsi les exigences de couverture du secteur de la sécurité publique. Cette approche a d'ores et déjà reçu l'aval de nombreuses organisations en Europe et dans le monde entier. De toute évidence, l'attribution de la bande 400 MHz peut être complétée par l'attribution d'une bande supplémentaire afin d'accroître la capacité totale du réseau de sécurité publique.



PwC développe son pôle cybersécurité

Mohamed Bichr et Eric, tous deux consultants chez PwC et diplômés du master spécialisé SSIR (Sécurité Systèmes Informatiques et Réseaux), nous parlent des enjeux de la cybersécurité pour leurs clients et des missions qui leur sont confiées.

Mohamed Bichr CHENGUITI-ANSARI (mohamed.bichr.chenguiti-ansari@fr.pwc.com)

Eric SEMAAN (eric.semaan@fr.pwc.com)

En quoi la cybersécurité représente-t-elle un enjeu de taille aujourd'hui pour les entreprises ?

Eric : Avec le développement d'internet, les données sont désormais accessibles à tous et exposées à un nombre croissant de menaces. De plus, beaucoup d'entreprises utilisent des données personnelles pour leurs activités (ex : Facebook), ce qui touche directement le public. Les vols de données représentent des pertes catastrophiques pour les entreprises. Dans certains secteurs sensibles comme le secteur bancaire, la législation oblige désormais les entreprises à réaliser des tests réguliers de sécurité.

Bichr : La digitalisation des outils et les nouvelles tendances d'utilisation de tablettes et téléphones personnels dans l'entreprise (BYOD) augmentent aussi l'exposition des données sur l'extérieur et donc les risques potentiels de cybersécurité.
Selon une étude du Forum Economique Mondial, les cyberattaques pourraient engendrer des pertes économiques allant jusqu'à 2 000 milliards de dollars d'ici 2020. Notre objectif est d'anticiper les menaces de cybersécurité afin de protéger les données sensibles, qu'elles soient personnelles ou intellectuelles.

En tant que consultants en cybersécurité de PwC, comment pouvez-vous aider les entreprises à faire face à ce risque ?

Bichr : Au sein de l'équipe, je travaille côté gouvernance de la cybersécurité. Je rencontre les clients, établis des diagnostics et des recommandations.
Nos compétences nous permettent d'intervenir à 3 niveaux :

- anticiper les menaces en assurant la protection des systèmes informatiques existants et en accompagnant nos clients dans la la maitrise des risques inhérents à leurs nouveaux outils
- renforcer la sécurité des outils en évaluant les risques majeurs, en protégeant le système d'attaques potentielles et en sensibilisant les personnes qui utilisent le système.
- réagir lorsqu'un incident ou une fraude a eu lieu en reconstituant le scénario pour comprendre ce qui s'est passé et ainsi protéger l'entreprise d'un nouvel incident.

Eric : Pour ma part, j'interviens plus particulièrement sur l'aspect technique des missions, qui consiste à effectuer des tests d'intrusion sur les systèmes afin d'en détecter les vulnérabilités et de les exploiter, c'est-à-dire de prouver que ces défaillances peuvent avoir des répercussions néfastes pour l'entreprises (vols d'e-mails, de mots de passe, de fichiers…).
Chez PwC, nous disposons également d'un laboratoire de sécurité avec toutes les technologies nécessaires pour effectuer des tests à distance ou faire de la R&D. Nous sommes par exemple capables de recréer une maquette de l'environnement du client afin de simuler des attaques de ses systèmes.

Qu'est-ce qui vous plait dans votre métier ?

Bichr : Nous sommes en contact direct avec les Directions Générales, ce qui est très formateur. De plus, la plupart de nos clients étant des entreprises du CAC40 présentes à l'international, nous avons l'opportunité d'intervenir sur des missions dans les pays qui n'ont pas les compétences nécessaires. Dans le réseau PwC, la France est l'une des équipes les plus avancées dans le domaine de la cybersécurité.

Eric : Nous avons aussi la chance de travailler sur des missions très diversifiées tant en termes de secteurs d'activités (banque, finance, industrie…), que de métiers (systèmes de paie, interfaces web internes ou externes…). Les missions reposent sur des actions concrètes et sont relativement courtes (entre 5 jours et 3 mois). La diversité des clients permet également de se construire un réseau important de contacts dans différentes entreprises. Ils nous font confiance, c'est très valorisant.

PwC a-t-il prévu de recruter de nouvelles personnes dans son équipe cybersécurité ?

Bichr : Les besoins des entreprises sont de plus en plus importants, notre activité devrait donc croître en conséquence ces prochaines années. L'équipe compte une vingtaine de collaborateurs aujourd'hui, pour la plupart issus de formations ingénieurs, et nous prévoyons de recruter une dizaine de personnes cette année.

Eric : L'équipe est jeune, notre environnement de travail est fun et très stimulant.
L'important dans ce métier est d'être passionné et très curieux. PwC recherche des profils polyvalents qui soient très bons techniquement mais aussi à l'aise dans la dimension relationnelle que demande le métier de consultant. Nous avons ensuite la possibilité de choisir d'évoluer plutôt côté opérationnel ou plutôt côté conseil, selon nos envies.

Cybersécurité et Industrie : deux mondes à rapprocher

Par Laurent HAUSERMANN

Le passage à un monde hyper-connecté, 100% numérique et l'arrivée de nouvelles générations nées avec de nouveaux objets connectés entre les mains, renforcent notre besoin de cybersécurité. Si les conséquences des vulnérabilités numériques en matière de vol d'information, d'espionnage ou de détournements financiers commencent à être bien connues, la prise de conscience des risques qui pèsent sur les systèmes industriels et plus généralement sur tous les automatismes qui régissent notre monde physique, est plus récente.

« 41% des cyberattaques en 2012 ciblent les entreprises de l'énergie, particulièrement le pétrole et le gaz. »

General Keith Alexander, NSA[1]

L'avènement annoncé de l'Internet des Objets, et la connexion massive des centaines de milliers d'objets connectés posent le problème de manière encore plus aigu. Ces objets seront dotés d'une capacité de collecte et de traitement des informations issues du monde physique et pourront agir sur celui-ci. Dans cette perspective, la notion de périmètre n'a plus de sens, l'ouverture est l'ADN du système, le nombre d'intervenants est très difficile à contrôler et les contraintes technologiques sont spécifiques.

Ce monde n'est pas encore notre quotidien : notre réfrigérateur n'est pas connecté à Internet, nos lunettes ou notre montre ne sont pas intelligentes et beaucoup de ces objets connectés sont encore à un stade expérimental. En revanche, il est déjà là dans les domaines industriels qui, sans forcément en avoir pris conscience, possèdent les mêmes caractéristiques : absence de périmètre, ouverture difficile à contrôler, multiplicité des intervenants et contraintes technologiques qui empêchent l'application des méthodes et outils issus de la cybersécurité des systèmes d'information. Les systèmes industriels sont confrontés à des risques nouveaux, allant jusqu'à la destruction de l'appareil de production, la pollution de l'environnement ou la perte de vies humaines.

Ces risques qui pèsent, en particulier, sur les infrastructures critiques sont considérables du fait de leur impact systémique sur nos sociétés. Ils ne sont plus cantonnés aux films hollywoodiens à gros budget mais sont pris très au sérieux par les pouvoirs publics qui se sont engagés dans des campagnes de sensibilisation très importantes et dans la mise en place de réglementations contraignantes.

1/ "Energy Pipeline: Cyber attacks hit oil, gas, just as much as retail" <http://www.greeleytribune.com/news/business/10355602-113/cyber-oil-attacks-security>

110 millions de cartes bancaires volées via un réseau industriel

Une affaire récente illustre bien l'ouverture des systèmes. Le 19 décembre 2013, les magasins Target (2ème discounter des USA, derrière Wal-Mart Stores Inc., plus de 70 Milliards de $ de chiffre d'affaires) ont annoncé avoir été victimes du vol des données de 110 millions de cartes bancaires. Les criminels disposent désormais de toutes les informations, dont la piste magnétique, pour reproduire à l'identique des cartes bancaires parfaitement valables.

Les dirigeants de Target ont confirmé que l'origine de la faille se trouvait être liée à un de leur sous-traitant. Aujourd'hui tout porte à croire qu'il s'agit de Fazio Mechanical Service, une entreprise spécialisée dans les systèmes de chauffage et de climatisation.
Il aurait disposé d'une connexion à distance sur les installations de Target, dans chaque magasin, afin de superviser le bon fonctionnement des installations de climatisation. Il s'agit pour les commerçants de réduire les coûts en limitant la dépense d'énergie durant la nuit, et donc en laissant la température augmenter, et, à l'inverse, en conservant une température idéale pour ses clients durant le jour. Il s'agit aussi de supprimer le personnel résidant dans les magasins en mutualisant les coûts de supervision, surtout en horaires décalés.`

Bien que Fazio ait nié avoir un tel contrat avec Target, l'entreprise a reconnu posséder une connexion de données avec Target et être elle aussi une victime d'une attaque informatique.

Cet exemple montre comment les multiples relations clients / fournisseurs, et la logique de services aux entreprises, entraînent une complexité architecturale des réseaux. Cette complexité augmente indubitablement l'exposition au risque cyber.

Hack my car

Une étude récente, publiée lors de la conférence BlackHat 2013 à Las Vegas, illustre ces différences d'approche technologique.
Elle a été écrite par Charlie Miller, connu pour avoir été l'un des premiers à casser les protections des smartphones Apple. Au gré des 100 pages de ce document, Miller détaille comment il a pu, avec des moyens extrêmement limités, prendre le contrôle de deux voitures différentes. En effet, les voitures modernes sont des systèmes communicants. Elles possèdent un canal de communication standard, appelé bus CAN. Il permet aux éléments actifs (direction assistée, freins, phares, etc.) de communiquer avec les éléments de contrôle et de supervision (volant, tableau de bord).

Avec quelques lignes de code, envoyant plus d'informations que d'usage ou simulant des appareils de diagnostic, il a pu :
- rendre rigide le volant, au point qu'il était impossible de le tourner à plus de 45° ;
- mettre les freins en mode diagnostic, les empêchant de fonctionner ;
- prendre le contrôle du tableau de bord, notamment du compteur de vitesse ;
- ou, plus amusant, faire clignoter toutes les lumières de la voiture !

Ces attaques sont très simples à réaliser, il lui a suffit, au choix, de :
- envoyer de façon massive des paquets CAN invalides ;
- rejouer des paquets qu'il avait capturés sur le fil, en modifiant quelques octets.

Charlie Miller est un *whitehat*. Il réalise ces études pour comprendre au mieux les risques. Il publie ses résultats pour alerter les constructeurs et les consommateurs. Mais nul doute qu'une personne, ou une organisation mal intentionnée, y trouvera une méthode efficace pour causer des accidents ou exercer un chantage.
Un autre *whitehat*, Nitesh Dhanjani, a montré que les différents systèmes numériques inclus dans les modèles Tesla étaient ouverts et perméables à une rétro conception poussée, ainsi qu'à des attaques.

Le réseau industriel, cet orphelin

Contrairement aux domaines du commerce, de la gestion et de la bureautique, où les systèmes d'information font l'objet d'une direction intégrée, les réseaux industriels ne possèdent pas de logique d'urbanisme. Ceux-ci sont, en général, conçus autour des processus qu'ils pilotent. Ils sont pensés de façon indépendante des autres systèmes qui les entourent et sont sous la responsabilité d'une direction « industrielle ».

Il n'y a pas de couple « métier/IT » comme dans une Direction Informatique où un informaticien métier représente le client alors que d'autres informaticiens fournissent les éléments d'infrastructure, réseau notamment, en s'assurant de sa cohérence et de sa sécurité. Dans le monde industriel, ces deux rôles sont confondus avec un tropisme fort sur le « métier ». Ainsi, l'informaticien industriel est-il d'abord un automaticien qui connaît très bien le processus industriel à piloter et qui sait comment programmer, maintenir et gérer les automatismes pour le faire. Par nécessité, il s'intéresse au réseau industriel mais sans en avoir la responsabilité en tant que tel. Cette situation génère du risque dans la mesure où le réseau industriel peut être partagé par plusieurs sous-systèmes dépendant de responsables différents sans que personne ne soit capable d'assurer que celui-ci est maîtrisé et ne fait pas l'objet de compromission.

Cette absence de responsabilité crée une difficulté en matière de cybersécurité. Elle complique l'interaction entre les hommes de la sécurité informatique et ceux des technologies opérationnelles, dans lequel les interlocuteurs sont des automaticiens qui n'ont pas de culture informatique et des managers de production ou de maintenance pour qui le risque cyber arrive très loin dans la liste des risques qui pèsent sur l'outil industriel.

Par où commencer ?

Les gestionnaires de systèmes industriels, d'installations de transports, ou encore les responsables d'infrastructures publiques, pour ne citer que quelques exemples, doivent se poser une

question simple : « Par où commencer ma démarche cybersécurité ? Comment obtenir des résultats rapides et atténuer les risques auxquels je fais face… »

Il faut se garder d'adopter une posture, naïve, de recherche d'un absolu visant à sécuriser le système de manière parfaite. Cette posture théorique donnerait le sentiment aux responsables qu'ils doivent s'engager dans un effort considérable pour voir apparaître les premiers bénéfices, ce qui aurait pour conséquence de les inciter à ne rien faire. Les règles qui en découlent sont souvent issues des pratiques de la sécurité des systèmes d'information, par exemple :

- l'obligation d'appliquer des correctifs de sécurité ;
- la création de politiques de sécurité détaillées, issues d'une analyse de risque ;
- une logique de «tout interdire et verrouiller» au risque d'empêcher les uns et les autres de travailler et les machines de fonctionner.

Ces approches ne sont en général pas économiquement viables à court terme. Elles demandent un investissement initial important et une expertise interne qui n'est pas disponible. Elles sont complexes, car se voulant exhaustives (tous les serveurs, tous les points d'accès, etc.), et manquent de pragmatisme.

Plus encore, les solutions de cybersécurité IT existantes nécessitent de disposer d'une expertise technique pointue pour les mettre en œuvre et les exploiter efficacement. Elles s'adressent à des informaticiens, bien formés, maîtrisant les problématiques de cybersécurité. Et même si la plupart des solutions bénéficient maintenant d'interfaces graphiques ergonomiques, il faut la plupart du temps plusieurs jours à un technicien bien formé pour les déployer.

Trois points clefs pour réussir

Il est important de mettre rapidement en place une première initiative. La question posée *(«par quoi commencer ?»)* appelle une réponse pragmatique. Trois points sont essentiels pour démarrer[2].

Le premier est d'identifier des responsabilités claires sur le réseau industriel. La démarche doit être menée par des hommes de terrain, qui connaissent la réalité des opérations de leur entreprise. Un rôle doit être clairement identifié, celui de : *Responsable des Systèmes et Réseaux Industriels*.

Le second est de connaître précisément sa situation actuelle (*« où on en est ? »*). Cela passe par la connaissance détaillée du parc d'équipements connectés à son réseau et de sa cartographie complète. Cette connaissance permettra de mettre en place très vite des règles simples qui permettront d'augmenter rapidement le niveau de protection.

Le troisième est de se préparer à répondre à une intrusion ou une activité malveillante («être prêt à se défendre»). Il passe par la centralisation des événements de sécurité et des journaux d'événements.

La cybersécurité des systèmes industriels est un sujet à prendre rapidement en considération. La protection numérique des infrastructures critiques, de l'appareil de production n'est plus une option. C'est un impératif.

Nul n'est censé ignorer la loi !

En France, l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) prend très au sérieux le risque d'attaques sur des infrastructures critiques, et sur les systèmes industriels en général. Elle a publié plusieurs guides de sensibilisation ainsi qu'un guide détaillé de recommandations au moment du Forum International de la Cybersécurité 2014 (FIC).

Ses recommandations sont issues des travaux du groupe de travail « Cybersécurité pour les systèmes industriels » qui réunit des industriels du monde de l'automation, de la cybersécurité et des utilisateurs finals. Ces recommandations distinguent les installations en 3 classes correspondant à des niveaux de sensibilité et proposent 283 recommandations.

La loi de programmation militaire (LPM) votée au parlement en décembre 2013 impose dans son article 21 aux opérateurs d'importance vitale (OIV) la mise en place de moyens organisationnels et techniques pour se protéger du risque cyber. Les décrets d'applications sont attendus pour la fin 2014.

Les entreprises soumises à ces réglementations engagent leur responsabilité pénale. Les amendes pour non-conformité peuvent s'élever jusqu'à 750 000 €.

L'AUTEUR

Laurent HAUSERMANN, est le co-fondateur de Sentryo est un éditeur de logiciels de cybersécurité et de situation awareness dédiés aux réseaux industriels et à l'Internet des objets.
Laurent est passionné de logiciels, de hacking et d'innovation. Il a passé les 15 dernières années à créer des produits de cybersécurité pour défendre les grandes et les petites entreprises. Il était dernièrement le CTO d'Arkoon où, tirant parti de l'agilité, il a dirigé une équipe de plusieurs dizaines d'ingénieurs dans des projets de R&D ambitieux.
Laurent était aussi le Chief Information Security Officer d'Arkoon où il a dirigé plusieurs programmes classifiés. Il enseigne à l'Ecole des Mines. Il est l'auteur du blog "En Route pour l'Innovation" et un inconditionnel de la philosophie Lean Startup.

2/ Un e-book détaillant cette approche est disponible sur http://www.sentryo.net. Il est complémentaire de cet article.

Cyberdéfense le ninja de la tortue

Par Eric DUPUIS

Cybersécurité, Cyberprotection, Cyberdéfense, Cyberrésilience : de nombreux concepts viennent chahuter les responsables d'entreprises en ces temps de risques informatiques et télécom grandissants. Si se construire une carapace de protection de ses biens et services sensibles est essentiel pour garantir la pérennité de son organisation, il est aussi fondamental d'être attentif, aguerri, et de savoir réagir efficacement aux attaques. La question aujourd'hui n'est plus de savoir si les organisations (entreprises, institutions, états) seront attaquées… mais plutôt quand elles le seront… et surtout comment elles se sont préparées à réagir. Je vous propose au travers de cet article une petite exploration de la cyberdéfense « dans cette guerre digitale ».

Cyberdéfense et guerre informatique : Une histoire de militaires ?

Les grands concepts de cyberdéfense sont anciens et certains puisent leurs sources dans le domaine de la guerre de l'information. Nous pouvons dater les grands débuts de la Cyberdéfense dans les années 95 avec les travaux de la RAND[1] et particulier ceux de Martin C. Libicki sur la guerre de l'information. Dans les écrits de John Arquilla en 2001 on trouve les définitions de ces actions de l'« Information Warfare » : « *Actions conduites pour obtenir la supériorité dans le domaine de l'information, en altérant l'information adverse, ses processus basés sur l'information, et ses systèmes supports, tout en protégeant nos propres informations, processus, et systèmes* ». Le traumatisme du 11 septembre 2001, fonde les nouvelles doctrines du volet « cyberwarfare », guerre de l'ombre et renseignement. Le cyberespace devient un enjeu majeur pour sécurité intérieure des Etats-Unis avec la création d'une organisation « Homeland Security ». Dès 2002, Le volet cyber prend au sein de cette organisation une importance fondamentale dans la protection cyber des infrastructures critiques : Transports, Energie, Santé … en quelques années, le monde se met au diapason « Homeland ».

En France, en 2006 le rapport du député Pierre Labordes (LAS06) donne aux politiques le premier « coup de semonce » sur la menace Cyber. En 2008, le rapport du sénateur Roger Romani « la Cyberdéfense : un nouvel enjeu de sécurité nationale » (ROM08), définit les grands axes d'organisation de cette sécurité.

En 2008, le Livre blanc sur la Défense et la Sécurité nationale apporte le nouveau volet « savoir et pouvoir se défendre » au volet classique « se protéger » dans l'espace numérique. On y trouve aussi l'exploration de « l'action et la neutralisation de l'adversaire », ce dernier volet ouvrant d'autres voies hors du champ de mon propos.

En 2009, L'ANSSI remplace la DCSSI avec des nouvelles compétences et missions, pour assurer une cybercontinuité de la nation.

Dans le rapport « cyberdéfense » de 2012, du sénateur Jean-Marie Bockel, ce concept de « cyberdéfense » devient une notion complémentaire de la « cybersécurité », qui offre un nouveau cadre d'accueil pour la protection des systèmes d'information, la lutte contre la cybercriminalité et la cyberdéfense.

2013 est certainement l'année majeure de la cyberdéfense avec d'une part la publication du livre Blanc « Défense et sécurité nationale » au mois de juin, qui place le cyber au cœur des enjeux de défense, et d'autre part le vote de la loi de programmation militaire 2014-2019 (LPM) qui donne des moyens concrets aux ambitions nationales dans ce domaine.

1/ Rand Corporation : www.rand.org

De la protection des infrastructures critiques à la cyberdéfense d'entreprise

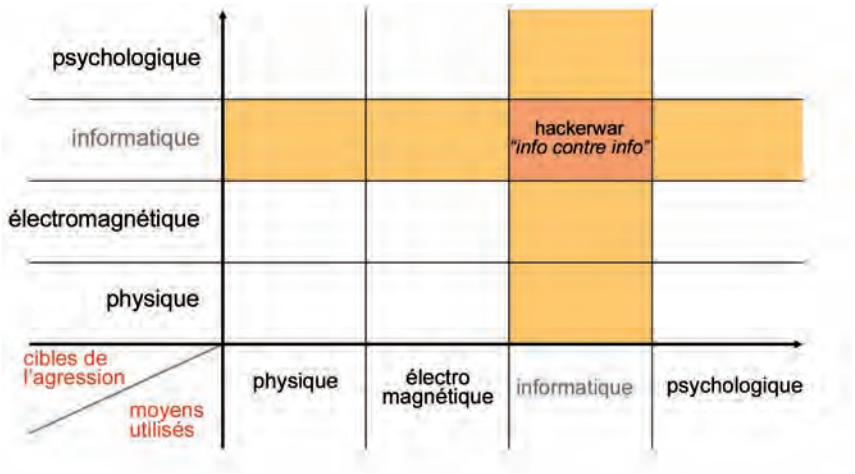
Cette LPM « impose » à plus de 200 opérateurs d'importance vitale, répartis en 12 secteurs d'activités, de mettre en place des mesures pour gérer les incidents graves « cyber ». Jusqu'ici, seule une obligation de moyens leur était demandée, maintenant il s'agira d'une obligation de résultat qui devrait s'étendre rapidement par capillarité à toutes les autres structures économiques.

Car il faut se protéger, gérer les cyberattaques, savoir réagir : l'entreprise peut se retrouver confrontée à des situations complexes, par la difficulté de comprendre les causes de la crise ou par l'obligation de fonctionner en mode dégradé lorsque son SI n'est plus pleinement opérationnel. Pourtant, elle se doit de prendre des décisions pour contenir l'incident, d'assurer la continuité de son activité, de communiquer de manière pertinente, ceci avec ses partenaires, ses clients, ses fournisseurs etc.

Il est peu envisageable d'être dans un mode « reflex » pour répondre à ce type d'incident. L'ensemble des structures de décisions doivent être impliquées dans cette réflexion pour passer d'une culture sécurité de moyens à une culture de résultats. La culture de l'entreprise doit aussi s'imprégner « des risques » inhérents à l'informatique. L'entreprise doit non seulement disposer de moyens pour se protéger mais elle doit être aussi apte de se défendre.

La notion de cyberdéfense reste toutefois peu répandue dans le monde de l'entreprise, car encore trop fortement connotée « sécurité nationale et continuité de l'état ».

L'entreprise doit pourtant aussi défendre ses intérêts dans le cyberespace en adoptant une posture de défense réactive qui nécessite connaissance et anticipation.
L'augmentation des attaques ciblées démontre en outre les limites des produits de sécurité classiques. Les attaques les plus élaborées ont recours à des manœuvres complexes techniques et non techniques.



Hackerwar vs Cyberwar avec Hackerdefense vs Cyberdefense
Source : Yves Correc dans "vers la guerre informatique" - DGA - 2001

L'entreprise a besoin d'assurer la continuité de son activité (Business Continuity[2], résilience[3]), dans un environnement économique qui se digitalise à très grande vitesse. Si cet engouement technologique apporte de nouvelles opportunités, il fait aussi émerger de nouvelles menaces, qui, de surcroit, combinent ces différents niveaux d'attaque (voir figure ci-dessus : Hackerwar vs Cyberwar).

L'entreprise doit surveiller son environnement avec ses propres « yeux » pour analyser, comprendre et devancer ce qui la menace.

« se cyberdéfendre » en entreprise

Pour la cyberdéfense d'entreprise, l'analyse systémique et dynamique l'environnement est nécessaire pour acquérir une bonne vision de son écosystème et en faciliter la veille. Si des vecteurs de menace sont clairement identifiés, des actions d'influence, de persuasion, voire de déception à l'encontre des attaquants peuvent modifier leur perception de la situation et les dissuader à agir contre les intérêts de l'entreprise. Cette approche globale impose donc la définition d'objectifs clairs et nécessite l'analyse de toutes les forces en présence.

L'entreprise évolue dans un contexte incertain, notamment dans un cyberespace qui est de plus en plus prégnant, où l'attribution des actions demeure une problématique encore non résolue. Ainsi, la meilleure maitrise de la situation, désignée par les militaires par le terme ***Cyber situational awareness*** (KAU14), implique au minimum la connaissance étendue de son environnement « digital » et la veille en temps réel de la menace. On trouve par ailleurs dans des méthodologies de cartographie de l'environnement de nombreux recoupements entre cyber-renseignement, sécurité économique et intelligence économique et stratégique.
Mon propos ne consiste pas à chercher à « militariser » l'entreprise, car celle-ci n'a pas à être lourdement armée pour se défendre, elle doit simplement disposer des méthodes, faire preuve d'organisation et posséder des méthodes pour utiliser au mieux ses moyens de protection, de les compléter si besoin, guidée par une posture à 3 piliers adaptée à ses enjeux et ses ambitions : « Veille, Alerte, et Réaction ».

Veiller donc sur son environnement cyber en surveillant :

- **son écosystème digital :** son propre système d'information, ses interactions numériques avec ses partenaires, fournisseurs et clients ;
- **sa signature « Internet » :** ses sites Web, l'usage des réseaux sociaux par l'entreprise ou ceux que pratiquent les salariés ;

2/ Continuité d'activité
3/ Reprise d'activité

- **sa vulnérabilité « digitale » :** les vulnérabilités des composants technologiques informatiques constituant les systèmes de décision, d'information, de production…

Disposer de systèmes de détection d'anomalie et d'incident avec des moyens d'alertes efficaces (SIEM[4], SOC[5] …)

- pour instrumenter la traçabilité sur toutes les couches digitales : du réseau à l'informatique décisionnaire, en passant par la téléphonie, les systèmes de productions SCADA, et déjà les objets connectés ;
- et construire des scenarii d'agrégation d'évènements capables d'identifier les effets redoutés qui pourraient impacter gravement l'activité économique.

Réagir de manière adaptée (CSIRT[6] …)

- selon des modes dégradés, être capable d'activer un PCA (Plan de continuité d'activité) ;
- pour analyser les évènements de sécurité, les traces, pour éviter les propagations éventuelles, comprendre quels sont les impacts collatéraux ;
- et gérer de manière la plus sereine la reprise d'activité, la communication de crise avec ses clients, ses partenaires, etc.

Au-delà de ces trois fonctions essentielles, on pourra aussi noter qu'en quelques années l'approche des risques informatiques a fortement évolué. Il n'est pas loin le temps où les experts cartographiaient les risques informatiques, dont les attaques font partie, en conjuguant probabilités et impacts supposés. Depuis les révélations d'Edward Snowden certains experts annoncent que la probabilité que des événements surviennent sur vos systèmes est passée à « 1 », et qu'il est simplement nécessaire d'analyser l'impact pour convaincre un responsable de prendre les mesures adaptées et de développer ses capacités de « cyber tortue ninja ».

- **Cyberprotection :** capacité à se protéger contre les rigueurs de l'hiver « Cyber », les menaces connues…
- **Cyberdéfense :** capacité à se défendre pour se sortir d'un mauvais « pas » tout en restant en alerte et en étant aguerri : voir, anticiper, réagir ;
- **Cyberrésilience :** capacité à se remettre sur pied rapidement après une agression aussi douloureuse et/ou invalidante qu'elle puisse être.

La littérature « cyberdéfense » s'enrichit chaque jour de nouveaux ouvrages explorant la cyberstratégie, la cyberpolitique et la cyberguerre, mais si vous aimez les cyber-technologies, des travaux sur l'autodéfense et la survivabilité des systèmes informatiques commencent à poindre… et ils vous donneront bien d'autres cyber-peurs.

L'AUTEUR

Eric DUPUIS dirige depuis 2011 le centre « cyberdéfense & confiance numérique » d'Orange Consulting pôle « Audit, Conseil, et Expertise » d'Orange Business Services après avoir occupé différents postes dans des sociétés de services informatiques.
Ingénieur des corps techniques de l'armement, il a exercé pendant plusieurs années à la Délégation Générale pour l'Armement dans les domaines du renseignement, de la lutte informatique et de la Cyberdéfense. Il y a en particulier développé des services d'expertises en menaces informatiques & télécom au profit de différents services du ministère de la défense.
Ingénieur du Conservatoire National des Art et Métiers, il y enseigne l'ingénierie et la sécurité des logiciels. Auditeur IHEDN de la 50ième Session Armement et Economie de Défense, il est lieutenant-colonel réserviste citoyen Cyberdéfense au titre de la Gendarmerie.

Contact : eric.dupuis@orange.com
Orange Business Services

Références

Bibliographie

- **(KAU14)** David Kaufman - Cyberdéfense d'Entreprise - Mastère Cybersécurité, Télécom Bretagne – 2014
- **(VEN11)** Daniel Ventre, - Cyberattaque et cyberdéfense – août 2011
- **(ARQ01)** John Arquilla - Networks and Netwars: The Future of Terror, Crime, and Militancy – 2001
- **(LIB95)** Martin C. Libicki - What Is Information Warfare Hardcover – Juin 1995

Urlographie

- **(BOC12)** rapport BOCKEL du n°681 du 18 juillet 2012
- **(ROM08)** Rapport d'information n° 449 (2007-2008) de M. Roger ROMANI (Sénateur), juillet 2008 (http://www.senat.fr/rap/r07-449/r07-4491.pdf)
- **(LB13)** Livre blanc défense et sécurité nationale 2013 (http://www.gouvernement.fr/sites/default/files/fichiers_joints/livre-blanc-sur-la-defense-et-la-securite-nationale_2013.pdf)
- **(LAS06)** La sécurité des systèmes d'information : un enjeu majeur pour la France (http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/064000048/0000.pdf)

3/ SIEM : Security information and event management
4/ SOC : Security Operation Center
5/ CSIRT : Computer Security Incident Response Team

CONCILIER LES BESOINS DE CONNECTIVITE AVION AUX ENJEUX DE LA CYBERSECURITE.

L'introduction de produits avioniques avancées permettant d'assurer la connectivité entre les avions et le sol en tout temps offre des opportunités substantielles aux compagnies aériennes en terme d'optimisation de leurs opérations. Cet evolution crée néammoins un besoin de sécuriser ces plateformes IT dans les airs.

Rencontre avec Jean-Marie Bégis, directeur Aircraft Information Systems, CMC Electronique Esterline.

Pourriez-vous présenter les activités 'Aircraft Information Systems' de CMC.

Les activités de CMC dans ce domaine impliquent des systèmes d'informations de type tablette durcie pour poste de pilotage (communément appelés EFB) et des serveurs de données spécialisés supportant un large éventail d'applications (documentation intégrée, calculateur de performance, outils de gestion de maintenance avion).

Quel est le positionnement de CMC et quels marchés ciblez vous ?

CMC est un pionnier dans ce domaine et offre ses produits au marché des avions d'affaires et de l`aviation commerciale. Nous avons développé une gamme de solutions pour les avionneurs et les compagnies aériennes, des tablettes de différentes tailles conçues pour faciliter une utilisation permanente en cockpit couplées avec des serveurs applicatifs et de communications.

Notre approche produit vise à combler les besoins des opérateurs en terme de systèmes ouverts, de performance (écrans tactiles, processeurs applicatifs de derniére génération) permettant une installation à faible impact dans différentes configurations d'avions et conçus pour offrir un haut niveau de fiabilité à long terme.

Quel est votre opinion sur les enjeux de Cybersecurité dans l'environnement des opérations aériennes ?

La communauté aéronautique a développé plusieurs références et réglementations dont la norme EUROCAE DO203 qui ont des points communs avec les standards en pratique au sol tout en ayant des objectifs plus spécifiques au marché :

- Garantir la sécurité informatique en vol qui est un sous-ensemble des contraintes supportant la sureté,
- Assurer le respect des règlements de navigabilité émis par les autorités (aviation civile),
- Maintenir la continuité des opérations en vol, la performance, et l'image des compagnies aériennes.

Avec l'introduction des systèmes intégrés de communications air-sol dans les avions de plus récentes générations, un certain nombre de vulnérabilités peuvent apparaitre au niveau de la sécurité des réseaux embarqués causant intentionnellement ou non des corruptions ou pertes de données pour les systèmes essentiels aux opérations et à la maintenance.

Les réseaux avioniques, de maintenance, de cabine, et ceux supportant les services aux passagers offrent différents niveaux de sécurité et partagent néammoins certaines ressources réseau. Les configurations de ces réseaux sont établies en ligne avec les résultats de l'analyse méthodique des risques de sécurité, et de vulnérabilité à ces risques. L'évaluation de ces risques compte tenu des probabilités et de l'impact de ces menaces éventuelles mènent à l'application de contre-mesures matérielles, logicielles ou à l'introduction de nouveaux processus (comme par exemple l'implémentation d'une double entrée d'information pour un calculateur de performance).

A ce jour, le traitement de ces enjeux résulte en des solutions onéreuses au niveau matériel (duplication d'équipements) et logiciel (haut niveau de certification) afin d'assurer une isolation suffisante et démontrable entre les différents domaines de communications avion.

Quels sont vos atouts technologiques dans cet environnement ?

CMC a établi une approche pragmatique dans le développement de ses produits AIS en utilisant des composantes éprouvées sur le marché industriel et en adaptant le matériel et le logiciel aux contraintes avion.

Un élément essentiel de cette approche est d'offrir des produits à la fine pointe de la technologie et de les intégrer efficacement en puisant dans les compétences de CMC en terme de certification matérielle et d'ingénierie logicielle.

A titre d'exemple, CMC offre une configuration de ses produits intégrant des commutateurs-routeurs ethernet de dernière génération. Ces derniers permettent d'isoler des réseaux via des listes de contrôle d'accés (ACLs) appliquées au niveau matériel et de traiter et de rapporter des intrusions sur des inter-connections haute vitesse (1GbaseT) en temps réel. Dans le cas de réseaux ayant des niveaux de sécurité différents, l'option d'une interconnection non-routable est également disponible.

Ces solutions visent à offrir de nouvelles solutions et adresser certains enjeux de la Cybersecurité dans notre domaine.

CMC ÉLECTRONIQUE EN BREF

Esterline CMC Électronique (CMC) conçoit et fabrique des produits électroniques de haute technologie destinés aux marchés de l'aviation. CMC concentre ses efforts à livrer des solutions novatrices d'avionique et d'intégration de systèmes de poste de pilotage à ses clients commerciaux et militaires du monde entier. Ses principales installations sont situées à Montréal, au Québec; à Ottawa, en Ontario; et à Chicago, en Illinois.

CMC est une filiale en propriété exclusive d'Esterline Corporation (NYSE : ESL, www.esterline.com).

Esterline CMC Electronics

SAGEMCOM CONÇOIT ET FABRIQUE DES TERMINAUX COMMUNICANTS À HAUTE VALEUR AJOUTÉE DANS TROIS DOMAINES

Haut-Débit

Grand Public

Energie

Sagemcom SAS - Société par Actions Simplifiée au capital de 158 291 885 Euros - 440 294 510 RCS Nanterre - Crédits photos : © smoky - Fotolia.com.jpg - © dell - Fotolia.com.jpg - © Blend Images - Fotolia.com.jpg

Sagemcom

La sécurité des objets connectés

Par David HOZÉ (2000)

Les révolutions technologiques se succèdent et ne se ressemblent pas. Une révolution en cours répond au doux nom de IoT : « Internet of Things », ou encore les « objets connectés ».

La révolution du smartphone a ouvert la voie à celle des objets connectés

C'est probablement grâce au remplacement du téléphone mobile par les smartphone que les objets qui nous entourent sont en train de se transformer en « objets intelligents et connectés ». Les énormes volumes de smartphones vendus dans le monde ont entrainé une course effrénée à la miniaturisation électronique et une généralisation de l'Internet mobile, ouvrant ainsi une voie royale à l'informatisation et au raccordement à Internet des objets qui nous entourent.

Le Cabinet McKinsey estime que le marché des objets connectés va représenter en 2025 entre 5 et 7 milliards de dollars. Les principaux domaines où sont attendus ces objets sont la santé (mesure des constantes vitales, systèmes d'alerte en cas d'accident…), le sport et le bien-être (coachs sportifs, mesure des cycles du sommeil, du taux de stress…), la domotique (réfrigérateur intelligent, TV connectée, contrôle de température…) et l'automobile. L'internet mobile quant à lui se déportera peut être de l'écran des smartphones vers les lunettes ou les montres. La liste des objets connectés est impossible à dresser, car elle s'allonge tous les jours et elle est sans fin.

L'incroyable apport de ces objets connectés pour l'utilisateur et la course contre la montre que se livrent les fabricants pour sortir leurs produits repoussent au second plan les interrogations sur les risques de sécurité présentés par ces nouveaux compagnons. L'utilisateur, fortement demandeur de nouveaux services connectés pour l'aider dans sa vie au quotidien et se divertir, a déjà accepté avec le smartphone un certain niveau de risques et souvent mis de côté ses inquiétudes concernant la gestion de ses données personnelles.

Les équipements connectés et leur surface de vulnérabilités très importante

Et pourtant, cette révolution va entrainer son lot de risques et d'incidents de sécurité, qu'il sera important, voire vital, de chercher à éviter. Les premières analyses de sécurité menées sur ces équipements montrent un très grand nombre de vulnérabilités et de comportements anormaux (mots de passe triviaux, données non chiffrées transmises en clair sur Internet, interfaces mal sécurisées systèmes d'autorisation faillibles…).

Les smartphones ont pourtant apporté leur premier lot de vulnérabilités. Tout d'abord au niveau des systèmes d'exploitation, dont la fréquence de renouvellement (rarement plus de 6 mois) offre un boulevard à la découverte et l'exploitation de vulnérabilités par les hackers. Rares sont les applications anti-virus pour mobiles qui arrivent à détecter un malware ou un cheval de Troie lorsqu'il est bien caché au sein du système d'exploitation du smartphone. Les applications ensuite, qui totalement officiellement, récupèrent l'accès aux listes de contacts, aux SMS, à la ligne téléphonique, voire aux emails de l'utilisateur. Les plates-formes hardware ensuite, qui pour des raisons de « time to market » des équipementiers présentent de nombreuses vulnérabilités.

Les objets connectés arrivent avec les mêmes types de vulnérabilités que les smart-devices, permettant potentiellement le vol d'informations, la prise de main de l'équipement à distance, ou la modification des données contenues dans l'équipement… Ils présentent par contre des scénarios de menace propres aux équipements connectés. Et ces derniers peuvent avoir de graves conséquences : détournement du système de pilotage d'une automobile, modification du dosage d'une pompe à insuline, modification d'une variable dans le carnet d'entretien d'un avion stocké dans les google glasses du technicien et utilisé lors de la maintenance d'un avion.

Même si la sécurité est un argument souvent avancé par les fabricants d'objets connectés, l'heure est pourtant essentiellement à la recherche des nouveaux usages et donc des marchés. Ainsi, Google avec son programme « Glass at Work », dont la vocation est de trouver les usages de demain pour les Google Glass dans le monde professionnel, a ouvert l'accès à ses API (interfaces informatiques) afin d'encourager les développeurs à créer les applications de demain. Ainsi, des sociétés type Aumedix, ambassadeur de Google dans le domaine de la santé, équipe déjà aujourd'hui plusieurs médecins dans des hôpitaux américains, leur permettant de consulter et de compléter les dossiers des patients en temps réel et d'afficher des informations complémentaires durant leurs opérations.

L'auteur avec des Google Glass

Objets connectés : source de risques ou source de progrès ?

Faut-il cependant tomber dans la psychose des objets connectés et refuser les extraordinaires apports qu'ils laissent présager ? Tout d'abord, peu de personnes réussiront à éviter les objets connectés. Ces derniers vont se multiplier et il y a fort à parier que d'ici quelques années, il sera difficile de trouver une voiture sortant d'une usine qui ne soit pas connectée. Qui demande aujourd'hui à son médecin de ne pas taper sa prescription sur son ordinateur et de privilégier l'ordonnance papier, par peur du piratage de l'ordinateur du médecin ?

Ensuite, la plupart des objets connectés proposeront des services dont les enjeux pour les pirates seront de faible intérêt, et qui ne présenteront pas de risques majeurs. Pourquoi un pirate s'attaquerait-il à un réfrigérateur connecté ou bien à une visite interactive d'un musée sur des Google glass, alors qu'il risque une peine de prison de 5 ans et des centaines de milliers d'euros d'amende ?

Les enjeux sécurité des objets connectés sont donc à lier aux usages qui vont en être faits. Il est bien sûr effrayant qu'un pirate puisse prendre la main sur un système de micro-chirurgie pendant une opération, mais dans le même temps, les objets connectés vont permettre de sauver de nombreuses vies, par exemple avec la généralisation de systèmes d'alerte en cas d'AVC pour les personnes à risques. Il n'y a donc pas d'inquiétude générale à développer face à cette révolution, mais bien des inquiétudes ciblées, en fonction des usages qui en seront faits et des risques induits.

Quant à la principale préoccupation des usagers (85% des français sont préoccupés par le détournement de leurs données personnelles – Etude CSA Février 2014), celle-ci bénéficie en France du travail de la CNIL qui définit et fait appliquer le cadre réglementaire concernant la protection des données.

Reste à l'usager à faire attention aux éventuelles demandes d'accès à ses données personnelles qui lui sont présentées par les éditeurs lorsqu'il accède à certaines applications ou certains équipements. Que pourrait faire la CNIL face à des utilisateurs qui, sans s'en rendre compte, auraient lors de l'installation de l'application autorisé une société à collecter et à partager leurs données de santé, par exemple avec des compagnies d'assurance, qui pourraient ainsi augmenter leur prime, refuser un remboursement ou refuser d'assurer un prêt ? Dans certains cas, si l'utilisateur refuse le partage de ses données personnelles, il est alors empêché d'accéder au service.

L'utilisateur et l'entreprise doivent apprivoiser intelligement les objets connectés

C'est donc bien une utilisation responsable et avertie, ainsi qu'un cadre réglementaire fortement contrôlé et applicable par tous les fournisseurs de services où qu'ils soient dans le monde, qui permettra aux utilisateurs d'être protégés des risques associés aux objets connectés. L'utilisateur doit également penser à se protéger. Par exemple, une application pour smartphone permettant le contrôle de ses stores électriques ne nécessite pas de connaitre son nom ni son adresse postale. Question de bon sens !
En parallèle de l'accélération des cycles technologiques, et de l'explosion de la quantité des données, les équipes de sécurité informatique en entreprise voient l'arrivée des objets connectés comme autant de de nouveaux fronts à adresser pour assurer la protection des Assets de l'entreprise. L'utilisation des objets connectés pour optimiser les processus métiers de l'entreprise la rendra certes plus agile et plus concurrentielle, mais s'il n'est pas accompagné d'une bonne démarche de sécurité, il pourrait également entrainer sa perte. Expertise sécurité et bon sens seront les maîtres mots de cette protection qui devra permettre à l'entreprise de gagner en agilité tout en maîtrisant ses risques sécurité.

L'AUTEUR

David HOZÉ (2000), a démarré sa carrière dans les Cabinets de Conseil technologiques généralistes. Il crée en 2010 le Cabinet de Conseil WISE PARTNERS, spécialisé en sécurité de l'information et en confiance numérique, avec pour ambition de rendre la sécurité plus agile et plus efficace, au service de l'entreprise innovante. Il accompagne depuis plus de quinze ans les grandes entreprises et les administrations dans leurs démarches de gestion du risque informationnel, de sécurité informatique et de confiance numérique.
Contact : david.hoze@wise-partners.fr

Cybercriminalité

Evolution des menaces à l'aube de 2020

Par Jean-Paul PINTE

Le succès et l'avènement d'Internet depuis plusieurs années s'expliquent par son degré d'ouverture et sa capacité à interconnecter des réseaux existants bien qu'ils aient des spécificités conceptuelles différentes.

Pourtant nul n'aurait pu imaginer qu'un tel réseau puisse être inventé à l'époque sans penser à sa sécurité tant il était magique et nous ouvrait de nouvelles fenêtres vers une société de la connaissance sans frontières. Aujourd'hui, cependant, il faut avouer qu'Internet est devenu un terrain où le risque criminel a pris de l'ampleur.

En effet, la cybercriminalité se conjugue maintenant à tous les domaines et impacte toute notre société. Une prise de conscience du phénomène semble se dessiner car il en va en effet de notre propre identité et sécurité jusqu'à notre défense nationale si nous n'y prenons pas garde. Focus sur les principales menaces présentes et à venir.

La cybercriminalité est le terme employé pour désigner l'ensemble des infractions pénales qui sont commises via les réseaux informatiques, notamment, sur le réseau Internet.

Ce terme désigne à la fois

Les atteintes aux biens : fraude à la carte bleue sur Internet ire ; vente par petites annonces ou aux enchères d'objets volés ou contrefaits ; encaissement d'un paiement sans livraison de la marchandise ou autres escroqueries en tout genre ; piratage d'ordinateur ; gravure pour soi ou pour autrui de musiques, films ou logiciels.

Les atteintes aux personnes : diffusion d'images pédophiles, de méthodes pour se suicider, de recettes d'explosifs ou d'injures à caractère racial ; diffusion auprès des enfants de photographies à caractère pornographique ou violent ; atteinte à la vie privée.

Si cette définition demeure encore valable à ce jour, il faut noter qu'elle a, avec l'évolution d'Internet beaucoup évolué avec de nouveaux concepts qui sont apparus comme le Cloud Computing, le BYOD (Bring Your Own Device), et depuis quelques temps les objets connectés par exemple. De la notion de cybercriminalité nous sommes passés à celle plus large de cybersécurité. Aujourd'hui il n'est donc plus surprenant d'entendre parler de cyber-harcèlement, de cyber-arnaque, cyber-contrefaçon, cyber-défense, cyber-infiltration, cyber-société, cyber-surveillance, cyber-terrorisme, ... jusqu'à celles de Cyber-guerre et de Cyber-paix évoquées lors du dernier Forum International de la Cybersécurité à Lille en janvier 2014 (www.forum-fic.com/2014/fr/).

Ceci pourrait nous arriver un jour

Tous les secteurs de l'entreprise comme chaque citoyen et chaque État seront amenés un jour à être cyber-attaqués. De cela nous pouvons en être certains même si aucune statistique fiable en France ne peut nous en faire la preuve officielle à ce jour.
Seules les quelques évaluations fournies par des organismes de sécurité informatique ou des extrapolations à partir de cas faisant la une de l'actualité nous permettent aujourd'hui d'en mesurer l'ampleur.

Nous ne sommes qu'aux balbutiements des possibilités de la cybercriminalité car chaque évolution des technologies apporte avec elle un flot de possibilités pour les personnes mal intentionnées. On dit même que ces dernières ont toujours un pas d'avance. Les réseaux sociaux, les smartphones, les objets connectés et la production par les individus et les entreprises de données massives aujourd'hui qualifiées de « mégadonnées » (big data). La quantité de données atteint en effet aujourd'hui 4,4 milliards de milliards de gigabits et double tous les deux ans.

Les menaces à venir

Voici quelques années, l'objectif des hackers était encore de démontrer qu'ils pouvaient réussir à s'introduire dans les systèmes informatiques ou dans les ordinateurs. Aujourd'hui il en est autrement car la cybercriminalité fait vivre les hackers et leur tâche a même parfois été facilitée par le jeu de l'ingénierie sociale qui consiste à user de la faiblesse psychologique, de l'indiscrétion, voire encore de la méconnaissance par les internautes du réseau Internet pour en retirer des signaux d'alerte ou de renseignement bien utiles dans les attaques menées sur la toile. Alex Türk parle même dans son ouvrage « *La vie privée en péril : des citoyens sous contrôle* » (Odile Jacob, 2011) de déchets info-actifs !

Les fraudes bancaires

Ce type de fraude est une des plus anciennes. La France y afficherait le plus haut taux de fraude à la carte bancaire en Europe, indique une étude de l'éditeur de logiciels financiers Fico. Une entreprise sur 6 affirme avoir été victime d'au moins une tentative de fraude en 2013 selon une étude interne au secteur bancaire. Les grandes PME restent la cible privilégiée des hackers.
Trois types de fraude font la une :

- Les fraudes aux virements internationaux (escroquerie dite « à la nigériane »)
- L'« escroquerie au président » ou arnaque « au faux patron » où les escrocs exigent des virements des responsables d'une entreprise, en se faisant passer pour leur PDG.
- Enfin la dernière ruse à la mode est celle qui profite de la norme Sepa, l'espace de paiement unique européen. Les escrocs se font alors passer pour le responsable informatique de la banque qui gère les comptes de l'entreprise ciblée.

Les aides humanitaires avec les dons ainsi que les catastrophes naturelles et maladies comme l'Ebola profitent aussi à ce que l'on appelle les brouteurs qui saisissent l'occasion pour vendre en ligne des remèdes miracles et réceptionner des dons. De même, début août 2014, des retraits d'argent opérés aux États-Unis et en Russie ont mis à jour un acte de cybercriminalité visant les pompes à carburant 24 h/24 de l'Intermarché Montrichard à Pont-à-Mousson.

Piratage du Cloud

Nous ne savons plus où stocker nos données et la mise en nuage de notre information (Infonuagique) devient une des seules solutions pour tous les internautes que nous sommes de protéger et de sauvegarder ces données. Tout paraît simple et pratique jusque-là mais si le Cloud, comme nous avons plus coutume de l'appeler, ne respectait pas nos données personnelles[1] comme celles d'une entreprise, imaginez le scénario !
Début septembre 2014, des centaines de photos privées et dénudées de stars américaines ont ainsi circulé sur le web. Que ce soit Jennifer Lawrence, Avril Lavigne, Mary Elizabeth Winstead, Mary Kate Olsen, Rihanna, Scarlet Johansson, Selena Gomez, ou encore Hillary Duff, leurs photos nues auraient été récupérées depuis leur compte iCloud. Le hackeur qui a posté les photos sur 4Chan s'est en tout cas vanté d'avoir récupéré toutes les photos de stars via leur compte iCloud. Même si rien n'est prouvé à l'heure où j'écris cet article et que ce problème proviendrait d'une attaque par force brute exploitant une vulnérabilité dans la fonction "Localiser mon iPhone", le simple fait de penser que j'utilise Dropbox me laisse entrevoir d'autres possibilités de fuites dans le Cloud…

Open data et Big Data menacent nos données

Ce sont deux concepts qu'il faudra surveiller dans les prochaines années en termes de cybercriminalité car Ils vont ouvrir les portes aux "mégadonnées". Ces dernières, même si l'on annonce qu'une forte sécurité sera mise en place pour leur non divulgation et leur protection demeurent des terrains d'investigation pour les hackers.
L'idée du concept d'Open Data de favoriser une politique d'ouverture et de partage des données publiques auprès des citoyens, est en vogue dans les pays développés.
« Open data » (données ouvertes), cette masse d'informations rendues publiques par les gouvernements et les entreprises viserait à renforcer la transparence. Mais pour Evelyne Ruppert, sociologue britannique « la transparence absolue est un leurre[2] », car les gouvernements choisissent toujours ce qu'ils communiquent, et ne partagent jamais les informations les plus importantes. C'est une des premières craintes sans aller jusqu'à penser aux fuites d'informations qui ne manqueront pas d'arriver. Un groupe de hackers chinois a ainsi subtilisé 4,5 millions de données médicales au Community Health Centre (CHS), le deuxième réseau hospitalier américain[3].

Trois quarts des 2000 milliards de gigaoctets de données numériques ont été créées par les consommateurs. Mises en réseaux et exploitées par des ordinateurs ces mégadonnées sont la

1/ http://www.lenetexpert.fr/et-si-le-cloud-ne-respectait-pas-vos-donnees-personnelles/
2/ http://www.henriverdier.com/2014/08/lopen-data-est-il-soluble-dans-la-big.html
3/ http://www.atlantico.fr/decryptage/que-chinois-ont-en-tete-en-cherchant-voler-millions-dossiers-medicaux-occidentaux-jean-paul-pinte-1716586.html

promesse de services nouveaux pour soit disant améliorer notre vie dans tous les domaines (Circulation, enseignement, santé, ...).
Il y a fort à parier aussi que Le Big Data transformera les modèles économiques sur Internet. Se présentant comme une collecte et une exploitation de grands volumes de données aussi appelée analyse prédictive, le Big Data verra se développer des technologies qui touchent déjà les acteurs du commerce électronique, les entreprises et notre économie réelle. La recherche scientifique, la finance et la santé seront impactés inévitablement.
Par exemple, prédire la propagation du virus Ebola grâce aux données collectées par les opérateurs mobiles en Afrique, a déjà été rendu possible, d'après l'ONG Flowminder.
L'anonymisation de toutes ces données devrait occuper une place de choix dans la sécurité des Data center les protégeant.

Le vol de données va devenir un sport international

Le vol de données personnelles est en phase de devenir de plus en plus commun car de plus en plus de données transitent via le Web et ses applications. Pas besoin d'être un grand spécialiste pour s'attaquer à la fouille de données afin de faire chanter, voire demander une rançon en échange de la non-diffusion massive de ces données sur la toile par exemple. Comme les mots de passe demeurent dans l'ensemble assez simples, la possibilité pour ces hackers qui ont du temps de prendre la main sur des comptes bancaires, des réseaux sociaux comme Facebook, et autres applications devient alors une aubaine pour les cybercriminels.

Ainsi des cybercriminels russes avaient détourné 1,2 milliard de noms et mots de passe à partir de 420 000 sites. À ce niveau, cela touche tout le monde, estime la firme de sécurité Hold Security qui a découvert ce groupe de pirates qu'il désigne sous le nom de CyberVor.
Autre exemple, le parquet de Shanghai a signalé une forte augmentation des vols de renseignements personnels en ligne, avec des délinquants qui volent et vendent ces données à diverses fins criminelles, allant de la fraude aux télécommunications au racket.

Bitcoin : une (crypto) monnaie pas aussi virtuelle et numérique que cela

Cette monnaie virtuelle d'Internet créée en 2009 s'inscrit tout doucement dans les esprits et les premiers distributeurs ont vu le jour dans des pays comme le Canada qui le considère maintenant comme une véritable monnaie. Certains ont aussi été installés récemment à Paris
La Banque de France estime que le mode de fonctionnement du bitcoin « alimente la spéculation ». La valeur du bitcoin n'est garantie par aucune autorité monétaire et peut donc représenter un « risque financier certain ». Créé par une communauté d'internautes (les mineurs »), le bitcoin[4] est contrôlé par un algorithme. L'origine même de cette monnaie consiste à se passer « d'autorité monétaire » et donc... de banque centrale !
Appréciée des geeks, on peut acheter des Bitcoins via son smartphone en se créant un compte, la machine délivre des papiers avec des flash codes en échange de bons vieux euros/dollars.
Les risques existent et ne manqueront pas de se présenter dans le temps car 100 000 bitcoins sont échangés chaque jour. Certains pirates ont déjà, par exemple, mis en vente 5 500 clés privées pour 200 bitcoins[5]. Les cellules de lutte contre le blanchiment et le financement du terrorisme peuvent sont déjà sur le pont.

La géolocalisation, la traçabilité des objets connectés et nos smartphones

Nous sommes tous devenus traçables et géo-localisables avec les technologies des puces à haute fréquence (RFID) et surtout par nos smartphones. Traçabilité des clients dans un magasin, connaissance des parcours de footing d'un coureur à pied, prise de contrôle de votre caméra, ...). Les smartphones pourraient à la longue devenir notre deuxième cerveau tant ils sont aujourd'hui associés à nos vies réelles devenues numériques.
Avez vous pensé à protéger vos webcams, imprimante, votre porte de garage, voire encore votre voiture ? Tous ces objets de la vie courante peuvent aujourd'hui être pris en main et contrôlés par des hackers, voire par de simples personnes mal intentionnées. Comme beaucoup, vous n'avez pas mis de mot de passe et j'ai pu accéder à votre adresse IP sur Shodanhq.com, un moteur de recherche qui répertorie les objets connectés dans le monde. Ils ont donc été le témoin de votre vie intime, à votre insu[6].

Ruben Santamara était sans conteste la plus attendue des conférences Black Hat consacrées à la sécurité informatique, qui se sont tenues à Las Vegas. Ce consultant en sécurité informatique y a démontré jeudi 7 août qu'il était possible de pirater certains équipements de communications par satellite utilisés dans les avions. Pour l'instant on se limiterait plus à des perturbations plutôt qu'à une prise de contrôle selon d'autres experts mais les constructeurs sont avertis, le hacking aérien est dans le tuyau.
Les Objets connectés et leurs failles de sécurité ont donc de quoi nous inquiéter signale l'étude HP faite sur 10 objets connectés et décrite sur le blog de Daniel Jacopini[7] .

Drones virtuels au service de la lutte contre la cybercriminalité et des contrefaçons.

La cyber-contrefaçon fait aussi partie des formes de cybercriminalité depuis déjà plusieurs années (médicaments, pièces automobiles, ...). Des sociétés comme Webdrone sont une belle illustration de développements spécifiques pour contrer ce risque.
La jeune start-up bourguignonne Webdrone vient de développer une nouvelle technologie pour parcourir le web à la recherche d'activités cybercriminelles, en particulier sur les réseaux de vente de contrefaçons, les réseaux de ventes parallèles, ou la fuite d'informa-

4/ https://bitcoins.org.fr
5/ http://www.nextinpact.com/news/89284-synolocker-pirates-mettent-en-vente-5-500-cles-privees-pour-200-bitcoins.htm
6/ http://rue89.nouvelobs.com/2014/06/09/jai-pris-les-commandes-camera-ai-retrouves-252793
7/ http://www.lenetexpert.fr/les-objets-connectes-et-leurs-failles-de-securite-ont-de-quoi-nous-inquieter/

tions stratégiques : les drones virtuels. À l'instar des drones civils ou militaires, les drones virtuels de Webdrone sont paramétrés pour réaliser des missions de détection et de surveillance automatique dans des zones du Web particulièrement propices au développement de la cybercriminalité. Les informations ainsi recueillies sont ensuite analysées par des experts pour isoler et extraire celles pouvant être produites lors des actions contre les sites ou les entités en infraction.

Cyberbullying ou cyberharcèlement

On connaissait déjà le cyber-harcèlement de personnes sur la toile, pratique d'intimidation par Internet, les menaces au chantage pour obtenir une somme d'argent. Nous passons à une dimension supérieure. On parle de plus en plus aujourd'hui de « cyberbullying » lorsque le harcèlement se produit par mél ou à travers des « blogs » sur lesquels les agresseurs peuvent notamment diffuser des images truquées montrant la victime dans des situations embarrassantes ou dégradantes.
Une victime des pirates informatiques guidée en ligne pour payer la rançon[8], ceci n'est plus de la fiction et c'est ce qui est arrivé à l'informaticien Robert Hyppolite a dû payer une rançon en bitcoins aux pirates de SynoLocker qui lui ont offert une assistance en ligne.
Kaspersky Lab a même découvert un ransomware de chiffrement utilisant le réseau Tor - un type de programme malveillant qui chiffre les données d'un utilisateur puis réclame une rançon pour en déverrouiller l'accès.

Usurpation d'identité et désinformation sur Internet

Si l'essence de notre vie sociale a toujours été basée sur la confiance nous signale Gérald Bronner dans La démocratie des crédules (Puf. 2013), il faudra désormais compter sans elle à l'ère du Web. Tout peut se savoir aujourd'hui sur Internet et il suffit parfois de trois informations retrouvées sur Internet pour se recréer vite fait une identité visant à nuire à un tiers, une entreprise ou encore un État.
Les réseaux sociaux personnels comme professionnels sont devenus un terrain fertile pour qui voudrait s'attaquer à l'identité numérique d'une personne voire à sa réputation.

Le premier ministre de la Russie Dmitri Medvedev, que l'on sait être un utilisateur très assidu des réseaux sociaux, s'est ainsi vu faire pirater jeudi matin son compte Twitter officiel @MedvedevRussia sur lequel il écrit en langue russe, suivi par plus de 2,5 millions d'internautes. Le but était d'annoncer sa démission.
Nous sommes tous appelés à savoir surveiller notre ADN numérique !

La cybercriminalité est un marché d'avenir

Éviter un « Pearl Harbour numérique », comme le surnomment les Américains, figure parmi les grandes priorités des États. Dans un article du Figaro[9] on signale même que la lutte contre la cybercriminalité est un marché d'avenir. Personne n'est en effet à l'abri d'attaques massives qui pourraient mettre un pays à terre en quelques heures en le plongeant dans le noir, en mettant hors d'usage ses réseaux de télécommunications, de transport et d'énergie... En France, la prise de conscience de cette menace s'est traduite par la sélection de quatre programmes de cybersécurité dans le cadre des 34 projets d'avenirs. Une réserve citoyenne cyberdéfense[10] a aussi été mise en place.

Parler de cyber-guerre voici encore quelques années était une chose presque inimaginable. Les trois virus Stuxnet (2010), Duqu (2011) et Flame (2012) ont ouvert le bal des cyberattaques notamment en Iran. Flame serait aujourd'hui la troisième arme informatique la plus sophistiquée capable à elle seule de collecter des données, d'intervenir à distance sur les réglages d'un ordinateur, d'activer le micro d'un PC et d'enregistrer une conversation, de faire des captures d'écran et de se connecter à des messageries instantanées. La cyberguerre pourrait donc se faire sans char ni avion et pouvoir attaquer sans être repéré signale cet article[11]. Le niveau de sophistication des attaques et l'étendue des dégâts ne cessent d'augmenter. Les grandes organisations se rendent compte que les phénomènes de cyber-attaque, de cyberespionnage et de terrorisme économique ne peuvent plus être ignorés.

Les seuls derniers exemples de cyberattaques des Iraniens contre Israël lors de l'opération à Gaza et l'attaque informatique DRAGONFLY contre les fournisseurs d'énergie en sont un cuisant exemple. Ces pirates ont la possibilité de saboter la distribution d'énergie de certains pays.

L'AUTEUR

Jean-Paul PINTE est Maître de conférences à l'Université Catholique de Lille et spécialiste de la cybercriminalité. Conférencier, il intervient sur les problématiques de fouille de données et d'identité numérique. Il est l'auteur de nombreux articles et de plusieurs ouvrages sur ces sujets. Lieutenant-colonel de Gendarmerie (RC) il intervient aussi à l'INHESJ et est membre du comité scientifique du Forum International sur la Cybersécurité depuis sa création.
Il est enfin l'auteur du blog : http://cybercriminalite.wordpress.Com

8/ http://www.tdg.ch/high-tech/hard-software/pirates-informatiques-guident-victimes-ligne/story/19256356
9/ http://www.lefigaro.fr/secteur/high-tech/2014/08/06/01007-20140806ARTFIG00271-la-lutte-contre-la-cybercriminalite-est-un-marche-d-avenir.php
10/ http://www.defense.gouv.fr/actualites/dossiers/la-cyberdefense/dossiers/bilan-cyberdefense-de-l-annee-2013/le-reseau-de-la-reserve-citoyenne-cyber-defense
11/http://tsahal.fr/2012/01/31/cyber-guerre-sans-char-ni-avion-attaquer-sans-etre-repere/

De la cybersécurité au Cloud de Confiance

Comment développer votre activité en confiance grâce au Cloud ?

Par Thierry FLAJOLIET (1984)

Comment profiter du Cloud sans augmenter ses risques ? Comment superviser de bout en bout la sécurité des SI de l'entreprise virtualisée ? En tant que dirigeant, pour la sécurité de son organisation comme pour sa propre protection juridique, il est devenu vital de prendre en compte les risques que font peser les services Cloud mal maîtrisés, et la responsabilité qui découle de l'arsenal très évolutif des réglementations sur les données personnelles et d'entreprise.

Avec la révolution numérique de l'échange, les entreprises veulent faire levier sur le digital pour **se développer, développer les ventes, améliorer leur efficacité opérationnelle, motiver les équipes avec des outils modernes et connectés 24X7.**

Ce levier dépend de la confiance qu'elles ont dans le numérique, avec leur approche systématique de la gestion de la Gouvernance, du Risque, de la conformité (GRC). De ce fait, les organisations veulent aussi se protéger du cyberrisque qui explose. En effet, le cybercrime prélève chaque année directement ou indirectement sur l'économie mondiale entre **300 et 1000 milliards de dollars, précisément 445 d'après le Center for Strategic and International Studies** (CSIS) [1]. D'après le World Economic Forum (Davos, janvier 2014) [2], les tendances sont alarmantes : en l'absence de plan d'action cyber spécifique, la croissance par le numérique d'ici 2020, estimée entre 9600 et 21600 milliards de dollars, pourrait bien être amputée de 3000 milliards de dollars. D'où l'importance croissante de la **cybersécurité**, avec son volet de **lutte contre la cybercriminalité** et son volet **cyberdéfense.**

Dans cet environnement ouvert, à nous de faire comprendre que **la cybersécurité facilite et accélère en réalité le développement économique,** alors qu'elle est encore souvent vue comme une contrainte, un coût superflu… En même temps, les entreprises doivent maintenant relever le défi de la **sécurité de bout en bout**, serveurs, stockage, réseaux, end-points **qu'ils soient en dur ou virtualisés, internes ou chez des prestataires cloud** - *Cloud Service Providers*, ou CSP-. Et comment faire pour tirer tous les bénéfices de ce Cloud ? Les nouveaux risques sont-ils bien compris ? Mesurés ? Anticipés ? C'est à ce prix que le Cloud donnera toute la mesure de son potentiel transformationnel, et sera massivement adopté dans de nouveaux secteurs comme la finance.

Il ressort des études et des échanges que j'ai pu avoir dans le cadre d'associations d'usagers, DSI, RSSI (CLUSIF, CESIN, CIGREF…) que le Cloud semble intensifier 10 risques principaux qui sont au moins autant organisationnels, juridiques, humains, que techniques, chaque domaine pouvant faire l'objet d'un livre blanc complet ! La première moitié réunit des risques plutôt techniques, et la deuxième des risques plutôt organisationnels, humains, juridiques.

(1) Center for Strategic and International Studies (CSIS) et McAfee, juin 2014, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

(2) Rapport "Risk and Responsibility in a Hyperconnected World", 20 janvier 2014, World Economic Forum en collaboration avec McKinsey & Company, http://www.weforum.org/news/increased-cyber-security-can-save-global-economy-trillions

	risque	exemple	D	I	C	T
1	API pas assez sécurisées	peut mettre à mal tout le provisionnement, le management, l'orchestration et la supervision des services clouds qui en dépendent totalement	X	X	X	x
2	Déni de service	peut avoir un impact simultané sur plusieurs clients, avec arrêt pur et simple de leur activité économique	X			
3	Vol ou Modification/Destruction de données	une attaque par une application vulnérable sur une BDD du cloud multi tenant mal conçue peut conduire à compromettre / perdre ses propres données, et celle de ses "voisins"	x	X	x	X
4	Kidnapping de comptes et de services	la prise de contrôle de services communs peut permettre de faire levier sur l'ensemble des ressources du CSP	X	X	X	x
5	Prise de contrôle du CSP	l'abus du CSP par des tiers malveillants peut avoir un impact mondial, sur une grande région ou un pays entier, sur des milliers d'entreprise simultanément.	X	X	X	x
6	Attaques de l'intérieur	le CSP sous-traitant de rang 1 a une multitude d'intervenants de rang supérieur, la chaine de service complexe peut multiplier les dégâts des malversations et du social engineering	X	X	X	X
7	Due diligence et audits/ contrôles insuffisants	devant les questions contractuelles et de responsabilité de plus en plus complexes, le client peut avoir tendance à baisser en compétences, en exigence, en vigilance	X	X	X	X
8	Dépendance de technologies de virtualisation quasi monopolistiques	le client peut devenir dépendant d'un fournisseur leader du cloud - exemple VMWare pour la virtualisation -, mettant en péril coûts, support, souveraineté	X	X	X	X
9	Conformité à l'ensemble des lois/ règlements en vigueur dans les zones/ pays ou opère l'entreprise	le client et ses dirigeants peuvent facilement être attaqués au civil comme au pénal, car dans la plupart des législations, dont l'Europe, c'est le client qui est responsable du traitement effectué par ses CSP, car il contrôle la finalité et les moyens (G29), pour les données personnelles comme pour celles de l'entreprise.				
10	Conformité à la réglementation européenne...un sujet en soi	le client et ses dirigeants peuvent facilement être attaqués au civil comme au pénal, notamment avec le durcissement des directives et réglements européens sur la protection des réseaux et de l'information (directive NIS/ SRI), futur réglement sur les données personnelles.				

DICT : Disponibilité, Intégrité, Confidentialité, Traçabilité

Au-delà du contrôle de la localisation des données, un sujet en lui-même déjà complexe, il y a toute une série d'obligations qui incombent de ce fait au client : par exemple, il doit être en mesure de faire de nombreuses déclarations à ses propres clients, parties prenantes, autorités de sécurité dont il peut dépendre, concernant des compromissions de données personnelles ou d'entreprise, ou encore des attaques sur certains SI critiques pour les OIV (Organismes d'Intérêt Vital pour la nation).

La question du décideur : « *Quel est mon risque légal si mon CSP est attaqué ou fait des bêtises avec les données personnelles ou d'entreprise ? Comment être conforme à toutes les règles qui touchent à la lutte contre la cybercriminalité, à la cyberdéfense française et européenne, et à la protection des données personnelles ?* ». D'autant qu'à l'avenir, les clients et leurs dirigeants vont encourir des peines nettement plus importantes en cas de manquement. Tout doit être prévu dans les contrats qui les lient aux CSP.

Avec le Cloud, les dégats causés par des attaques ou des déficiences internes peuvent être multipliés par plusieurs ordres de grandeur

Focus Europe

Les multiples scandales liés à l'espionnage numérique de masse révélé par E. Snowden et aux pratiques jugées intrusives de grandes firmes *(notamment les « GAFA » : Google, Amazon, Facebook et Apple, mais pas seulement !)* ont alerté la société civile et les pouvoirs publics sur le caractère dépassé des réglementations en vigueur en Europe. Les travaux sur un nouveau règlement européen sur les données personnelles avaient démarré en 2011, et les projets de textes ont été adoptés en première lecture par le parlement en mars 2014. Ils font encore l'objet d'un lobbying violent de la part de grands groupes américains pour amoindrir les obligations, et de pas mal d'européens pour au contraire les augmenter, aller plus loin dans le droit à l'oubli, le contrôle des règles du Safe Harbor ou l'encadrement des Corporate Binding Rules.

Aujourd'hui, **le projet de règlement**, qui pourrait être adopté au final au 1er semestre 2015, est ambitieux : **renforcer les amendes** en cas de violation (cent millions d 'euros, ou 5% du CA mondial), imposer que la communication d'informations par des entreprises à un Etat tiers soit soumise à une **autorisation préalable d'une autorité nationale de protection des données dans l'UE**, instaurer un droit à **l'effacement des données** (« opt-out »), nommer un **délégué à la protection des données** dans les grandes entreprises, organiser **l'exécution** par une autorité de contrôle européenne de la **protection des données**, définir l'autorité de protection dans l'Etat membre comme **interlocuteur à l'échelle européenne** (« guichet unique »). C'est déjà beaucoup !

L'autre directive significative, la **NIS (Network & Information Security) ou Directive SRI (Sécurité des Réseaux et de l'Information)**, a été adoptée définitivement par le parlement en mars 2014. Les pays attendent les décrets d'application avant de la décliner dans les droits nationaux. Elle reprend et étend certains aspects de la LPM (Loi de Programmation Militaire) adoptée en France dès décembre 2013, et **fixe notamment des obligations à certains OIV à caractère européen** - qui opèrent dans les domaines de souveraineté : télécoms, IT, santé, alimentation, eau, énergie, transport, industrie, activités civiles des états...- et des **droits supplémentaires aux autorités nationales de sécurité**, tout en en **promouvant la coordination européenne de leurs actions.**

En France, un **CO**mité de **FI**lière **S**écurité (COFIS) a également été créé par le Premier Ministre, pour dynamiser les initiatives de l'aérien, du naval, du terrestre et en général des industriels de la sécurité, au sein du **CICS**. Le Plan Nouvelle France Industrielle (NFI) vise lui à développer la filière sécurité Française au sens large, incluant l'industrie de la cybersécurité.

Ainsi, dans le **plan CLOUD No 24** de la NFI, trois propositions sur 11 relèvent de la cybersécurité : **Label « Secure**

Cloud », espace de confiance européen, accélération de la transformation numérique des entreprises. De son côté, le **plan CYBERSECURITE No 33** met en place 16 actions regroupées en quatre thèmes : accroitre significativement **la demande en solutions de confiance,** notamment avec un **Label France**, développer pour les besoins de la France des **offres de confiance**, organiser la **conquête des marchés à l'étranger, et renforcer les entreprises nationales** du domaine de la cybersécurité, par exemple par la création d'un fonds d'investissement privé.

Dans les deux cas, l'un des objectifs est, par la sécurité, d'augmenter le niveau de **CONFIANCE**, et donc les bénéfices du numérique sur l'activité économique : *« En tant que décideur, je peux y aller, pousser le numérique, investir, c'est bon pour l'activité, l'efficacité opérationnelle, les collaborateurs, et je n'augmente pas mes risques business ou juridiques. Mon entreprise est à la pointe de la cybersécurité, et j'ai mis en place tout ce qu'il faut pour aller massivement vers le cloud… »*. Mais est-ce bien le cas ? Pas toujours aujourd'hui ! D'où l'idée de ces labels qui revient au galop.

Quelles Certifications pour la Confiance Numérique ? ?

Il en existe aujourd'hui beaucoup, **mais aucune n'est alignée sur les objectifs de la France et de l'Europe, notamment en termes de respect des réglementations et de souveraineté.** Pour prendre l'exemple du **Cloud**, il y a bien des certifications pour les CSP : *ISO 27001 peu spécifique sur ces sujets, Cloud Security Alliance CSA (USA), AICPA (USA), Tüv Rheinland (Allemagne) ou Eurocloud*, mais aucune ne prend en compte de façon systématique l'**Espace Economique Européen (EEE) de 31 pays et 508 millions d'âmes, la première puissance économique mondiale**, ou encore **les directives et règlements les plus récents mentionnés plus haut.**

Processus pour les CSP en Europe

Par exemple, il faudra s'assurer que les processus sont en place pour pouvoir **informer chaque victime en cas de perte de ses données par le CSP,** ou encore pour **communiquer rapidement les cyberattaques du CSP à l'autorité compétente** quand elle touche un SI d'intérêt vital. **Les données gérées par le CSP devraient aussi rester cantonnées dans l'EEE**, incluant back-ups, archivage, données temporaires. Si un Etat de l'EEE caractérise des **sous-ensembles de données CD/ SD qui doivent rester sur le territoire national,** cela devra être contrôlable. Il faudra aussi prendre en compte **le contrôle des fournisseurs de rang supérieur à un dans la chaine de service cloud,** et donner dans tous les cas la **préférence à des fournisseurs européens et français**, labellisés ou certifiés de confiance, quand ils existent.

Supervision de bout en bout de la Sécurité des SI & SI industriels par les SIEM et les SOC

Il faudra également maintenir une **supervision étendue de la sécurité du monde physique et virtualisé**, que ces VM soient chez le CSP ou dans l'entreprise, en IaaS, PaaS, SaaS, ou DaaS. Ainsi, la nouvelle génération de Security Operations Centers (SOCs) **devra mettre en œuvre la supervision de bout en bout, incluant le CSP. Les SIEM souverains de nouvelle génération comme PRELUDE de CS Communication & Systèmes** et les autres outils des SOC auront la visibilité et les logs de toutes les fonctions virtualisées, et **on saura ainsi par exemple en temps réel si une VM critique a été attaquée**, alors qu'elle vient d'être montée en quelques secondes pour une application critique ERP, BI, CRM ou autre, on verra **si notre espace privé et sécurisé chez notre CSP a été pénétré et nos données d'entreprise volées** par la porte de notre voisin de palier Cloud, ou si nos **données sont en train de sortir de France ou de l'EEE, mettant en cause directement la responsabilité de l'Entreprise et de ses dirigeants…**

Conclusion : aller plus vite et plus fort dans la certification européenne des Clouds de Confiance et Services Numériques

Nous sommes à la croisée des chemins, et les opportunités sont immenses, sur cette vague d'innovation qui a démarré il y a 20 ans, avec le Cloud comme l'un des derniers avatars. Cette 3ème révolution industrielle métamorphose tout : civilisation, cultures, société, entreprises, familles, valeurs, vies personnelles. Elle a besoin d'un surcroit de **confiance** pour donner le meilleur d'elle-même. Pour l'Europe, certifions nos prestataires de Cloud pour qu'ils nous donnent des garanties sur la **localisation des données dans l'EEE, le respect des lois et règlements européens sur les données personnelles et d'entreprise**, et l'usage de **l'état de l'art des technologies/ processus/ moyens humains pour mettre en œuvre les plus hauts niveaux de Sécurité des SI et des SI industriels**. C'est grâce à ces **CLOUDS DE CONFIANCE** que l'Europe gagnera la bataille du numérique.

L'AUTEUR

Thierry FLAJOLIET (1984), est Directeur Cybersécurité de CS Communication & Systèmes, un intégrateur de systèmes critiques pour la Défense et le civil, spécialisé dans les Services de Confiance et la Supervision (SOC, SIEM…), avec une vision européenne et française de la souveraineté. Il était auparavant directeur de l'innovation et membre du comité exécutif du Groupe LaSer, une banque filiale de BNP Paribas et des Galeries Lafayette, intégrateur/ opérateur de SI critiques et éditeur de solutions pour la Finance et le Retail, notamment en charge de la création des nouveaux business de croissance. Il a également été Directeur Commercial, Marketing & Relation Clients du Groupe Wolters Kluwer, spécialisé dans l'information professionnelle à forte valeur ajoutée, DG de startups dans la SSI, P-DG de l'éditeur de logiciel franco-américain Atempo - spécialiste de la sécurité des données pour les data centers -, General Partner Private Equity chez KBC à Bruxelles, DG du Groupe Monétique et Transactions Sécurisées de Dassault Electronique devenue Thales, et VP en charge des Produits Numériques & Nouveaux Services chez Thomson multimedia devenue Technicolor. Il est diplômé de l'Ecole Polytechnique (1979) et de Télécom ParisTech, et titulaire d'un MBA de l'INSEAD (1989).

PARTICIPEZ À LA 17ème CÉRÉMONIE DU PRIX DES TECHNOLOGIES NUMÉRIQUES

Télécom ParisTech et son association de diplômés Télécom ParisTech alumni organisent chaque année la cérémonie des Prix des Technologies Numériques. Ce Prix récompense les acteurs clefs de la société numérique et illustre l'impact du numérique dans tous les secteurs d'activités. Les organisateurs s'appuient sur un jury d'experts indépendants qui sélectionnent les acteurs et les projets ayant marqué le monde numérique et contribué à l'innovation grâce aux nouvelles technologies. Il attribue ainsi chaque année trois prix, remis lors d'une cérémonie, devenue un rendez-vous majeur qui rassemble près de 300 personnalités et décideurs de la société numérique.

LES LAURÉATS 2014

Prix du Manager
Henri Seydoux
Parrot

Prix de l'Innovation
Frédéric Potter
Netatmo

Prix de l'Objet connecté
Jean-Luc Errant
Cityzen Scinces

Prix spécial du Jury 2014 - Espoir du Numérique
Paul Benoit, Qarnot Computing

APPEL À CANDIDATURE DU PRIX DES TECHNOLOGIES NUMÉRIQUES 2015

Pour sa 17e édition, le Prix des Technologies Numériques poursuit sa reconnaissance des femmes et des hommes qui révolutionnent notre quotidien, en relevant le défi d'éclairer l'incroyable diversité de cette transformation. Pour la seconde fois depuis sa création, le Jury appelle créateurs et innovateurs à candidater à deux des trois prix qu'il décerne.

Ces deux prix sont placés cette année sous le thème de **l'économie collaborative.**

Le Prix de l'Innovation

Le Prix de l'Objet connecté

Qui peut participer ? Les entreprises, leurs dirigeants ou des innovateurs.

Informations : www.prixtechnologiesnumériques.org

SOUTENEZ UN ÉVÉNEMENT MAJEUR

DEVENEZ PARTENAIRE
DU PRIX DES TECHNOLOGIES NUMÉRIQUES 2015

Rejoignez les premiers partenaires de l'édition 2015
qui ont choisi de renouveler leur confiance aux organisateurs du Prix des Technologies Numériques.

Pourquoi nous soutiennent-ils ?

Pour découvrir les interviews de nos partenaires rendez-vous sur **www.prixtechnologiesnumeriques.org**

NOUS VOUS OFFRONS

Votre identité visuelle sur l'ensemble des supports de communication	✓	✓	✓
Présentation de votre entreprise sur le site dédié PTN	✓	✓	✓
10 invitations VIP pour la cérémonie de remise des prix	✓	✓	✓
Intervention du représentant de votre entreprise pendant la cérémonie	✓	✓	✓
Présence sur les photos officielles avec les lauréats et citation en qualité de Partenaire	✓	✓	✓
Interview vidéo de votre représentant et diffusion sur le site dédié	✓	✓	✓
Remerciements dans la revue Télécom de juin/juillet 2015	✓	✓	✓
5 invitations VIP supplémentaires		✓	✓
Invitations personnalisées aux diplômés Télécom ParisTech de votre entreprise		✓	✓
1 page de publicité dans la revue TELECOM spéciale PTN		✓	✓
Un annuaire Télécom ParisTech offert		✓	✓
5 invitations VIP supplémentaires			✓
Intervention plus importante de votre représentant pendant la cérémonie			✓
1 page d'interview de votre représentant dans la revue TELECOM spéciale PTN			✓
Diffusion d'une vidéo de l'entreprise sur le site dédié			✓
Diffusion de l'interview du représentant sur le site Télécom ParisTech alumni			✓
Vous participez à hauteur de	**5 000 €**	**10 000 €**	**15 000 €**

Contact
Christelle RIFFET, Responsable des Relations Entreprises à Télécom ParisTech
Tél. : 01 45 81 76 73 – christelle.riffet@telecom-paristech.fr

DU SECTEUR DE L'ÉCONOMIE NUMÉRIQUE

MOBILITÉ

Editorial

Par Paul JOLIVET (1995)

Mobilité, entre évolution techniques et révolutions business

La mobilité est un mot clé de nos sociétés en ce début du XXI[ème] siècle. Le Monde est en mouvement, chacun est en mouvement dans ce Monde. Le téléphone mobile, introduit dans les années 1990 a été un des outils, des catalyseurs de ce qu'il est convenu d'appeler la Révolution Numérique. D'évolutions en révolutions (pour citer le concept cher à Steve Jobs), l'appareil s'est imposé dans les poches de chacun, le taux de pénétration dans les pays développé dépassant 100%, pour atteindre dans certains cas 200% !

Les évolutions technologiques ont été fulgurantes depuis l'ouverture des premiers réseaux de seconde génération dans les années 1990. L'interface radio, le cœur de réseau ont rapidement permis à tous de communiquer. La capacité des réseaux continue de s'accroître au point qu'on peut se demander si un réseau fixe aura toujours un sens. Il est devenu rare qu'un hébergement, un lieu public ne propose pas d'accès internet, généralement sans fil. Les technologies sont devenues standard à travers le Monde, on parle de GSM, de 3G ou de 4G, de Wifi ou de Bluetooth. Se connecter est devenu un geste naturel.

Les technologies évoluent toujours, mais c'est maintenant sur les usages que la révolution est la plus visible Les téléphones sont devenus intelligents (smart) pour servir à bien d'autres usages que l'appel téléphonique. Ils digèrent ce que nous transportons dans nos poches (organiseur, appareil photo compact, gps, passe de transport, portemonnaie électronique et bientôt les clés de la maison). Dans le même temps, les réseaux ayant considérablement grandit, de plus en plus d'objets sont connectés (voitures, distributeurs de boissons, réfrigérateur, station météo personnelle, installations domotiques, alarmes), et chacun commence à pouvoir piloter son monde à distance. Même les machines communiquent entre elles, les compteurs d'électricité, d'eau ou de gaz vont bientôt pouvoir échanger des informations et offrir des services évolués, nos voitures signaleront leurs défaillances ou appelleront les secours en cas d'accident.

Dans ce contexte, les modèles d'affaires changent de dimension et de nouveaux acteurs entrent dans la danse. L'opérateur de téléphonie historiquement au centre de l'écosystème se trouve en concurrence avec des fournisseurs de service ou de terminaux. L'interaction entre machines, les données personnelles et de localisation transitent, imposant au régulateur la vigilance.

Le dossier qui suit tente de faire par plusieurs angles de faire le point les technologies en déploiement, quelques usages qui se développent, et des modèles économiques qui évoluent.

Paul JOLIVET (1995) est Directeur Recherche et Standards en Europe de LG Electronics (téléphones mobiles). Son champ d'action est principalement l'innovation et la standardisation. Il est Président du 3GPP CT WG6 (Applications carte à puce) et de l'ETSI SCP TEC (Spécification de la plateforme carte à puce multi applicative).
Il enseigne régulièrement dans plusieurs Ecoles dont Télécom ParisTech et Télécom Bretagne. Il étudie par ailleurs à l'Université Paris Dauphine dans le cadre d'un Doctorate of Business Administration sur le domaine de l'Innovation.

LTE pour les réseaux mission critique

Par Christophe MATHIEU

L'introduction à court terme de services large-bande est un besoin fort des réseaux mobiles mission critique. La technologie LTE, en cours de déploiement commercial, semble un bon candidat pour bâtir la prochaine génération des réseaux mission critique. Quels sont les verrous technologiques et opérationnels et les évolutions à apporter à cette technologie pour atteindre ce but ?

Un besoin bien particulier

Les réseaux mobiles dits mission critique, sont impliqués dans les situations où les opérations de secours et le respect des lois sont en jeu. Ils sont utilisés par des organisations comme la police, les pompiers, les premiers secours. On les retrouve dans les organisations militaires principalement hors du périmètre de combat et auprès des opérateurs de transport ou d'infrastructure critiques.

A ce jour principalement orientés vers des services voix, ils se différencient des réseaux commerciaux sur plusieurs points :

- des services spécifiques axés sur les appels de groupe avec prise de parole à l'alternat (Push-To-Talk) et des fonctions de priorité-préemption,
- des performances spécifiques comme un temps de prise de parole très faible et une latence minimale,
- un niveau de sécurité accru avec des mécanismes de bout en bout laissant la possibilité aux organisations d'implémenter leurs algorithmes.

Les technologies P25 (Etats-Unis) et Tetra (Europe, Asie) se partagent les déploiements dans le monde depuis une vingtaine d'années et offrent principalement à ce jour des services de voix et de transmission de données bas débit permettant notamment la géolocalisation.

Les nouveaux besoins sont clairement orientés vers des services de données, tout en gardant la composante mission critique pour la plupart de ces nouveaux services.

On voit ainsi apparaître, en complément des services de voix, des besoins de transferts sécurisés de données (fichiers, cartes,...), de vidéo et photos en temps réel ou non, toujours sous la forme de communications de groupe.
Ces besoins de communications large-bande en mobilité ont ciblé la technologie LTE (dite 4G). Les déploiements des réseaux commerciaux se multiplient dans le monde entier, gage d'une maturité sans pareille.

Les instances de standardisation et la communauté des réseaux mission critique se sont naturellement tournées vers LTE pour définir la prochaine génération de ces réseaux, dont le marché estimé avoisine les 9 Mds $ à l'horizon 2020.

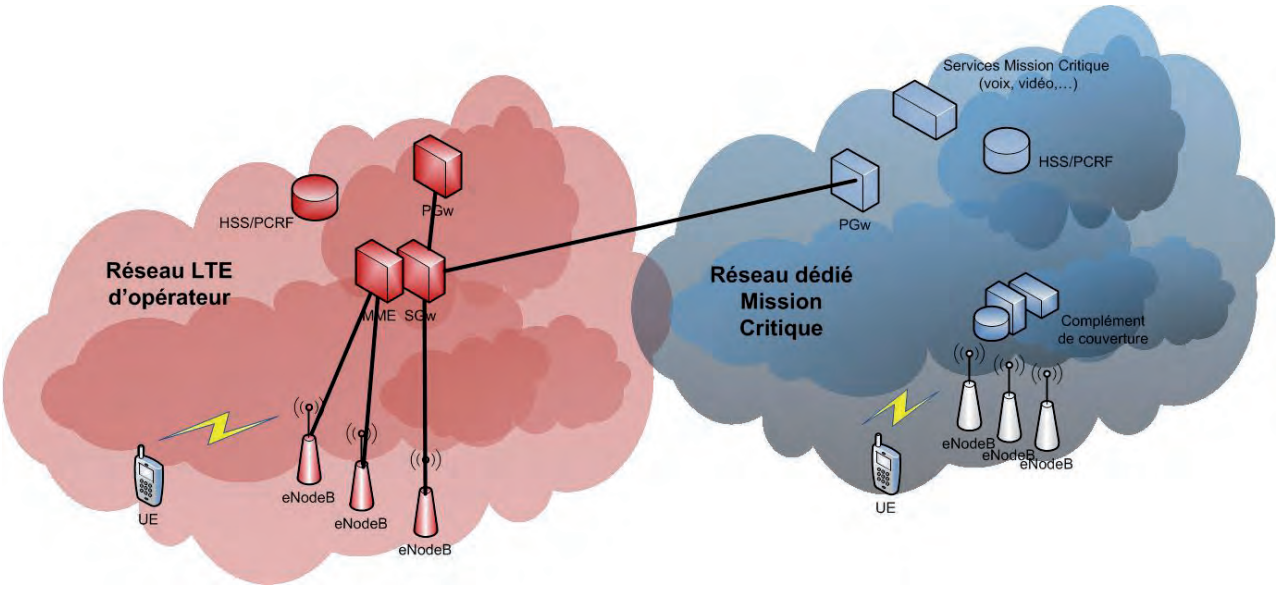
Les points forts de LTE

La technologie LTE est le fruit de l'effort de standardisation l'échelle mondiale. On dispose ainsi d'un standard utilisable par des milliards d'usagers. On devine alors les premiers bénéfices que l'on peut tirer de cette technologie

- une interopérabilité inter-organisationnelle et à l'échelle mondiale : cela n'avait pas été le cas aupravant pour les services mission critique de voix, des évènements tragiques (11 Septembre 2001) ont rappelé ce besoin primordial ,
- un marché adressable suffisamment vaste pour amortir les coûts R&D importants dans un marché ultra concurrentiel.

Il est ainsi apparu évident que la prochaine génération des réseaux mission critique large bande devait puiser dans le vaste panel de technologies développées autour de l'éco-système LTE.

C'est le cas de la technologie radio (forme d'onde LTE), du cœur de réseau tout IP (Evolved Packet Core) conjointement développés mais aussi des services multimédia développés dans le cadre de l'IMS (IP Multimedia Sub-system).



L'architecture du réseau LTE mission critique

Néanmoins, un réseau mission critique se différencie sensiblement d'un réseau commercial. Il faut donc analyser en détail les verrous technologiques et opérationnels et les réponses que le marché et les standards apportent pour promouvoir le LTE en tant que technologie de référence pour les futurs réseaux mission critique large bande.

Problématiques de fréquences et d'architecture

Le spectre radioélectrique fait partie de ce patrimoine immatériel dont les états tentent de tirer le meilleur parti. En temps de crise et avec le formidable succès des services de mobilité large-bande, les états ne résistent pas à la manne financière que représente l'allocation du spectre de fréquences.

Envisagée un temps, la réallocation du spectre des technologies Tetra et P25 s'avère complexe à mettre en place en raison de la granularité respective des technologies (25 kHz en Tetra versus 1.4, 5 et 10 Mhz en LTE).

Pour répondre à la pression des utilisateurs souhaitant démarrer une offre de service large-bande, on se dirige dans de nombreux pays vers une architecture de réseau s'appuyant sur des réseaux d'opérateurs. La figure ci-dessus illustre les grandes lignes de l'architecture.
Le réseau mission critique s'appuie sur un ou plusieurs réseaux d'opérateurs suivant un modèle dit full MVNO (Mobile Virtual Network Operator) dont les grands principes sont que le réseau mission critique :

- maîtrise la gestion de ses abonnés (profils, SIM,...) grâce à une base de données des abonnés (HSS) gérée en propre,
- maîtrise la qualité de service de bout en bout au travers du couple passerelle réseau PGw/ PCRF gérés en propre et de mécanisme inhérent à la technologie LTE tels que la gestion de la priorité et de la préemption,
- apporte les services large-bande de communication de groupe non déployés,
- apporte des compléments de couverture aux réseaux d'opérateurs via des plaques locales ou régionales de stations de base (eNodeB) fixes ou rapidement déployables connectées à leur propre cœur de réseau.

Améliorer la disponibilité des réseaux

Les compléments de couverture se justifient par un besoin d'accroissement ponctuel ou permanent de bande passante et/ou de résilience accrue du réseau. Ce dernier point peut être adressé par des évolutions fonctionnelles de l'architecture standard du cœur de réseau LTE.

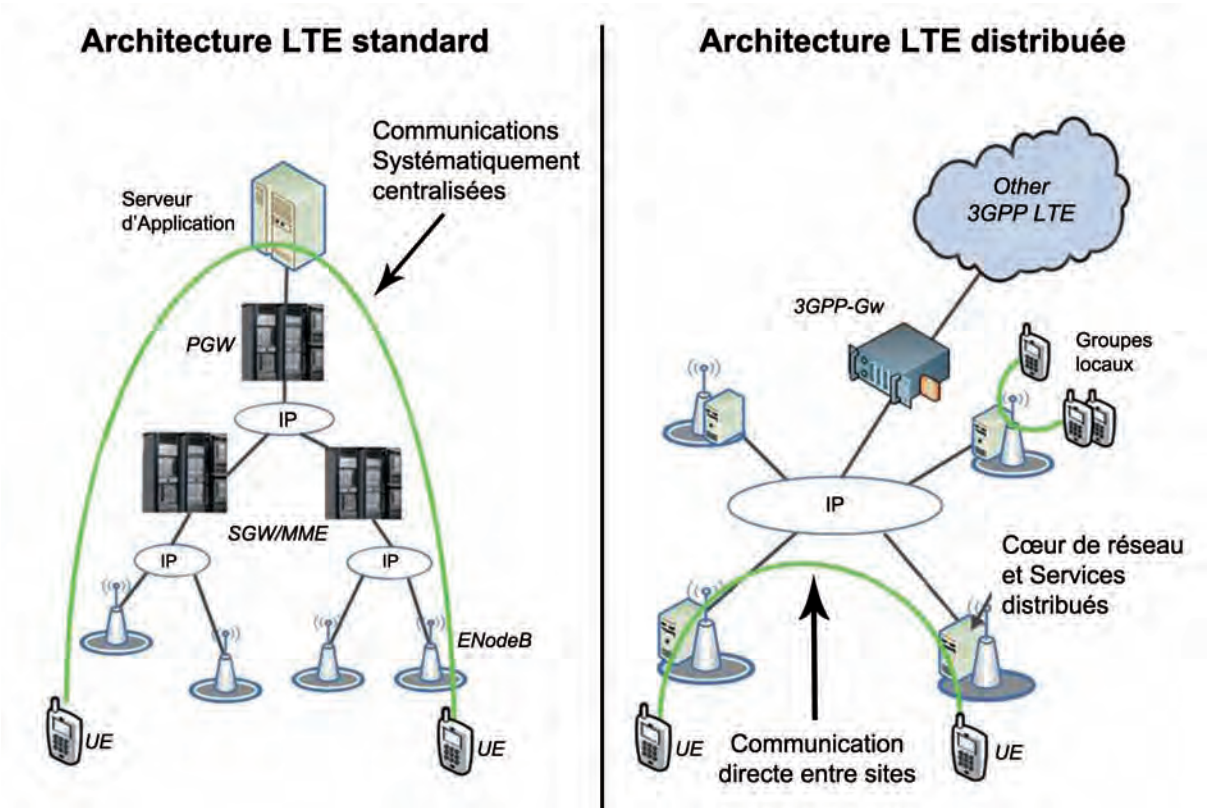
LTE propose des mécanismes de réplication qui correspondent aux exigences de fiabilité des réseaux commerciaux et qui peuvent s'avérer insuffisants pour les réseaux mission critique. Typiquement, disposer d'une architecture de cœur de réseau sans dégradant de sécurité ou services en cas de pannes multiples simultanées et massives est une capacité recherchée pour les réseaux mission critique.

Les architectures actuelles, centralisées, ne proposent que des mécanismes de réplication ponctuels ou de dégradation des services et performances. Une approche consiste à s'orienter vers une architecture massivement distribuée garantissant la disponibilité de l'ensemble des fonctions du réseau dans chacun des sites radio (ou groupe de sites radio) comme illustré dans la figure page suivante.

Le principe consiste à répliquer de petites instances à la fois du cœur de réseau LTE et des serveurs d'application des services mission critique. Ainsi quelque soient le nombre de pannes simultanées, le réseau dispose de mécanismes de résilience permettant aux sites d'accéder à 100% des services.

De plus, ce type d'architecture offre une bonne optimisation de la bande passante d'interconnexion des sites radio puisque le trafic ne remonte pas systématiquement vers un site central comme dans l'architecture LTE standard.

Ce type d'architecture est également favorable aux performances globales des services, en particulier sur des paramètres critiques comme le temps d'établissement des communications.



Vers une architecture distribuée du réseau

Services et Sécurité des réseaux

Les services de communication spécifiques aux réseaux mission critique sont orientés autour des communications de groupe, immédiatement accessibles via des boutons dédiés sur les téléphones.
On peut mentionner quelques fonctions clefs nécessaires à tout déploiement de type mission critique :

- appels de groupe avec prise de parole à l'alternat et appels individuels full ou half duplex avec de hauts niveaux de performances en termes de temps d'établissement (400 ms) et de latence des communications (200 ms),
- gestion de la priorité et de la préemption d'appels respectant les procédures opérationnelles et les hiérarchies des organisations utilisant les réseaux,
- communications directes entre terminaux en l'absence de l'infrastructure réseau.

L'introduction des services large-bande (vidéo, données) doit strictement respecter ces modes de fonctionnement.
Ces dernières années, les instances de normalisation des réseaux mission critique ont œuvré à promouvoir la prise en compte de leurs besoins par les instances de standardisation des réseaux LTE (3GPP). Les releases 12 et 13, disponibles chez les constructeurs à l'horizon 2016, prendront en compte les besoins spécifiques et permettront les premiers déploiements des réseaux mission critique large-bande.

Il en est de même pour la sécurité : le standard LTE apporte des mécanismes de sécurité à la pointe de la technologie ; on peut citer :

- des mécanismes d'authentification mutuelle terminaux/réseau
- des mécanismes de cryptage des données sur l'interface air et entre les éléments du cœur de réseau
- des mécanismes de cryptage du plan de contrôle de l'ensemble de la solution

Il manque à ce jour des mécanismes de cryptage de bout en bout et la possibilité pour le client final d'implémenter ses propres algorithmes.
Ce besoin sera intégré dans les releases à venir de LTE, en même temps que les évolutions fonctionnelles précédemment mentionnées.

Une solution crédible qui prend forme

On constate ainsi que la technologie LTE, enrichie par les spécifications venant des organismes de standardisation des réseaux mission critique, apporte une réponse crédible aux besoins des utilisateurs concernant l'évolution de leurs réseaux vers le large-bande.

Les briques technologiques sont disponibles à un coût raisonnable car s'appuyant sur les développements des réseaux commerciaux LTE, une infrastructure correspondant aux attentes des clients finaux et prête à intégrer les ultimes fonctionnalités mission critique que le standard LTE aura développé.

Ainsi étendue, la technologie LTE peut également servir utilement les réseaux militaires, en complément des radios de combat, dans les contextes où le brouillage n'est pas d'une impérieuse nécessité (opérations de maintien de la paix, bases arrière,....).

L'AUTEUR

Christophe MATHIEU, est actuellement responsable des développements de la solution PMR chez Thales.

De l'espace pour votre avenir

Aux quatre coins de la planète comme dans l'espace, Eutelsat apporte son expertise pour relier les hommes. Diffusion de programmes TV et radio, réseau d'entreprise, accès à l'internet,... Eutelsat est au coeur des spécificités locales et des cultures nationales. Ingénieurs, commerciaux, financiers, juristes,... nos 1000 collaborateurs issus de près de 32 nationalités cultivent l'esprit d'équipe et l'excellence.Premier opérateur européen de satellites, n°3 mondial, Eutelsat s'appuie sur une culture résolument européenne pour relever des défits planétaires.

eutelsat

www.eutelsat.com

Avec Eutelsat, le WiFi prend l'air !

Une connexion Internet WiFi dans un avion de ligne ou un paquebot de croisière ? Une connexion GSM dans un ferry ou a Yacht ? Eutelsat - 1er opérateur européen de télécommunications par satellite et 3éme opérateur au niveau mondial - fournit une gamme de solution complète et innovante pour apporter maintenant la connexion haut débit à bord, que ce soit sur mer, sur terre ou dans les airs.

Olivier Risse, Directeur des Services Mobiles chez EUTELSAT, nous parle de ces projets innovants.

Quelle est la place des services mobiles chez un opérateur de satellites comme Eutelsat ?
Eutelsat est historiquement un opérateur de services fixes, que ce soit pour l'image, avec la diffusion des bouquets de télévision pour alimenter les réseaux câblés de nos villes, pour la réception directe de la télévision à la maison, pour les grands réseaux de données à destination des entreprises, et pour l'accès internet haut débit par satellite pour les particuliers.
A ce titre, Eutelsat propose maintenant par exemple un service d'accès internet, appelé Tooway™, qui permet avec une petite parabole extérieure de disposer chez soi, à la maison, d'un accès internet à haut débit, indépendamment des réseaux terrestres.

A présent, avec la croissance très rapide des besoins de communications en mobilité, nous constatons que le satellite est une solution également très efficace, pour tous les modes de transport, véhicules, trains, bateaux ou avions. C'est pourquoi Eutelsat participe activement au développement de solutions mobiles par satellite avec des partenaires clef dans chaque secteurs.

Quels sont les services mobiles maritimes proposés par Eutelsat ?
Eutelsat dispose d'une couverture Ku quasi globale, qui va de l'océan Atlantique à l'Indien et au Pacifique. Nous sommes donc naturellement présents dans le domaine des services maritimes et nous proposons des services de données à haut débit par satellite, notamment à bord de navires de transport de la marine marchande. De grands noms du secteur nous font confiance. Nous proposons soit des services de communication maritimes régionaux, couvrant l'Europe, le Moyen-Orient, l'Afrique, l'Océan Indien ou le Pacifique, soit des services Globaux, permettant à un même navire de disposer d'un service de communication où qu'il se trouve.
Par ailleurs, nous sommes également présents à bord de navires de transport de passagers, ainsi qu'à bord de paquebot de croisière. Les services fournis à bord via satellite sont des services d'accès internet WiFi pour les passagers ou des services de téléphonie GSM, via tablettes, smartphones ou ordinateurs portables habituels.

Enfin nous proposons des services maritimes sur mesures et sécurisés pour des applications professionnelles.

Avez-vous des projets de services mobiles par satellite dans le domaine aéronautique ?
Oui, les services satellite à bord des avions représentent également un axe de développement important.

Nous sommes déjà présents sur le marché aéronautique avec des solutions en technologie Ku et une couverture semi globale. Cette technologie Ku est actuellement utilisée pour les Jets privés et pour les avions de ligne long-courrier.

En complément aux solutions globales Ku adaptées aux long-courriers, nous allons ouvrir un service de connectivité aéronautique Ka, baptisé *Eutelsat Air Access*, adaptées aux court et moyen-courriers. La technologie Ka permet des débits 10 fois plus importants par avion et ce dans des zones à forte densité de trafic aérien, comme par exemple l'Europe.
Eutelsat Air Access permettra aux partenaires « In Flight Entertainment & Connectivity » de Eutelsat qui commercialiseront ce service de proposer aux compagnies aériennes et à leurs passagers un accès internet WiFi à bord, des services de streaming vidéo ou des services de téléphonie accessibles directement sur les tablettes, Smartphones.

Enfin, pour étendre ces services aéronautiques par satellite à d'autres types d'avions ou à d'autres types de besoins à bord, Eutelsat noue également des partenariats avec des équipementiers aéronautiques, spécialistes en SatCom, afin de tester et de valider sur nos satellites leurs nouvelles solutions mobiles Ku et Ka.

Le groupe Eutelsat

Premier opérateur européen de télécommunications par satellite et l'un des trois premiers mondiaux, Eutelsat emploie plus de 1000 collaborateurs de plus de trente nationalités. Le groupe collabore avec des entreprises et opérateurs de télécommunication dans plus de 150 pays et met sa technologie et ses solutions à disposition de tous les secteurs d'activité.

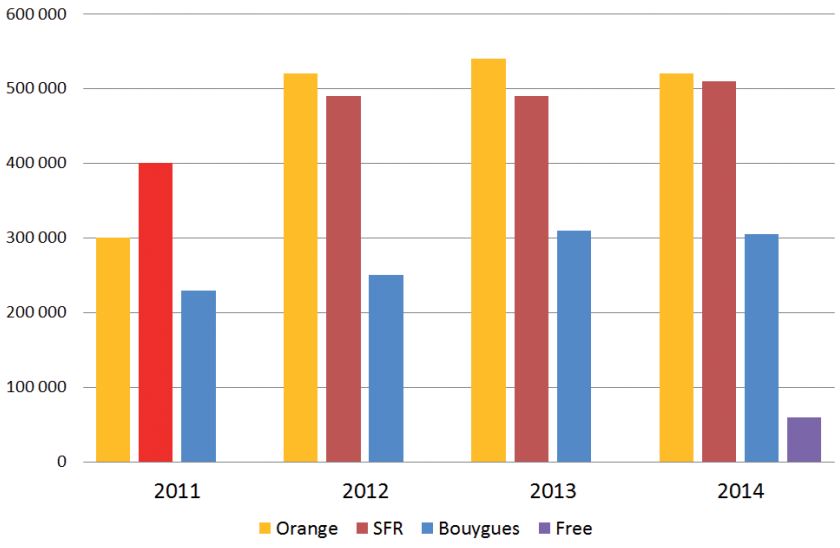
Joyn ou le nouveau service de communication 100% opérateur !

Par Grégoire GALIEVSKY (2000)

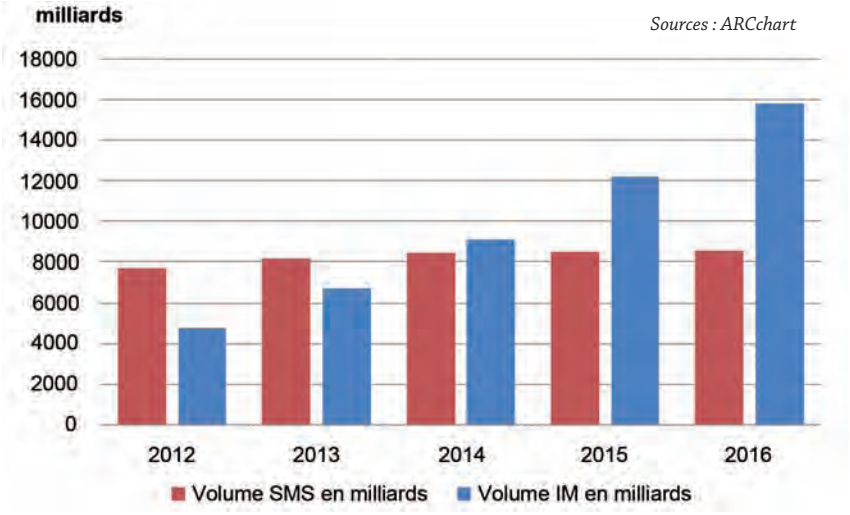
Avec l'arrivée massive de nouveaux acteurs en provenance du monde de l'Internet, les opérateurs se voient désormais concurrencés sur des services qu'ils considèrent comme appartenant à leur cœur de métier. What'sapp, Skype, Line ou encore iMessage et FaceTime grignotent chaque année des parts de marché aux SMS ou aux appels vocaux.
Ces services en pleine croissance profitent largement des possibilités techniques offertes par les réseaux 4G en proposant toujours plus de fonctionnalités à leurs clients.
En 2014, le nombre de messages instantanés envoyés depuis un mobile devrait dépasser celui des SMS. Pour rester dans la course, les opérateurs doivent réagir en proposant de nouveaux services de communication innovants et 100% 4G. Leur réaction s'appelle Joyn !

La fin d'une ère

Le SMS reste largement utilisé par les Français, pour s'échanger leurs vœux de bonne année. On bat à chaque fois de nouveaux records ; cependant pour la première fois en 2014 l'augmentation semble marquer le pas.
Les opérateurs ont fait leurs comptes et en dehors de Free qui est un nouveau venu dans le monde de la téléphonie mobile, le nombre de SMS envoyés tous opérateurs confondus n'a pas progressé en 2014.
Et même si le nombre de MMS envoyés a augmenté, ce phénomène n'explique pas à lui seul la stagnation du nombre de SMS envoyés.
Les Français seraient-il moins enclins à se souhaiter la bonne année ? Ou faut-il chercher une réponse autre part, dans les solutions de messagerie instantanée alternatives comme Skype, Viber, What'sapp, ooVoo ou plus récemment



Source : Orange SA



Sources : ARCchart

Line qui proposent aux clients des opérateurs d'appeler ou d'envoyer des messages gratuitement ?
Ces messageries alternatives ont tellement de succès que les constructeurs de terminaux mobiles eux-mêmes s'y mettent ; certains comme Nokia intègrent directement Skype dans leurs téléphones, d'autres proposent leurs propres services comme Apple avec iMessage, BlackBerry avec BBM ou Samsung avec Chaton.
Face à autant de concurrence, les opérateurs peuvent-ils encore sauver le SMS ?

Les opérateurs sur la défensive

La fin du SMS est déjà une réalité dans certains pays qui n'ont pas pu empêcher l'irrésistible ascension des OTT (Over The Top) ; ainsi l'Espagne, la Corée, les Pays-Bas ont déjà pu constater l'effondrement de l'usage du SMS au profit de concurrents comme What'sapp ou Kakao Talk.
Et ce succès ne laisse pas indifférent les géants de l'Internet puisque Skype s'est fait racheter 8m$ par Microsoft et que Facebook vient d'acquérir What'sapp pour 16m$.
De manière générale, dès 2014, l'usage des messages instantanés devrait dépasser celui des SMS.
Pour rester dans la course, les opérateurs devront recréer un nouveau service de communication plus performant, capable de tirer profit des très hauts débits offerts par la 4G.

Les clés du succès

Objectivement, rien ne prédestinait le SMS à devenir le premier service de messagerie mobile, qui, 20 ans après son lancement, continue de devancer des géants de l'Internet comme Facebook ou Microsoft.

Lors de son lancement commercial en 1997, 80% des français affirmaient qu'un téléphone servait avant tout à téléphoner et non à écrire. Et les chiffres semblaient leur donner raison : pendant deux ans, ce service est resté méconnu et peu utilisé.

Il faudra attendre l'interconnexion du SMS entre les trois opérateurs français pour en voir l'usage décoller. Avec sa tarification à l'unité, le SMS s'est vite révélé comme une poule aux œufs d'or pour les opérateurs.

A posteriori, on peut résumer la recette du succès du SMS en trois mots :
- **Simplicité**
- **Fiabilité**
- **Universalité**

Or ces trois spécificités sont loin d'être acquises par les concurrents du SMS.
En analysant de près la situation, les opérateurs semblent encore disposer d'atouts importants dont ils peuvent jouer pour contrer la concurrence.

La simplicité tout d'abord. Les services comme Skype ou Viber nécessitent la plupart du temps l'installation d'une application sur le mobile, la création d'un compte et imposent d'inviter des contacts avant de pouvoir les appeler. Ce n'est pas le cas du SMS.

La fiabilité impose un contrôle de bout en bout du service : réseau, distribution, assistance, ce qui est le cas pour le SMS.

Or les tiers ne contrôlent pas les réseaux qu'ils utilisent pour diffuser leurs services, ce qui permet à certains opérateurs de filtrer ces usages. Cependant la pression des organismes de régulation et l'arrivée des réseaux de 4ème génération permettront d'améliorer la qualité des réseaux pour les services concurrents en assurant une fiabilité quasiment identique.

Les opérateurs ont la possibilité de demander aux fabricants de téléphone d'installer des services comme le SMS ou le MMS sur les téléphones. Les OTT n'ont généralement pas cette opportunité.

Les opérateurs ont aussi la possibilité d'installer une relation de confiance en assurant le service après-vente et éventuellement la facturation ce qui est généralement plus compliqué pour les OTT.
Enfin, la fiabilité fait également intervenir la confiance que peut avoir l'utilisateur dans un service. Les opérateurs sont en mesure de garantir cette confiance.
Les rumeurs sur une utilisation inappropriée des données personnelles des utilisateurs par les OTT sont nombreuses. Les révélations faites sur les méthodes de la NSA viennent renforcer la méfiance des clients et les sensibilisent sur l'importance de préserver leur vie privée.

L'universalité enfin consiste à proposer un service disponible pour tout support et pour tout réseau. Avant d'envoyer un SMS, le client ne se pose généralement pas la question de savoir si le correspondant a un téléphone compatible.

Cela n'est possible que parce que le SMS est un service **standardisé.** Le SMS a été défini dans le cadre de la GSMA, un organisme de normalisation intégrant les principaux opérateurs européens.

C'est donc au sein de la GSMA également que devra naître la norme de communication du futur.

RCS : la nouvelle norme de communication

En 2007 les cinq grands opérateurs européens ont décidé de se lancer dans l'aventure « RCS » pour Rich

Source : Orange SA

Communication Suite. Cette norme prendra par la suite le nom de Joyn, plus facilement mémorisable.
Le cahier des charges de Joyn consiste à proposer de manière standardisée les mêmes services de communication que les OTT. Ces services ont été répartis en deux familles :

Le rich messaging qui comprend :
- Le tchat entre utilisateurs ;
- l'envoi de fichiers entre utilisateurs ;
- les discussions de groupe instantanées.

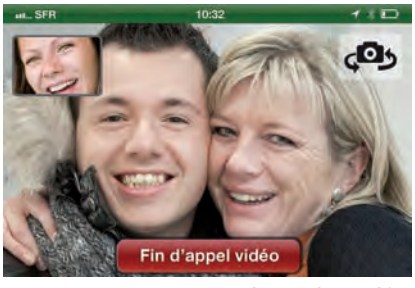
Le rich call qui comprend :
- Le partage de vidéo en cours d'appel ;
- Le partage de fichiers pendant un appel.

Grâce à cet effort de normalisation, ces services sont mis en place de façon homogène par l'ensemble des opérateurs. Ils peuvent également être intégrés nativement par les constructeurs de terminaux : Samsung, Nokia, LG, BlackBerry, Huawei, ZTE, Sony ont choisi d'intégrer la norme RCS directement dans leurs téléphones.
Le service se veut aussi simple à utiliser que le SMS : pas d'application à télécharger, pas de compte à créer : « it's just there, it just works ! »

Illustration des fonctionnalités de Joyn

A titre d'exemple, un fil de discussion Joyn entre deux personnes se présente de manière assez similaire à celui proposé pour les messages SMS (voir écran ci-dessus). Il propose cependant les améliorations suivantes :
- Joyn permet de connaître l'état de réception du message par le destinataire : envoyé/reçu/lu ou en échec,
- Joyn permet d'envoyer/recevoir des fichiers de haute définition et de différentes sortes : images, vidéos, musiques, fiche contact, localisation…
- Joyn permet l'envoi et la réception d'une liste d'Émoticônes normalisées par la GSMA.

A tout moment lors d'un tchat, l'utilisateur peut ajouter d'autres interlocuteurs et ainsi commencer une conversation de groupe.
Enfin, lors d'un appel, si les deux interlocuteurs sont compatibles Joyn, ils verront s'afficher sur l'écran de leur smartphone deux icônes. L'une d'elle permet de réaliser un appel vidéo, l'autre de partager un fichier en cours d'appel.



Source : Orange SA

Joyn : déjà une réalité dans plusieurs pays

2013 a été l'année du lancement de Joyn dans plusieurs pays.

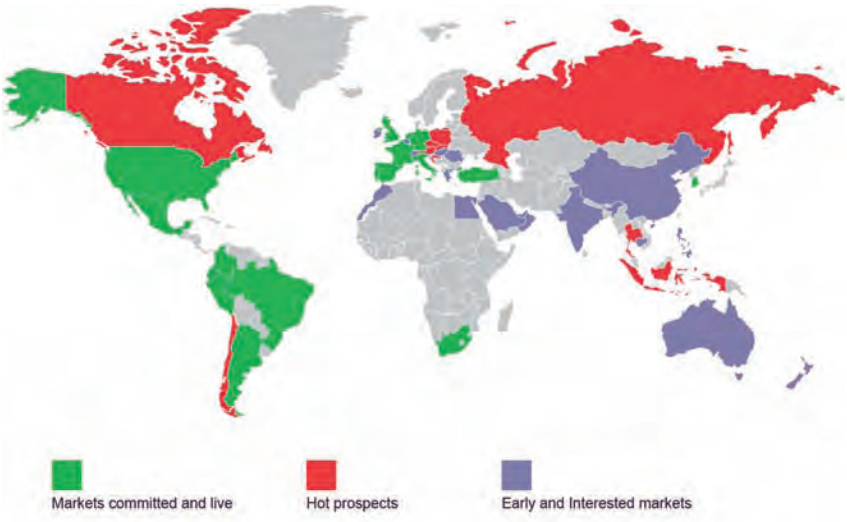
A ce jour, 11 pays ont mis en œuvre un service homologué Joyn. Cinq pays ont franchi l'étape du lancement commercial :
- **En Allemagne :** Vodafone, T-Mobile, O2
- **En Corée :** KT, LG et SK Télécom
- **Aux États-Unis :** Metro PCS, AT&T prochainement
- **En Espagne :** Movistar, Orange, Vodafone
- **En France :** Orange

De prochains lancements sont annoncés en Belgique, Chine, Pologne, Roumanie, Slovaquie. En France, SFR prévoit de rejoindre Orange.

Mais malgré ces lancements, le succès se fait attendre.

Des problèmes structurels à résoudre

A l'exception de la Corée, où le lancement a été réalisé en simultané par les trois opérateurs dans une version 4G, le service n'a pas encore rencontré le succès attendu.



Joyn déjà une réalité dans plusieurs pays - Source : GSMA - www.gsma.com

Cela peut s'expliquer par plusieurs raisons :
En France par exemple, Joyn n'est disponible que pour les clients d'Orange. Il faudra attendre que SFR, Bouygues, Free et les opérateurs virtuels lancent Joyn pour en voir l'usage augmenter significativement.
En Espagne, le nombre de terminaux proposant Joyn est encore limité, le service est au final rarement utilisable.
Il faudra attendre un nombre critique d'utilisateurs pour que l'usage puisse décoller.
Enfin, la norme actuelle est perfectible. Certaines fonctionnalités importantes ne sont pas disponibles, comme le partage de fichiers dans une discussion de groupe. L'implémentation dans les téléphones n'est pas toujours optimale. Le logo et le service sont encore mal connus. Le service de vidéo dépendant de l'établissement d'un appel ne fonctionne actuellement qu'en 3G en attendant l'arrivée de la VoLTE, Voix sur LTE. Joyn ne dépasse pas encore les frontières, il ne permet pas d'envoyer de message d'un pays à l'autre même s'ils ont déjà lancé Joyn. Les opérateurs vont devoir réaliser des contrats de partenariat pour permettre au service d'interfonctionner entre leurs réseaux.
Tous ces défauts sont autant de freins au développement de l'usage, mais ces contraintes devraient se résoudre dans un futur proche.
Le nombre de téléphones intégrant Joyn augmente régulièrement et des accords entre opérateurs de différents pays sont en cours.
L'arrivée de la Voix sur LTE, c'est-à-dire de la voix sur les réseaux 4G, permettra un fonctionnement optimal de Joyn en rendant le service full IP.
Il faudra encore plusieurs mois pour que Joyn devienne véritablement un concurrent sérieux du SMS. Néanmoins, la prochaine norme de Joyn prévoit de fusionner les services SMS et Joyn : les messages seront affichés dans une même boîte de réception, et lorsque les deux interlocuteurs seront compatibles Joyn, le téléphone choisira l'envoi d'un message Joyn plutôt qu'un SMS/MMS.

La substitution est en marche !

La communauté des développeurs est déjà mobilisée pour améliorer le service et inventer le service Joyn de demain.

Quel Joyn pour demain ?

Joyn se veut un standard ouvert. Le service pourra donc être utilisé bientôt par la communauté des développeurs.
La GSMA a organisé en février 2013 un concours d'innovation autour de Joyn. Des applications concrètes ont été développées dans des services comme Dailymotion ou Viadeo.

Les possibilités d'usages professionnels sont également nombreuses : services de Visioconférence, partage de documents ou sessions de travail collaboratif depuis une tablette avec le tchat de groupe et le partage de document.
La communication intervenant partout, les applications de Joyn sont sans limite dans la santé, l'éducation, la surveillance, les transports, les loisirs.
Et qui sait, les OTT se décideront peut-être à intégrer Joyn dans leurs applications ? On peut tout à fait imaginer Facebook intégrer Joyn dans son site pour réaliser ses fonctionnalités d'IM.
Ainsi, ironie de l'histoire, Joyn pourrait devenir un partenaire indispensable des OTT !

Conclusion

Face à la montée des OTT comme Skype, Viber ou What'sapp, Joyn est la réponse la plus pertinente que pouvaient concevoir les opérateurs.
En s'appuyant sur les forces qui ont fait le succès du SMS - simplicité, fiabilité et universalité -, les opérateurs capitalisent sur leurs meilleurs atouts pour s'imposer dans le monde des communications.

Mais Joyn est un projet au long cours. Entamé en 2007, le projet n'a vu le jour qu'en 2012 et avec une offre de services inférieure à celle que propose le marché. C'est donc une course contre la montre qui s'est engagée et c'est seulement dans leur capacité à équiper rapidement le marché et à se concentrer sur les fonctionnalités clés que les opérateurs parviendront à garder la main sur les services de communication.
Dans le cas contraire, il faut s'attendre à ce qu'un Google ou un Facebook se substituent à l'opérateur sur ces services, celui-ci se voyant réduit au rôle de « tuyau ».

Réussir l'adoption de Joyn est une question de crédibilité pour les opérateurs qui prouveront par-là même qu'ils sont toujours les mieux placés pour continuer à inventer la communication de demain.

L'AUTEUR

Grégoire GALIEVSKY (2000), a pendant quatre ans chez Orange France SA, conduit un programme consistant à moderniser la suite des services de communication de l'opérateur pour l'adapter aux évolutions technologiques et aux besoins des clients. Au sein de ce programme Grégoire a notamment piloté le lancement de Joyn chez Orange France. Grégoire est actuellement manager chez Orange Consulting dans le secteur Banques et Assurances.

Entre collaboration et concurrence, le standard : un incontournable

Par Paul JOLIVET (1995)

La standardisation s'est imposée au départ comme le lieu de l'action collaborative de l'industrie naissante de la mobilité. L'impératif économique et les intérêts industriels se sont doucement imposés, aboutissant parfois à des échecs ou à la fragmentation d'un marché hyperconcurrentiel. Les contributeurs cherchent aujourd'hui dans la standardisation un nouvel équilibre (rapport de force) …

Au commencement étaient les solutions propriétaires

Les systèmes de télécommunications mobiles ont été développés autour de grandes sociétés comme Motorola, Nokia, Ericsson ou Nortel. Leurs solutions propriétaires avaient pu s'imposer comme des standards de facto, tel le NMT scandinave. Le besoin d'un système commun s'impose dans les années 1980-90, le continent européen regroupant typiquement les contraintes de l'interopérabilité (beaucoup de pays développés, une « faible » superficie et donc un besoin d'harmonisation transfrontalière et des situations d'itinérance plus fréquente) ainsi que solutions à ce défi (des industriels maîtrisant la technique, un soutien politique et un marché suffisamment vaste pour tous les acteurs).

On voit naturellement une initiative naître en Europe qui donne le GSM. Cependant les industriels posent rapidement des bornes au champ de la standardisation, pour permettre le développement de produits interopérables sans toutefois les priver de différenciation. C'est ainsi par exemple que l'interface homme-machine du téléphone n'a jamais été standardisée.

L'évidence d'un monde qui vise l'interopérabilité

Pour atteindre la dimension internationale et permettre l'itinérance, les systèmes mobiles doivent apporter un niveau d'interopérabilité idéal, qui est apportée par la standardisation (ou le monopole!). L'approche « standard » supportée par une volonté politique forte fait le succès du GSM, issu de centres de recherche d'opérateurs à l'époque contrôlés par les administrations nationales puis intégré à des instances européennes : Conférence Européenne des administrations des Postes et Télécommunications (CEPT) d'abord, European Telecommunication Standard Institute (ETSI) ensuite. L'influence politique directe s'estompe à la suite de la privatisation des opérateurs historiques. Cette influence se retrouve maintenant au niveau d'instances supranationales, comme la Commission Européenne.

Pour sortir d'un cadre parfois jugé trop européen, l'évolution du GSM en 3ème génération est spécifiée au 3rd Generation Partnership Project (3GPP) qui réunit les membres d'organisations régionales ou nationales :

- Américaine (ATIS),
- Chinoise (CCSA),
- Japonaises (ARIB et TTA),
- Coréenne (TTC),
- Européenne (ETSI).

Cette dimension permet de construire un consensus mondial en préservant les fiertés régionales. Les partenaires formant le 3GPP transposent au niveau régional les résultats du consensus international. Si certains regrettent la lourdeur du système qui en découle d'autres en jouent. Dans certains cas, intégrer un changement dans les spécifications peut prendre au mieux des mois, des fois des années. C'est le prix du consensus au sein des organisations ouvertes à tous les acteurs de la téléphonie mobile. Il arrive aussi que ce consensus soit impossible à atteindre et que le standard échoue à définir une seule implémentation, laissant à plusieurs options la possibilité de s'imposer sur le marché.

Une prolifération de forums …

A côté de la standardisation « institutionnelle », des forums d'industriels se sont créés pour développer des solutions hors cadre de la standardisation ou pour accélérer la spécification, géné-

ralement en réunissant des acteurs aux intérêts convergents et entre lesquels il est plus naturel de collaborer. Il s'agit parfois de mettre en place un cadre qui donne l'apparence du consensus alors que le but est de s'en affranchir. Il peut s'agir d'associations d'industriels aux métiers proches, voire identiques (ex. GSM Association qui regroupe les opérateurs) ou de forums focalisés sur une problématique (ex. Wireless Village sur la messagerie instantanée en son temps).
L'enthousiasme un peu euphorique, et l'investissement tous azimuts ont fait les beaux jours de ces organisations qui n'ont pas toutes survécues au retour à des considérations plus rationnelles et aux exercices de priorisation budgétaires liés à la contraction économique post-2000. Une sorte de ruée vers l'or en quelque sorte dont seuls ceux bénéficiant d'une véritable légitimité sortent renforcés. Lutte insensée entre les forums qui défendent leurs solutions, au dépends parfois du déploiement d'une solution voire au profit de l'émergence de solutions propriétaires.

Standardisation, une fin, mais aussi un moyen

La propriété intellectuelle et industrielle est au cœur des initiatives de standardisation. Un industriel ne se lance dans de tels travaux qu'avec l'espoir d'y influencer la sélection de solution techniques basées sur les brevets qui lui sont les plus favorables (idéalement les siens!) afin de limiter les coûts de licences nécessaires à l'implémentation de ses produits ou mieux de générer un revenu lié à son portefeuille de brevets. Etrangement, le revenu de licence pour Microsoft est aujourd'hui supérieur sur un produit Android à celui dégagé par son équivalent Windows Phone.

Bien souvent, les acteurs impliqués disposent chacun d'arguments à faire valoir lors de négociations liées à la propriété industrielle. C'est sur un constat d'équilibre des forces que se basent notamment les accords de licences croisées. Cet équilibre est fragile et peut représenter une barrière infranchissable à l'entrée pour un nouvel acteur. Un rôle de l'organisme de standardisation est également de fournir un cadre clair quant à l'utilisation de technologies brevetées dans les standards (par exemple, un organisme peut ériger en exigence de base l'attribution de licences à coût raisonnable et sans discrimination). Le standard est ainsi également perçu par les différents acteurs comme un environnement où le risque est limité : les solutions techniques pourront être mises en œuvre dans un cadre borné; en d'autres termes, «on sait où on met les pieds».

Pour les entreprises, la participation aux travaux de standardisation est aussi gage de visibilité, d'une certaine rentabilité et de lobbying. Nombre de sociétés développent des structures au sein de leur R&D dont les membres ont pour objectifs d'occuper des rôles officiels au sein des comités, d'offrir une meilleure visibilité pour l'entreprise (innovante) et de déposer des brevets essentiels. On s'est éloigné de l'image du lieu de collaboration que la standardisation était dans les années 1980-1990. Le contexte économique incertain et une concurrence féroce sont passés par là.

Le renouveau des standards de facto

La puissance de certains géants de l'Internet a donné lieu à plusieurs initiatives d'envergure et au destin plus ou moins heureux. On pense évidemment d'abord à Google et à sa plateforme Android ou à Microsoft et Windows Phone. Le premier choisit une approche business de l'open source alors que le second propose la licence gratuite (pour les écrans de moins de 9 pouces). Dans les deux cas, le modèle économique n'est pas directement lié à la valorisation de la plateforme, mais plutôt à sa certification, l'utilisation d'une marque ou d'applications liées et payantes. Le standard de facto est avant tout l'illustration de la force de la loi de l'offre et de la demande, surtout lorsque certains acteurs maîtrisent bien le pilotage de cette demande. La visée monopolistique n'est jamais loin, soulevant la question de l'adhésion d'autres industriels à ce standard de facto. En effet ces derniers devront passer de la position de partenaire ou supporteur de la solution à celle de concurrent de son promoteur. Certains pensent donc à se protéger:

- Samsung par exemple tient à faire vivre son initiative Tizen qui lui permet autant de conserver une alternative à Android que de mettre un pied dans l'arène (non sans difficultés car la société peine à trouver du support chez les autres industriels).
- Afin d'éviter l'écueil du partenaire-concurrent, Google a choisi de revendre Motorola Mobility une fois le portefeuille de brevets récupéré.
- Microsoft peine à trouver des industriels ayant l'intention d'utiliser son système et tente de faire du rachat de la branche mobile de Nokia un catalyseur de l'adoption de Windows Phone.
- Apple s'est affranchi de cette problématique en n'accordant pas de licence pour iOS mais en développant un écosystème d'accessoires certifiés.

Interopérabilité et standard, un couple pérenne

L'interopérabilité est plus que jamais un impératif incontournable des technologies de mobilité. La standardisation conserve son statut de vecteur privilégié pour atteindre ce but. Les acteurs du domaine en ont pleine conscience et maintiennent leur investissement dans le standard, mais en tenant à maîtriser les coûts liés. Ils réduisent à cet effet le nombre d'organismes dont ils sont membres ou poussent ces derniers dans une démarche de consolidation.
Même si l'état d'esprit a changé, la standardisation reste basée sur la recherche du consensus. Ce dernier conserve toute sa valeur et son caractère d'impulsion pour une technologie, quand bien même il aurait été plus difficile à obtenir qu'auparavant.

L'AUTEUR

Paul JOLIVET (1995) est Directeur Recherche et Standards en Europe de LG Electronics (téléphones mobiles). Son champ d'action est principalement l'innovation et la standardisation. Il est Président du 3GPP CT WG6 (Applications carte à puce) et de l'ETSI SCP TEC (Spécification de la plateforme carte à puce multi applicative). Il enseigne régulièrement dans plusieurs Ecoles dont Télécom ParisTech et Télécom Bretagne. Il étudie par ailleurs à l'Université Paris Dauphine dans le cadre d'un Doctorate of Business Administration sur le domaine de l'Innovation.

Les nouveaux services pour développer l'usage des transports publics

Par Francis SYKES (1989)

La mobilité est au cœur des enjeux économiques et sociétaux des collectivités territoriales. Si les projets d'infrastructures de transport sont fondamentaux, ceux-ci doivent être complétés par des services facilitant l'adoption des moyens de transports par le public.
Le bus et les transports en commun présentent une apparente complexité qui pousse parfois les voyageurs, notamment occasionnels, à envisager des alternatives. C'est pour que cette complexité s'estompe et pour que les voyageurs « osent » les transports publics que se sont développées des panoplies de services permettant de franchir cet obstacle.
Pour être plus proches des voyageurs, ces services peuvent être accessibles sur le lieu de travail, à domicile, ou encore en situation d'itinérance profitant de moments d'oisiveté forcée. Ils reposent souvent sur l'utilisation d'objets personnels tels que smartphones, ordinateurs/tablettes ou cartes bancaires que les voyageurs utilisent déjà pour accéder à des nouveaux services.
Le développement de tels services répond souvent aussi à des enjeux économiques.

Tag RFID et bus - © - RATP - Bruno Marguerite

Ainsi, si déployer des écrans d'information voyageur est généralement reconnu comme justifié là où la fréquentation des transports est la plus forte, c'est rarement le cas des lignes secondaires. L'emploi de smartphones permet de répondre à ce besoin : certains opérateurs équipent les points d'arrêt moins fréquentés de tags NFC, petites étiquettes dotées d'une puce et d'une antenne RFID. A l'aide de leur smartphone NFC, les voyageurs peuvent scanner le tag et ainsi accéder facilement aux informations relatives au point d'arrêt (prochains horaires de passage etc.). Cette solution est de plus en plus pertinente, la majorité des nouveaux smartphones étant compatibles avec la norme NFC.
L'application mobile RATP sur smartphone répond à la même logique. Elle permet de disposer partout et à tout moment d'informations relatives au transport, notamment horaires, calculs d'itinéraires et informations en cas de perturbation.

Dans le même esprit et toujours pour optimiser les coûts d'investissement et de maintenance des infrastructures, une solution permettant d'acheter et valider un titre de transport à bord d'un bus a été expérimentée. Le bus n'est équipé que d'un simple tag NFC. Une application pour smartphone per-

met de scanner le tag, ce qui génère une transaction permettant l'achat et la validation en ligne.

Faciliter l'usage des transports publics

Les téléservices consistent à accéder à distance à des services tels que le rechargement d'un titre de transport sur Internet, sur téléphone NFC ou encore sur automate bancaire.
Pour le voyageur, ceci permet d'effectuer ces opérations n'importe où et n'importe quand. Pour l'opérateur ou l'autorité de transport, cela permet de soulager le réseau de vente et de gestion matérielle des titres de transport en profitant d'un réseau tiers, réduisant ainsi les coûts d'investissement et de maintenance.

Ces services ont pu voir le jour grâce à l'essor des smartphones communicants, à l'amélioration de la couverture 3G-4G et aux nouvelles architectures de sécurité permettant les transactions financières à partir de ces plateformes.

Des cartes bancaires comme sésame des transports

Le *Future Ticketing Project* de Londres repose sur l'utilisation des nouvelles cartes bancaires sans contact, conformes au standard EMV Contactless, basé sur la norme ISO14443 initialement déployée dans le domaine des transports. Les appareils valideurs s'assurent que la carte est valable puis envoient les informations de validation vers un système central. Ce dernier effectue les opérations de rapprochement et débite le prix du voyage. Ceci représente de nombreux avantages tant pour l'utilisateur que pour l'opérateur. D'une part, le voyageur n'a plus besoin d'acheter un titre de transport ni de support de titre de transport, sa carte bancaire en faisant office. D'autre part, l'opérateur ne gère pas les cartes bancaires RFID de ses clients, ce qui se traduit par une diminution très significative des coûts de gestion.
Enfin, cette solution permet d'adapter aisément la tarification.

Multimodalité

La barrière psychologique qui freine l'usage des transports publics est d'autant plus haute que le voyage est complexe. Si de nombreux citoyens sont prêts à effectuer un trajet en utilisant un mode de transport unique, la combinaison de modes rebute. C'est pour cela que l'information multi-modale est devenue la priorité pour de nombreuses autorités organisatrices, ce qui a donné lieu à l'émergence des centrales de mobilité. Ces dispositifs permettent de fusionner les informations provenant de plusieurs transporteurs et de les rendre accessibles aux voyageurs, notamment pour leur permettre de planifier un voyage impliquant plusieurs modes ou plusieurs opérateurs.

Zenway, l'écran tactile multiservice de proximité - © - RATP - ING - Isabelle Bonnet

Concilier transports publics et transports individuels

De nombreux voyageurs optent pour les transports individuels (voiture, moto etc.) soit parce qu'ils ignorent les offres alternatives de transport public, soit parce que l'utilisation exclusive des transports publics n'est pas adaptée à leurs besoins.

L'usage combiné des modes de transports publics et individuels favorisé par l'émergence des parcs relais reste encore peu développé. Aujourd'hui, il n'existe pas d'outil pour réguler l'écosystème que constitue l'ensemble des moyens de transports publics ou individuels. C'est l'ambition du consortium européen *Mov'In Cities* piloté par Ixxi.
Le développement des transports publics s'accompagne d'une nouvelle génération d'outils personnalisés visant à en faciliter l'usage et à les rendre attractifs au plus grand nombre. Cette large panoplie d'outils repose sur des technologies nouvelles et, dans la plupart des cas, s'appuie sur des objets communicants chers aux voyageurs, ce qui d'une part en facilite l'appropriation et d'autre part réduit les coûts des opérateurs et autorités de transport, critère essentiel en ces temps de rigueur budgétaire. ▮

Tag R

L'AUTEUR

Francis SYKES (1989) et (X84). Après un poste de recherche appliquée en traitement d'images, il participe à la grande aventure du GSM, d'abord à la direction technique SAGEM puis à la direction de la stratégie Alcatel où il était chargé de la stratégie Internet Mobile. Il rejoint la RATP en 2003 où il devient responsable de l'ingénierie de Navigo pour la RATP. Il rejoint la direction commerciale d'Ixxi en 2013. Ixxi, filiale de la RATP, conçoit, construit et opère des solutions et services innovants qui facilitent la mobilité urbaine et optimisent l'expérience voyageur, avant, pendant et jusqu'à l'aboutissement du voyage.

« Notre vocation est d'aider nos clients à transformer leur vision en résultats »

ICME est un cabinet international de conseil en stratégie et en management, spécialisé dans le secteur des Télécom et Media.

Rencontre avec Denis Lebrec, CEO du groupe.

Quels sont les secteurs d'intervention d'ICME?

Nos interventions auprès des opérateurs télécom, MVNO, FAI, équipementiers, opérateurs de Pay-TV,… couvrent 4 domaines :

• **Stratégie**

Nous assistons nos clients dans la définition de leurs stratégies : stratégies marketing et commerciales, stratégie de services, stratégie d'évolutions technologiques Réseau & IT. Ces interventions donnent lieu à des projets de déploiement de la stratégie par métiers et grandes fonctions (Balanced Scorecard). Nous avons ainsi récemment mis en place un pilotage stratégique pour un opérateur télécom, calé sur le plan stratégique à 5 ans.

• **Croissance**

Nous aidons nos clients à augmenter leur base clients et leurs revenus, en cadrant les initiatives de croissance, en développant de nouveaux produits et services, en pilotant le lancement de nouvelles offres, en mobilisant leur réseau de distribution (direct, indirect, web). Nous venons de terminer avec succès la mise en œuvre d'un programme de reconquête commerciale visant à faire croître significativement les revenus et améliorer la marge brute d'un opérateur mobile.

• **Excellence Opérationnelle**

Il s'agit d'adapter les organisations de nos clients (Marketing, Ventes, Services clients, Technologie, …) aux enjeux marché et aux meilleures pratiques. Nous menons actuellement la réorganisation d'une Direction Technique d'un opérateur télécom, selon le modèle Think/Build/Run. Il s'agit également de les aider à fluidifier les parcours clients (Acquisition, Commande-Livraison, Facturation-Recouvrement, SAV, …). Il s'agit enfin de les accompagner pour améliorer l'Expérience Clients dans tous les points de contact.

• **Programme Delivery**

Nous assistons nos clients dans la conduite de leurs programmes et projets, en garantissant les délais, la qualité de service et les coûts, grâce à notre large expérience en program management et PMO. Nous pilotons actuellement de grands programmes de transformation, mis en place soit en raison d'évolutions technologiques majeures (3G, LTE, …), de recherche d'améliorations opérationnelles (réduction des opex, …) ou de nouvelles orientations stratégiques (rebranding, stratégie de services, …).

Quels sont les 3 axes majeurs de la stratégie de développement d'ICME?

• **Focalisation sectorielle**

Nous nous concentrons sur 4 industries qui font face à des changements majeurs dans les marchés matures et stimulent le développement économique dans les marchés émergents: Energie&Utilités, Real Estate&Infrastructure, Santé, Télécom&Media. ICME dispose ainsi d'une connaissance approfondie du secteur Télécom & Media, appuyée sur une forte expertise fonctionnelle.

• **Positionnement différencié sur l'implémentation**

Notre focalisation s'accompagne d'un positionnement différencié auprès de nos clients. Nous sommes « hands-on » et résolument orientés vers l'implémentation, grâce à la très grande séniorité de nos consultants qui sont issus pour la plupart de l'industrie et disposent d'une expérience solide du conseil.

• **Présence mondiale à partir de « hubs » régionaux**

Pour accompagner nos clients, la stratégie ICME est d'offrir une présence mondiale, à partir de certains pays clés. D'origine Suisse, ICME s'est tout d'abord déployé en Europe (Berlin, Munich, Paris, Zurich), puis au Moyen-Orient (Abu Dhabi, Dubaï et Riyad) et enfin aux US (Chicago).

Quels types de profil recrutez-vous?

Nous recherchons des consultants curieux, autonomes, prêts à s'impliquer dans la réalisation opérationnelle. Ils doivent être capables d'accompagner nos clients jusqu'à la mise en œuvre, de créer de la transversalité et de déployer une véritable pédagogie du changement. Ces consultants doivent enfin être « internationaux » et ouverts à des missions à l'étranger.

Télécommunications mobiles
des acteurs pris dans des modèles d'affaires mouvants

Par Paul JOLIVET (1995)

Dans un domaine où les modèles d'affaires semblaient bien assis, l'arrivée du modèle low-cost et l'extension des usages de la mobilité bousculent les habitudes et pourraient changer durablement le paysage.

Un modèle économique historique

L'opérateur de télécommunications est l'entité qui gère d'une part l'accès à un réseau, ce réseau, et d'autre part une base d'abonnés. Il existe chez les opérateurs deux modèles économiques types :

- l'opérateur (de services) qui au-delà de la gestion du réseau, développe sa valeur ajoutée et sa différence par une gamme de services offerts à ses abonnés ; il propose généralement des offres packagées ;
- le « carrier » au sens américain, qui considère son rôle plus particulièrement centré sur l'offre réseau ; il est plus ouvert à une collaboration avec des fournisseurs de services tiers.

Le modèle européen reste encore très orienté sur le modèle des opérateurs de service. Les terminaux sont majoritairement fournis par les opérateurs à l'utilisateur final. Ils sont vendus packagés et au sein d'offres. Ils sont généralement subventionnés en contrepartie d'un engagement d'abonnement. L'offre de subvention est souvent reconduite à l'issue de la période d'engagement pour limiter le départ des abonnés vers l'opérateur concurrent (ou churn).

L'arrivée du modèle low-cost

Le modèle low-cost tend à se développer dans le domaine des télécommunications mobiles. C'est le cas en France avec Free Mobile. La concurrence avec les opérateurs low-cost change singulièrement la donne. Il devient ainsi plus difficile de disposer par exemple d'une R&D importante ou d'investir sur les technologies futures. C'est d'abord un modèle plus pragmatique et court terme.

Le modèle de la subvention mobile qui a permis aux utilisateurs d'accéder rapidement à d'onéreux terminaux devient coûteux. Il est par ailleurs dénoncé par les associations de consommateurs pour son manque de transparence. Les régulateurs (supra-) nationaux limitent l'engagement lié et poussent à la proposition systématique d'une offre « SIM only » pour faciliter la comparaison. Les autres modèles de distribution de terminaux, parmi lesquels le crédit et la location se heurtent encore souvent à une barrière culturelle d'acceptation.

La subvention mobile recule en Europe : la vente de terminaux packagés par les opérateurs est passée de 80% à 55% en 4 ans. De manière surprenante, les utilisateurs n'en investissent pas moins dans des terminaux haut de gamme. On note par contre clairement un ralentissement du renouvellement des terminaux, de plus de deux ans actuellement à comparer à 20 mois en 2010 (source Fédération Française des Télécommunications).

Les fournisseurs de service s'en mêlent

Les fournisseurs de services tiers tentent d'entrer dans le marché depuis plusieurs années. Une première tentative a été liée au service de télévision mobile. Les diffuseurs historiques ont tenté de fournir une offre parallèle à celle des opérateurs, et c'est l'échec du déploiement massif de la technologie qui a soldé tous partenariats ou tentatives de service indépendant.

L'arrivée des smartphones et des boutiques d'application donne à d'autres fournisseurs de services l'occasion de s'inviter dans les télécommunications. Apple puis Google ont développé un écosystème de services indépendant de l'opérateur mobile. Ces acteurs ont d'abord développé une communauté d'utilisateurs significative pour continuer à leur vendre les terminaux associés (respectivement iPhone ou Android). Ces fournisseurs

de services visent évidemment à prendre une part bien plus importante dans le domaine, visant à gérer directement leurs utilisateurs (abonnés) tendant à reléguer les opérateurs mobiles à un rôle de fournisseur d'accès au réseau.
La bataille est en cours. Les discussions tendues concernant la gestion (mise à jour) à distance de l'abonnement (la carte SIM intégrée, ou l'eUICC) en sont un exemple évident.

De nouveaux usages qui changent la donne

Les télécommunications mobiles offrent un terrain de développement pour un monde connecté. Le téléphone n'est qu'un élément de cet internet des objets (Internet of Things). Un autre élément est le domaine des communications entre machines est vaste, depuis la tablette jusqu'aux modules intégrés à des voitures. C'est par exemple la mise à jour d'informations sur un compteur électrique connecté ou encore l'ordinateur de bord connecté d'un véhicule qui sait appeler les secours de lui-même.
Le modèle change : l'abonné peut être le fournisseur de service ou un gestionnaire de flotte. L'utilisateur final peut ignorer tout de l'opérateur, un changement d'opérateur peut même se faire à son insu et à distance. Ce modèle de télé-administration pourrait glisser vers les téléphones mobiles, on peut imaginer dans le futur l'arrivée de solutions où l'utilisateur change d'opérateur par une simple connexion internet.

Réaction, ajustements, adaptation …

La guerre des prix et des modèles d'affaires s'installe, et les opérateurs historiques doivent s'adapter. La structure des opérateurs historique doit également prendre en compte cette concurrence, passant par des réorganisations parfois importantes. Les offres en lignes se développent autour de marques distinctes : en France Sosh pour Orange, B&You pour Bouygues Télécom ou Red pour SFR. La subvention mobile est en recul pour ne concerner qu'un nombre plus réduit d'offres. Cette réaction et ces ajustements d'offres permettent l'existence d'une offre à bas coût équivalente à celle des opérateurs low-cost. Il n'en reste pas moins des utilisateurs en attente d'un niveau de service ou de relation clientèle plus important et prêts à payer cet avantage. Certains opérateurs continuent dans ce contexte à chercher la différenciation par des services à valeur ajoutée en parallèle des offres à bas coût, c'est l'objet d'ailleurs d'une claire différenciation par les marques.

Un nouveau positionnement service

Le challenge des opérateurs de services est de proposer des services premium dont la qualité et l'intérêt justifie le coût pour l'utilisateur final.
Le développement de nouveaux services est une approche d'un tel positionnement. Il passe de nouveaux services : l'intégration d'un portemonnaie, d'un passe de transport, de télécommandes, etc… La force des opérateurs historique leur permet de négocier avec les partenaires indispensables pour l'implémentation de ces services. Le développement de nouveaux terminaux est également une source de valeur : la montre connectée, l'interaction du téléphone avec son environnement (appareil photo, cartographie, etc.). Dans ces deux domaines, les fournisseurs de services les plus importants (Facebook, Apple, Google, Amazon) investissent massivement présentant une concurrence significative.
Le développement de services de convergence où l'opérateur permet une interaction efficace entre ses offres de téléphonie mobile, de téléphonie fixe, d'internet, de cloud, etc … Ces offres de service demandent le développement d'une stratégie de synergie entre les divisions associées aux différents réseaux. L'offre de service potentielle est importante et implique des partenariats et un investissement de recherche plus à la portée des opérateurs dits historiques.
Un autre axe de développement dans le domaine des services est celui de la relation clientèle et de la qualité de service. Ce domaine est perçu comme un point faible connu des offres dans le domaine des télécommunications. Si certains utilisateurs sont prêts à tolérer une qualité de service moyenne en contrepartie d'un prix réduit, il reste un public pour une offre de service premium.

L'état des changements … et demain ?

Le modèle d'affaire qui s'était établi depuis le lancement de la téléphonie mobile est en mutation.
L'évolution vers un modèle à bas coût comme dans beaucoup d'autres domaines provoque l'arrivée de nouvelles offres et bouscule (parfois met en danger) les acteurs économiques du secteur. L'ensemble des opérateurs se sont aujourd'hui positionnés dans le domaine.
Le modèle de l'opérateur de services n'est pas pour autant voué à disparaître. Il s'adapte à son public et développe sa valeur ajoutée. L'offre de services (et les terminaux associés) vise à devenir plus « premium » et adaptée à des cibles marketing identifiées d'utilisateurs plus exigeants en qualité et garantie de services.
Il n'en reste pas moins que de nouveaux acteurs émergent, principalement fournisseurs de services qui tentent de s'emparer de la valeur aujourd'hui plutôt réservée aux opérateurs de réseaux. Ces sociétés sont souvent déjà puissantes dans le domaine internet et/ou high tech. Elles disposent d'atouts pour s'imposer dans le paysage télécoms.
Les télécommunications mobiles sont actuellement à un tournant qui pourrait provoquer la chute de certains acteurs historiques et verra se développer certaines des sociétés absentes du domaine il y a quelques années. L'adaptation sera probablement brutale. Elle correspond aussi à une évolution des usages et apportera de nouvelles offres de service.

L'auteur tient à remercier Eve HOHMAN, Responsable Marketing Sosh Mobile chez Orange France, pour son aide précieuse à la conception de cet article.

L'AUTEUR

Paul JOLIVET (1995) est Directeur Recherche et Standards en Europe de LG Electronics (téléphones mobiles). Son champ d'action est principalement l'innovation et la standardisation. Il est Président du 3GPP CT WG6 (Applications carte à puce) et de l'ETSI SCP TEC (Spécification de la plateforme carte à puce multi applicative).
Il enseigne régulièrement dans plusieurs Ecoles dont Télécom ParisTech et Télécom Bretagne. Il étudie par ailleurs à l'Université Paris Dauphine dans le cadre d'un Doctorate of Business Administration sur le domaine de l'Innovation.

VOUS COMMUNIQUEZ PLUS PLUS SIMPLEMENT.

Faciliter vos mouvements
Libérer vos échanges
Créer des liens

Des missions qui marquent notre ambition. La communication est notre métier et celui de nos experts qui conçoivent et déploient chaque jour des solutions pour votre entreprise.
Hub One *Telecom* propose des solutions de téléphonie d'entreprise, de transmission de données et de mobilité télécom.
Hub One *Mobility* fournit et intègre des solutions clés en main pour toute la chaîne logistique des entreprises.
Cette convergence d'expertises contribue à vous assurer une longueur d'avance dans un monde plus que jamais en mouvement.

www.hubone.fr

Hub One, GROUPE ***AÉROPORTS DE PARIS***

Hub One
Une connexion d'avance

Un réseau 4G LTE pour les aéroports Et les réseaux critiques & professionnels

Hub One, fournisseur global de services mobiles et télécoms pour les professionnels, et opérateur historique des Aéroports de Paris, a testé les apports de la 4G / LTE pour les usages critiques et professionnels sur l'aéroport de Paris Charles-de-Gaulle.

Rencontre avec Soline Olszanski, Directeur Stratégie & Innovation de Hub One

Pouvez-vous nous décrire rapidement l'expérimentation réalisée ?

Au premier semestre 2014, Hub One a réalisé une expérimentation 4G LTE sur l'aéroport de Roissy Charles-de-Gaulle sur la base d'une autorisation temporaire en 400MHz et 700MHz, en partenariat avec Air France et Aéroports de Paris.

Notre objectif était de valider la promesse technologique du LTE et d'en évaluer les apports dans le domaine des services critiques et professionnels.

Pour ce faire, nous avons analysé plus de 116 scenarii applicatifs aéroportuaires et professionnels, au nombre desquels nous comptons :

- La radio professionnelle dite PMR « Private Mobile Radio »
- Des applications de positionnement et de sécurité
- Des applications de gestion aéroportuaire
- Des échanges entre l'avion et le sol
- Des déploiements tactiques en situation de crise

Nous avons également réalisé plus de 500 tests radio destinés à valider le fonctionnement d'un certain nombre de mécanismes et en particulier le MIMO (doublement des débits) ou la priorisation des flux permettant la mutualisation de la solution entre activités critiques et non critiques.

Vous avez porté les fonctionnalités spécifiques de la Radio Professionnelle sur un réseau 4G LTE ?

Avec nos partenaires, nous avons mis en place une solution de radio professionnelle sur la base de la technologie 4G LTE comprenant un cœur de réseau LTE, une application de radio professionnelle, ainsi que des terminaux durcis et des smartphones du marché.

L'objectif de ce dispositif est de pérenniser les fonctionnalités utilisées dans le cadre des réseaux radio professionnels (appels de groupe, push to talk…) sur un réseau LTE de dernière génération apportant de nouveaux usages à travers les applications haut débit ou la vidéo.

Hub One est la première société européenne à avoir validé en conditions opérationnelles la coexistence sur un même réseau de fonctionnalités de radio professionnelle, mais également de téléphonie, d'échanges de données et de vidéo ; étant entendu que tous ces services sont disponibles sur un terminal unique, qui en fonction des usages sera un smartphone du marché ou un terminal durci.

En quoi la mise en place d'un réseau 4G / LTE professionnel contribue à la sécurité et à la performance des acteurs de l'aéroport ?

L'expérimentation a été conçue comme un pré-déploiement sur une zone de forte activité permettant ainsi de tester les besoins et les usages grandeur réelle.

Ces utilisations ont été testées sur trois zones aux contraintes différentes, représentatives de l'ensemble des environnements aéroportuaires et professionnels :

- une aérogare
- un trieur bagage
- les aires avion et les voies de circulation de l'aéroport

Les résultats obtenus démontrent l'obtention de très haut débit (17Mbps montant, 60Mbps descendant) y compris autour des avions ou dans les zones industrielles telles que le trieur bagage ou les zones au large ; mais également d'excellents temps de réponse et une meilleure continuité de service à l'intérieur de l'avion lui-même.

Du point de vue opérationnel, les dispositifs déployés démontrent la forte contribution de ces nouveaux outils à la performance de l'industrie aéroportuaire à travers la coordination des actions au pied de l'avion (nettoyage, fuel, repas…), les échanges de données haut débit entre l'avion et le sol, mais également en facilitant les travaux de maintenance à distance ou la gestion des crises grâce à la vidéo.

Au final, l'apport de haut débit en mode nominal comme en cas de crise, contribue de façon significative à la performance et à la compétitivité des aéroports et plus généralement de l'industrie française.

Quelles sont les perspectives de mutualisation des réseaux critiques et professionnels ?

Aujourd'hui, de nombreux réseaux critiques et de sécurité sont déployés sur des réseaux privés indépendants les uns des autres. Hub One a démontré la possibilité de mutualiser les infrastructures passives et actives entre plusieurs types d'acteurs critiques et professionnels sur un même réseau privé.

Pour ce faire, nous avons testé la compatibilité électromagnétique et spectrale de l'installation afin de mutualiser les technologies (tetra, 4G) et les acteurs sur une même infrastructure physique. Tout cela en assurant l'étanchéité réelle des réseaux et des flux, et la gestion dynamique des priorités à travers les classes de services.

Ces travaux ont démontré la possibilité d'héberger, en toute sécurité, plusieurs acteurs utilisant des fréquences différentes sur les mêmes infrastructures avec une étanchéité réelle des réseaux. Un élément déterminant pour la cohabitation d'utilisations critiques et professionnelles sur des environnements tels que les aéroports, où la qualité et la continuité de service sont primordiales. Les résultats obtenus permettent d'envisager la migration des réseaux radios existants vers un réseau 4G LTE professionnel à relativement court terme afin de répondre aux besoins d'aujourd'hui et de demain.

A l'heure des villes intelligentes, des magasins digitaux, l'utilisation de réseaux très haut débit pour les services critiques et professionnels ouvre des perspectives qui vont bien au-delà de l'aéroportuaire, en termes d'usages et de modèles économiques.

Le marché de l'Internet Mobile et l'enjeu de la performance

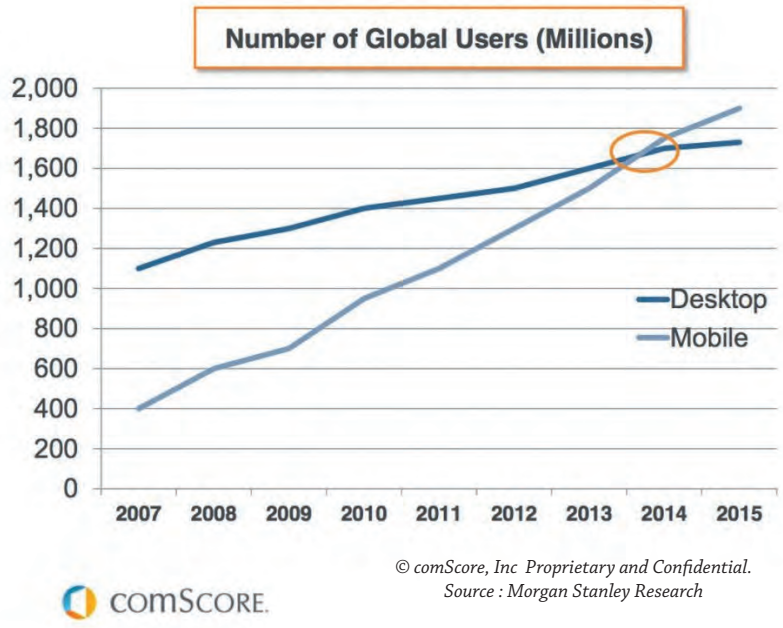
Par Nicolas BABEL (1996)

Dans cet article, je me suis intéressé à la maturité du marché dans l'usage du mobile pour des applications critiques. Après avoir rappelé quelques tendances sur l'Internet mobile, je propose de quantifier la proportion d'applications mobiles pour lesquelles la performance est critique.

L'Internet est devenu mobile en 2014

En janvier 2014, un point de bascule majeur et discret a marqué le monde 2.0 : pour la première fois, l'Internet est majoritairement mobile, dépassant les accès desktop web.

Cet événement s'inscrit dans la continuité de l'explosion de l'Internet mobile depuis la sortie de l'iPhone et la création de l'Open Handset Alliance autour d'Android en 2007. Dans sa phase suivante, l'Internet va se déplacer des desktops vers les tablettes qui deviendront prédominantes même dans l'IT d'entreprise en 2020.



© comScore, Inc Proprietary and Confidential.
Source : Morgan Stanley Research

L'Internet mobile se diversifie également au niveau des équipements d'interfaces utilisateur avec les Objets Connectés, lesquels prendront une place prépondérantes dans nos vies, pour représenter plus de trois fois le nombre d'équipements smartphones, desktops et tablettes combinés. L'Internet mobile devrait atteindre en 2020 plus de 18 milliards d'objets, presque trois par habitant ! Il semble difficile d'imaginer un environnement si différent du nôtre, mais le lancement de l'iWatch en 2014 par Apple confirme cette tendance forte sur les objets connectés devenant nos partenaires quotidiens.

En taille de marché, l'Internet mobile atteindra 700 Mds $ en 2017, soit en répartition suivant le PIB plus de 21 Mds € en France.

Dans ces proportions, l'Internet mobile est déjà critique pour de nombreux secteurs, en commençant par les jeux, les sites marchands, plus récemment la banque et l'épargne et depuis quelques mois les outils pour employés et l'industrie.

Device Type	2013	2014	2015
Traditonal PCs (Desk-Based and Notebook)	296,131	276,221	261,657
Ultramobiles, Premium	21,517	32,251	55,032
PC Market Total	**317,648**	**308,472**	**316,689**
Tablets	206,807	256,308	320,964
Mobile Phones	1,806,964	1,862,766	1,946,456
Other Ultramobiles (Hybrid and Clamshell)	2,981	5,381	7,645
Total	**2,334,400**	**2,432,927**	**2,591,753**

Worldwide Device Shipments by Segment (Thousands of Units) - Source : Gartner (June 2014)

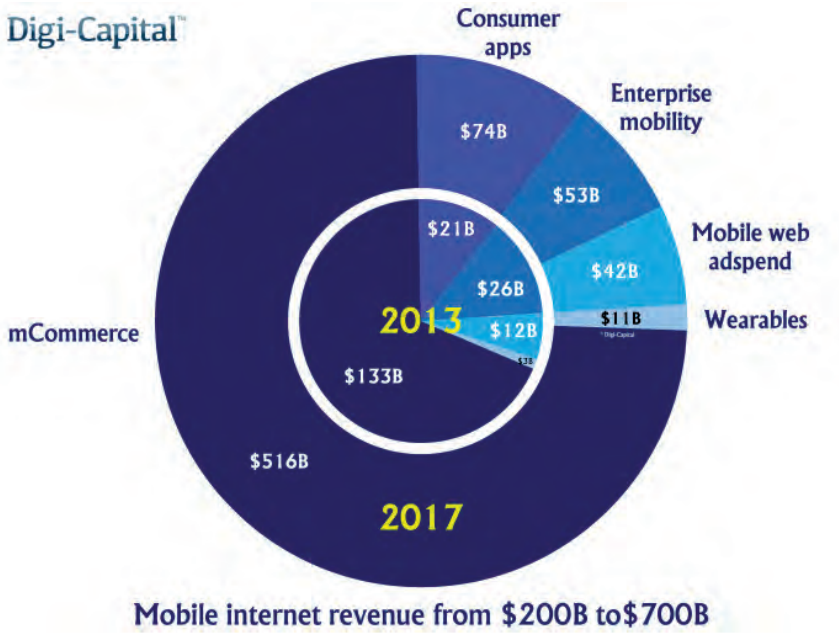
Operating System	2013	2014	2015
Android	898,944	1,168,282	1,370,893
Windows	326,06	333,419	373,694
iOS/Mac OS	236,2	271,115	301,349
Others	873,195	660,112	545,817
Total	**2,334,400**	**2,432,927**	**2,591,753**

Worldwide Device Shipments by Operating System (Thousands of Units) - Shipments include mobile phones, ultramobiles (including tablets) and PCs - Source : Gartner (June 2014)

Nous n'avons plus le temps d'attendre

En faisant référence à nos expériences quotidiennes avec certains sites ou certaines applications, et malgré la domination désormais acquise de l'Internet mobile, nous nous trouvons parfois voire souvent dans une situation émotionnelle forte, mélange de colère et d'impuissance face à l'icône maudite.

Cela nous rappelle à quel point nous sommes devenus dépendants des applications mobiles, mais aussi qu'elles ont modifié notre organisation au point que nous n'avons pas prévu d'alternative à leur utilisation lorsqu'elles ne répondent pas immédiatement. Comment en est-on arrivé là ? Pourquoi nos cerveaux d'ingénieurs n'ont ils toujours pas identifié ce problème ?
Et ce n'est pas un problème de moyens, car les GAFA (Google, Apple, Facebook, Amazon) connaissent les conséquences de ce décrochage de performance : Amazon l'a chiffré à 1% de Chiffre d'Affaires pour 100ms d'attente, et Google à 20% d'abandon de recherche pour chaque demi-seconde de retard.



Source : www.digi-capital.com

Ce problème n'est pas trivial, parce qu'il est à la croisée des télécoms et de l'IT, avec des décideurs dans les lignes de métier, des développeurs rarement internalisés et des équipes IT mises devant le fait accompli.

Déjà vu ?

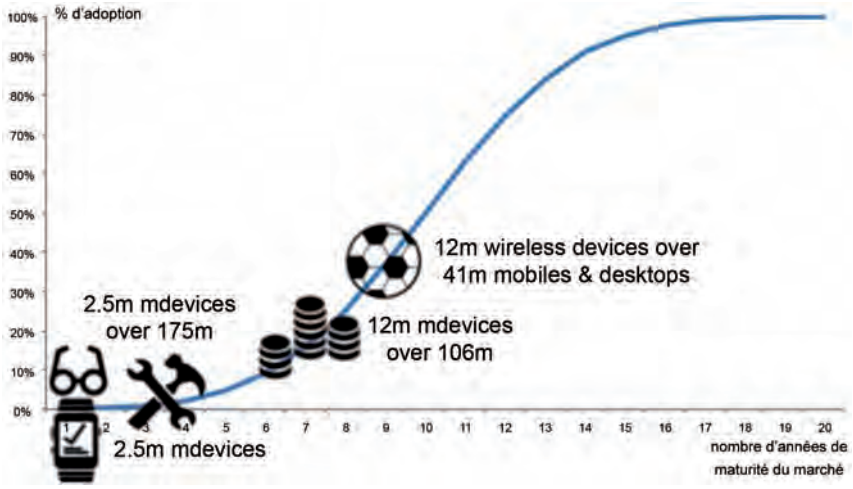
Rassurons-nous, ce problème s'est posé dès la définition du WWW en 1993, la normalisation du problème de performance dix ans après, et la structuration d'un marché de fournisseurs de solutions 15 ans plus tard. La Web Performance Optimization représente désormais une industrie relativement mûre, avec un groupe de fournisseurs de matériels dominé en taille par F5 (10 Mds $ de valorisation boursière), suivi de Riverbed, Radware et le « petit » dernier A10 ; et un autre groupe basé sur le Content Delivery Network, dominé par Akamai (lui aussi dans les 10 Mds $), et suivi par Limelight, Level 3 et autre Internap.

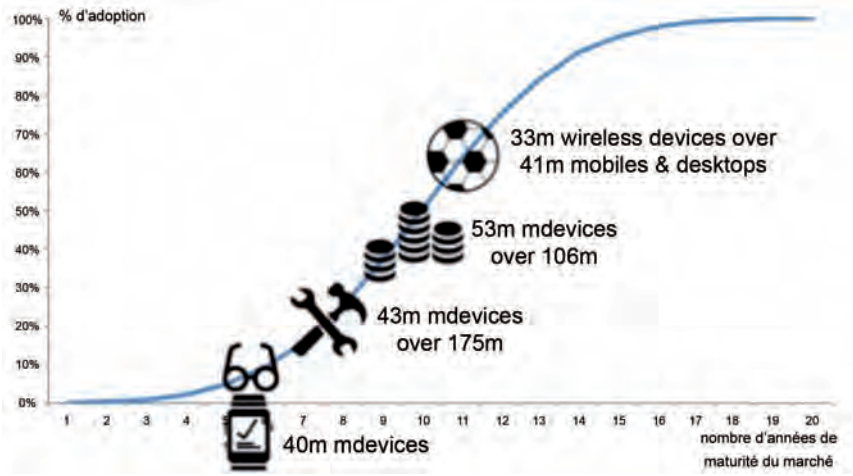
Si nous projetons cette durée de 15 ans pour résoudre ce problème, nous pouvons nous attendre à quelques années de frustrations avec une date de naissance de l'Internet mobile à 2007 (huit ans !).

Les usages les plus sensibles au temps

L'attente reste acceptable dans certaines situations, par exemple si je réserve un billet de train à usage privé sur une application publique une fois par mois. Elle devient inacceptable lorsque le temps représente incontestablement de l'argent : lors de l'accès à un marché fluctuant avec le temps (courtage-épargne, pari en ligne), lorsque la perte de temps implique une perte d'argent (temps des employés de vente ou techniciens de maintenance), ou un risque de perte élevée (ex : retard sur la fermeture d'une valve dans une usine). Entre ces extrêmes résident les applications sensibles à la qualité de l'expérience client : une marque de luxe peut-elle proposer une application lente à ses clients sans entacher sa marque ? D'ailleurs, peut-on envisager une seule application professionnelle de qualité médiocre ? Notre seuil de tolérance diminue à mesure qu'apparaissent des applications aussi rapides que nos réflexes naturels.

Nombre mondial en 2014, d'équipements sans fil par secteur sensible au temps, rapporté au nombre d'utilisateurs en ligne, suivant le modèle de diffusion de technologie de Rogers. Source : Motwin.





Dans la longue lutte pour la performance mobile, les secteurs en pointe sont les secteurs dont le cœur de métier est le plus sensible au temps. Dans ces secteurs (épargne, pari, applications métier), nous constatons que le degré d'adoption du mobile progresse fortement, mais a démarré relativement récemment. Le secteur le plus avancé en adoption semble le pari en ligne avec 30% sur mobiles, suivi par l'épargne en ligne (10%) et moins d'1% pour les applications métier.

Rapporté au nombre actuel d'équipements connectés (sept milliards), la part d'équipements supportant des applications directement sensibles au temps représente moins de 0,5%, ce qui semble cohérent compte tenu des difficultés des réseaux mobiles avec la latence.

En utilisant le même modèle d'adoption de la technologie sur ces secteurs, et en le projetant trois ans en avant, nous pouvons déceler une tendance de forte croissance par rapport au nombre total d'équipements pour atteindre 1% avec 169 millions d'équipements.

Au fur et à mesure que la technologie mobile saura contenir le problème de performance, nous pouvons nous attendre à ce que cette proportion augmente pour se généraliser à l'ensemble des applications B2B et mCommerce dans la fenêtre d'innovation technologique de huit ans.

Ressources :

- Marché France: http://www.atinternet.com/wp-content/uploads/2014/09/Web-traffic-2Q2014.pdf
- IDC & Gartner: http://www.zdnet.com/internet-of-things-market-to-hit-7-1-trillion-by-2020-idc-7000030236/
- Goldman Sachs: http://www.goldmansachs.com/our-thinking/outlook/iot-infographic.html
- Données marché mobile sportif Arjel & cas Betclic : http://pro.01net.com/editorial/607932/le-pari-gagnant-de-betclic-sur-les-appareils-mobiles/
- Rogers Technology Diffusion Model: https://www.uni-hohenheim.de/uploads/tx_uniscripts/25720/A7020_KIM_2011.pdf#page=37

L'AUTEUR

Nicolas BABEL (1996), Directeur Commercial et Marketing, Motwin. Motwin est un éditeur français d'APIs temps réel sécurisées pour une expérience utilisateur haut de gamme et multi-channel : mobiles, tablettes, web et objets connectés. Au préalable, Nicolas a travaillé comme consultant ERP chez PricewaterhouseCoopers, consultant en stratégie pour Monitor, directeur du développement pour Neopost France. Nicolas est Ingénieur Télécom ParisTech et titulaire d'un DESS de gestion Paris Dauphine.

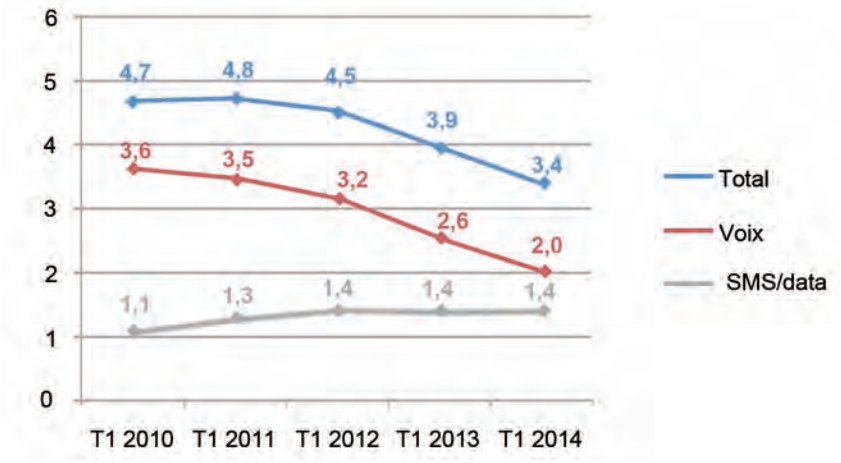
Et si les MVNO sauvaient les Télécoms ?

Par Philippe SIKORA (2003)

Dans un contexte de consolidation et de besoin d'investissement massif dans les réseaux à très haut débit, les MVNO permettent de financer les déploiements tout en poussant la concurrence et l'innovation.

Le marché mobile français baisse en valeur et explose en volume

Le secteur mobile français traîne une image sulfureuse héritée de la période (trop ?) faste de la décennie 2000, caractérisée par un marché peu concurrentiel, des marges élevées, et une croissance à deux chiffres. Tout le monde sait que la donne a changé depuis l'arrivée d'un quatrième opérateur, mais peu de gens réalisent l'importance de la rupture qui a eu lieu, et ce au plus mauvais moment, alors que les investissements nécessaires au déploiement de la 4G sont maximum.



Evolution des revenus mobiles France entière - Source : ARCEP

L'évolution du chiffre d'affaires du secteur est éloquente : il n'aura fallu que 3 ans pour revenir à la situation qui prévalait 10 ans plus tôt, et le profil de la courbe ne laisse pas espérer une reprise à court terme.

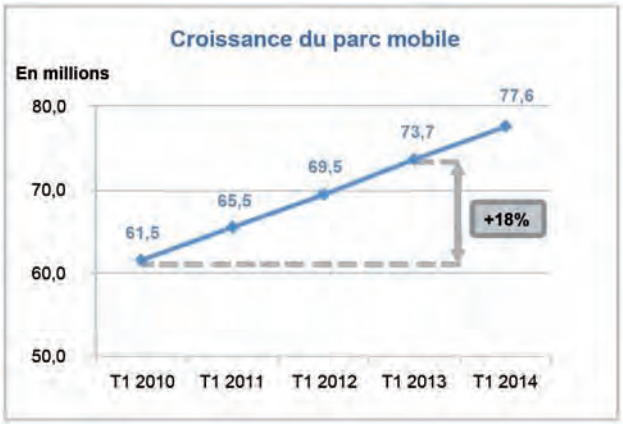
En effet, les revenus de la voix s'effondrent à vue d'œil depuis fin 2010, pratiquement divisés par deux en moins de quatre ans, et les revenus des SMS/MMS sont en baisse. Les revenus de la data ne permettent absolument pas de compenser cette baisse. Ils sont en cours de stabilisation depuis fin 2013 malgré le lancement de la 4G : le seul relai de croissance est au point mort.

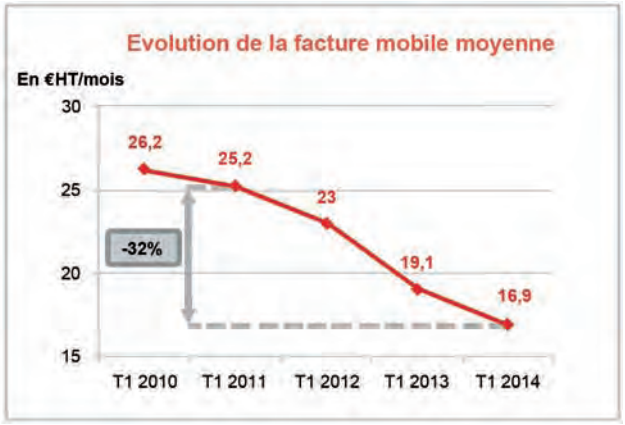
Cette baisse violente des revenus intervient paradoxalement sur un marché extraordinairement dynamique : le parc mobile métropolitain est passé de 42 à 78 millions de lignes en 10 ans, et les usages ont littéralement explosé, en particulier pour la data qui croît de 75% par an depuis 2010. On a consommé plus d'Internet mobile au premier trimestre 2014 que sur toute l'année 2011. Pourtant, la facture moyenne mensuelle par ligne est en chute libre. Elle a perdu pratiquement un tiers de sa valeur en trois ans, passant sous les 17€ au premier trimestre 2014.

Dans le même temps, les opérateurs sont engagés dans une course au déploiement de la 4G. Ainsi, le rythme des investissements du secteur télécom reste au-dessus de sa tendance historique, à plus de sept milliards d'euros par an, sans compter les achats de licences entre 2010 et 2012.

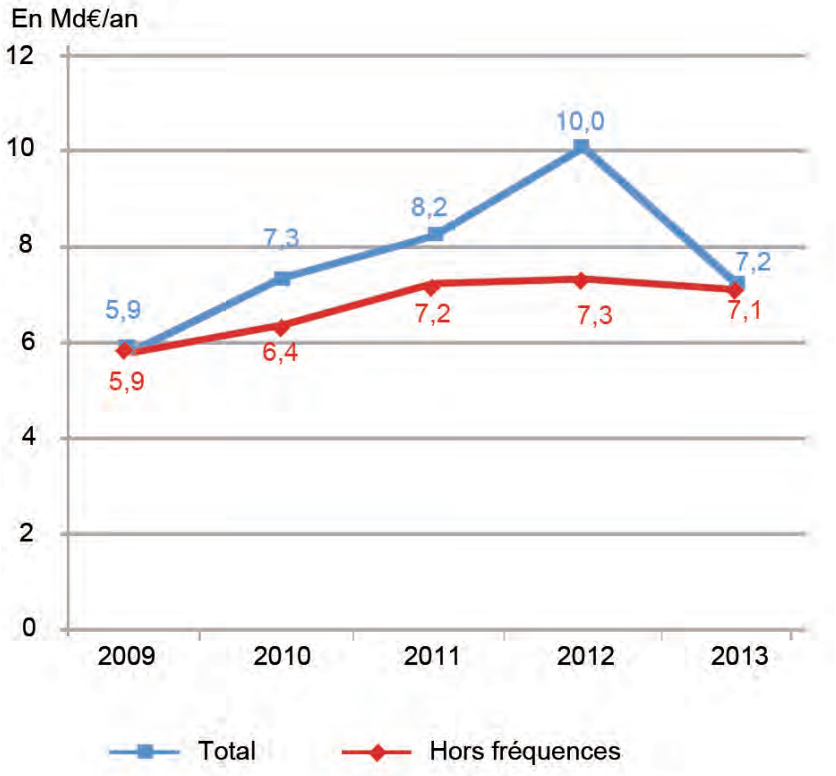
L'industrie des télécoms est par essence intense en capital : les coûts d'un réseau mobile sont importants, et une partie de ces coûts liés à la couverture du territoire ne dépend pas du nombre de clients. Face à ces coûts fixes, les plus petits opérateurs de réseau sont défavorisés.

La conséquence du tarissement des recettes conjuguée à des investissements élevés n'a pas tardé à se faire sentir : la santé financière des opérateurs, autre-





T1 2014, France entière
Source : ARCEP



Investissements des opérateurs de communications électroniques
Source : ARCEP

fois florissante, se dégrade. C'est particulièrement le cas pour le plus petit des opérateurs historiques, Bouygues Telecom, qui a affiché un résultat opérationnel négatif sur le premier semestre 2014 et s'est engagé dans un plan d'économie radical pour revenir à l'équilibre.

Le marché mobile se concentre en Europe … au grand dam des régulateurs

Les difficultés financières des opérateurs ne sont pas un particularisme français. De nombreux pays européens font face à des situations similaires, pour les mêmes raisons : marché mature, coûts d'infrastructure importants et concurrence forte sur le marché de détail dans un marché à 4 acteurs qui conduisent à la nécessité de faire des économies. Or dans une industrie de réseaux, pour réaliser des économies d'échelle, il faut d'une manière ou d'une autre opérer des rapprochements entre acteurs. Ces rapprochements peuvent être plus ou moins importants, depuis l'itinérance jusqu'à la fusion absorption en passant par la mutualisation des réseaux.

Le premier mouvement de rapprochement important a été la fusion d'Orange et T-Mobile au Royaume-Uni avec la création de la joint-venture Everything Everywhere qui opère à présent leurs deux marques.

Trois autres fusions pures et simples ont depuis été menées à bien, en Autriche, en Irlande et en Allemagne, réduisant à chaque fois le nombre d'opérateurs de réseau de quatre à trois.

En France toutes les voies sont expérimentées :

- l'itinérance 2G et 3G de Free sur le réseau d'Orange qui est une forme particulièrement étendue de MVNO ;
- l'accord de mutualisation de réseau entre SFR et Bouygues Telecom qui vont se partager la couverture du territoire en dehors des grandes agglomérations. Sur plus de 90% du territoire, il n'y aura plus qu'un seul réseau là où il y en avait deux auparavant.
- et surtout le possible rachat de Bouygues Telecom. Annoncé comme imminent début 2014, il semble s'éloigner après les déclarations récentes de ses dirigeants. Cependant, tout laisse penser qu'un rachat par les autres acteurs du secteur est inévitable à moyen terme.

Ce mouvement de consolidation est loin d'être terminé puisque début septembre 2014, le troisième opérateur espagnol (Orange) a manifesté son intérêt pour le quatrième (Yoigo). En Norvège, à l'issu du rachat de Télé 2 par Netcom, les deux principaux opérateurs mobiles concentreront 90% du marché.

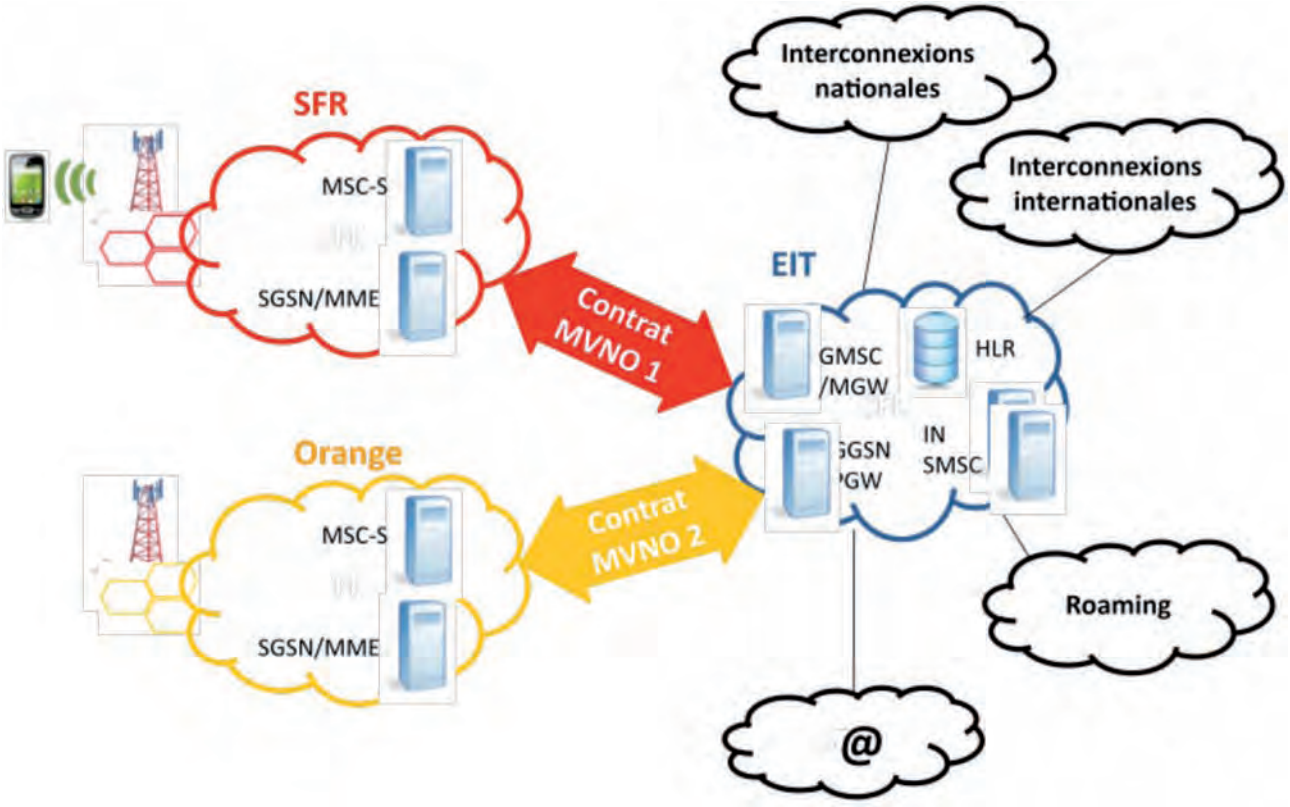


Schéma technique du FULL MVNO EIT raccordé à Orange et SFR
Source : EIT

Partout en Europe, les opérateurs cherchent à réduire les coûts fixes et limiter l'intensité concurrentielle. Les régulateurs sont inquiets et cherchent à maintenir la concurrence, ils se tournent systématiquement vers les MVNO.

Un MVNO est un opérateur mobile dégroupé

Un MVNO (Mobile Virtual Network Operator, ou Opérateur de Réseau Mobile Virtuel) est un opérateur qui n'a pas fait l'acquisition d'une licence l'autorisant à utiliser des bandes de fréquences pour développer un réseau de téléphonie mobile. Il bâtit des offres de téléphonie mobile destinées au marché de détail en achetant les prestations nécessaires à l'un des opérateurs disposant d'une telle autorisation (Orange, SFR, Bouygues Telecom et – théoriquement - Free Mobile) que l'on appelle MNO ou « opérateurs hôtes ». Un MVNO peut également vendre sur le marché de gros à d'autres MVNO, on parle alors de MVNE ou MVNO Enabler.

Le terme virtuel est tout ce qu'il y a de plus impropre. Il n'y a rien de virtuel dans un MVNO, le réseau mobile qu'il utilise existe bel et bien. Il faudrait plutôt parler de réseau mobile dégroupé, exactement comme cela se passe dans le fixe.

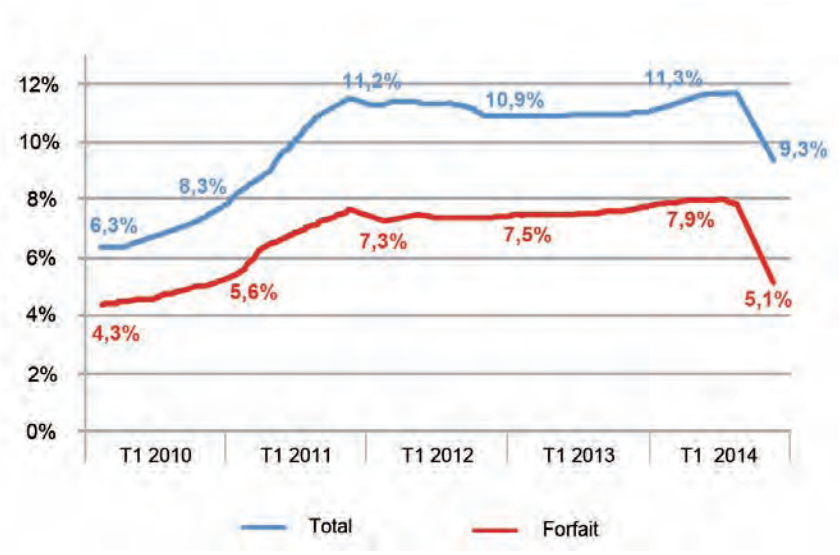
En pratique, il existe une multitude de « niveaux de dégroupage » pour un MVNO, depuis le light MVNO, qui n'a pas du tout d'équipement réseau, jusqu'au FULL MVNO qui possède un cœur de réseau complet.

Le light MVNO se contente d'acheter des lignes en gros à son opérateur hôte et de facturer ses clients sur la base des tickets de taxes que lui envoie ce dernier. C'est bien un opérateur qui conçoit ses offres, active et suspend des lignes grâce aux interfaces mises à sa disposition, gère sa relation client, recouvre ses impayés. Il peut même produire ses propres cartes SIM (compatibles avec le réseau de l'opérateur hôte) et être attributaire de ses propres numéros. Du point de vue du client final, la qualité du service télécom est équivalente à celle de l'opérateur hôte.

Le FULL MVNO, est un opérateur d'infrastructure, avec un « cœur de réseau » à lui. Il loue le réseau radio d'un opérateur hôte, exactement comme un opérateur fixe loue la boucle locale cuivre de France Télécom. Un FULL MVNO peut se raccorder à plusieurs opérateurs hôte, sous réserve de trouver un accord commercial avec ceux-ci.

Dans la configuration la plus étendue, le FULL MVNO possède donc le HLR, l'IN, la commutation et le GGSN, ainsi que toutes les plateformes de services (SMS, MMS, messagerie...). Il gère toutes ses interconnexions nationales et internationales, la fourniture de services à valeur ajoutée, le roaming, l'accès à Internet. Bâtir un FULL MVNO est un investissement lourd qui se compte en dizaines de millions d'euros, mais permet une forte indépendance vis-à-vis du ou des opérateur(s) hôte(s). En effet, le FULL MVNO peut faire passer ses clients d'un réseau radio à l'autre par une simple opération de paramétrage, sans changement de carte SIM ni portabilité.

Alors que la dynamique des MVNO était bonne jusqu'à fin 2011, la croissance s'est arrêtée lors de l'arrivée de Free au T1 2012. Sur le marché postpayé, celui qui a la plus forte valeur, la part de marché des MVNO a stagné sous le seuil des 8%. Sur le marché total, en incluant



Part de marché des MVNO en métropole - Sources : ARCEP, projection EI Telecom

également les clients prépayés qui génèrent des revenus nettement plus faibles, la part de marché des MVNO s'est stabilisée autour de 11%.

D'ici fin 2014, deux MVNO importants vont « disparaître » : d'une part Numéricable a absorbé SFR ce qui va entraîner l'absorption des 200 000 clients forfaits du MVNO de Numéricable, et d'autre part Virgin Mobile, avec environ 1,7 million de clients dont 1,3 million de forfaits a été racheté par SFR/Numéricable. Ainsi, la part de marché des MVNO sur le marché des forfaits va-t-elle passer brutalement de 8% à 5%. Encore ce chiffre est-il à manipuler avec précaution, le MVNO la Poste étant contrôlé à 49% par SFR. Les MVNO « indépendants des opérateurs hôtes » ne compteront alors plus que 2,3 millions de clients forfaits soit une part de marché de 4%. Ainsi, EI Telecom, le MVNO du groupe Crédit Mutuel-CIC avec 1,3 million de clients forfaits pèsera à lui seul 56% de ce parc.

Le modèle économique des MVNO n'est pas pour autant voué à disparaître. La situation actuelle en France relève de la succession de deux périodes :

- **Un marché mobile trop peu concurrentiel** (tant en gros qu'en détail) de 2005 à 2011, qui a limité le marché adressable, notamment parce que les MVNO n'avaient pas les moyens de faire des offres compétitives de forfait avec abondance, et que les consommateurs étaient engagés auprès de leur opérateur.
- **Un marché de détail trop concurrentiel** par rapport au marché de gros depuis 2012. Alors que les prix de vente au consommateur final baissaient rapidement, le marché de gros des minutes et de la data n'a pas suivi assez rapidement.

Il convient à présent de redresser la situation car les MVNO sont appelés à jouer un rôle important.

Le défi de la régulation résolu par les MVNO

On l'a vu, le marché baisse en valeur et tend à se concentrer car il est trop couteux de multiplier le nombre de boucles locales. Les pouvoirs publics doivent donc compenser la baisse d'intensité concurrentielle induite par les concentrations, en mettant en place une autre forme de concurrence qui soit efficace. La seule solution consiste à développer des concurrents agiles et innovants. Les FULL MVNO sont l'instrument idéal pour animer durablement le marché d'un point de vue concurrentiel à condition qu'on leur en donne les moyens. C'est d'ailleurs la solution adoptée par les régulateurs lors des fusions récentes, en Autriche, en Irlande et en Allemagne. Les fusions n'ont été accordées qu'à condition que la nouvelle entité propose des conditions d'accueil à des MVNO de façon à assurer une saine concurrence.

D'une part, les MVNO contribuent très largement au financement des réseaux mobiles qu'ils louent. Selon Alternative Mobile à fin 2012, 1,6 Md€ avaient été transférés aux MNO français, soit plus de 2 Md€ à l'heure actuelle – un montant supérieur au prix convenu entre Bouygues Telecom et Free pour la cession du réseau et des fréquences de Bouygues Telecom lors de la tentative de rachat de SFR début 2014.

D'autre part, les FULL MVNO sont particulièrement efficaces pour animer la concurrence et favoriser l'innovation :

- Les MVNO ont une structure de coût légère par rapport à un déploiement de réseau radio national.
- Ils évitent le problème de doublon de couverture sur la boucle locale dans les zones non denses et sont capables de monétiser les surcapacités des réseaux des opérateurs hôtes.
- Ils permettent d'adresser des niches de marché non adressées par les opérateurs historiques.
- Les nouveaux entrants sont par nature plus réactifs et plus innovants que les opérateurs installés.
- Ils peuvent jouer le rôle d'agrégateurs de trafic pour d'autres acteurs (light MVNO notamment).
- Ils constituent la seule solution pour certaines applications nécessitant une couverture étendue ou une forte résilience (applications de défense, de sécurité) grâce à leur capacité à utiliser plusieurs réseaux radio.

Encore faut-il que les conditions d'accès aux réseaux mobiles soient bonnes par rapport au marché aval. L'évolution récente du secteur en France montre que ce n'est pas encore le cas : toutes les parties prenantes au dossier doivent se convaincre que l'avenir de la téléphonie mobile passe (aussi) par les MVNO.

L'AUTEUR

Philippe SIKORA (2003), est diplômé de l'école Polytechnique et du Politecnico de Turin. Après une expérience au sein du cabinet TERA Consultants et un passage à la Direction des Affaires Economiques et de la Prospective de l'ARCEP, il est à présent Directeur de la Stratégie et du Contrôle Interne de Euro Information Telecom, qui opère notamment les marques NRJ Mobile, Crédit Mutuel Mobile, CIC Mobile et Auchan Mobile.

Quels réseaux pour la radio/télévision numérique en mobilité ?

Par Philippe de CUETOS (2003)

Alors que les projets de TMP et de RNT ont subi des retards importants, la distribution des contenus audiovisuels s'est développée sur les réseaux mobiles haut-débit (3G/4G). Evolution durable ou transition temporaire ?

La radio : premier média audiovisuel mobile

La radio n'est devenue un média mobile qu'après plusieurs décennies d'usage essentiellement fixe, à partir de l'imposant poste de radio installé dans le salon. A partir des années 1960, deux évolutions ont insufflé la mobilité à la radio : l'avènement du transistor, qui a permis de diminuer l'encombrement des postes de réception, et celui de la télévision, dont l'usage croissant par les foyers a amené le média radio à se différencier de son concurrent en programmant des contenus plus adaptés à l'écoute en mobilité. La vieille radio que l'on écoutait chez soi en famille s'est ainsi transformée en un média qui accompagne l'auditeur tout au long de sa journée. Aujourd'hui, l'écoute de la radio – trois heures par jour en moyenne pour plus de huit Français sur dix – est réalisée pour moitié de son volume hors domicile, dont un tiers en voiture[1], encore essentiellement en analogique en modulation de fréquence (FM).

La numérisation plusieurs fois retardée du réseau de diffusion de la radio (RNT)

Le média radio a cherché dès la fin des années 1990 à numériser sa diffusion hertzienne à partir d'un nouveau réseau de diffusion, la radio numérique terrestre (RNT). A l'instar de la TNT pour la numérisation de la télévision, la RNT permet :

- de moderniser le média radio en améliorant la qualité sonore de sa diffusion et en enrichissant les programmes avec des données associées, visuelles et interactives ;
- et, dans un contexte de saturation de la bande FM, de disposer de nouvelles ressources spectra-les permettant la diffusion de nouvelles stations.

La RNT a ainsi déjà été lancée dans plusieurs pays d'Europe, comme au Royaume-Uni ou en Allemagne. En France, après plusieurs années de retard sur le calendrier initial, elle vient tout juste d'être lancée depuis juin 2014 mais, pour le moment, sur trois villes seulement (Paris, Marseille et Nice) et sans la participation des grands groupes de radios nationaux.

En effet, la RNT nécessite le déploiement d'un nouveau réseau de diffusion. Bien que ce nouveau réseau puisse réutiliser une partie des infrastructures existantes et qu'il ait vocation à se substituer à terme au réseau analogique, avant de pouvoir éteindre le signal FM les deux réseaux devront continuer à coexister pendant un temps suffisant pour permettre aux auditeurs de s'équiper en récepteurs numériques. Or, l'étendue importante du parc de récepteurs radio à rendre compatibles avec le numérique (un foyer français possède aujourd'hui en moyenne pas moins de neuf récepteurs de radio, autoradios inclus[2]) laisse présager d'une longue période de double diffusion analogique/numérique, pouvant s'avérer financièrement dissuasive pour certains éditeurs. Pour la télévision, près de sept ans de « *simulcast* » analogique/numérique auront été nécessaires avant le passage au tout numérique fin 2011, mais avec un nombre de récepteurs à adapter plus réduit (moins de deux écrans de télévision par foyer en moyenne) et une convoitise des opérateurs de télécommunications mobiles sur les fréquences utilisées par la télévision – celles issues du « dividende numérique » – qui a sans doute accéléré le processus.

L'échec des premières tentatives visant à apporter la mobilité à la télévision (la TMP)

La télévision mobile personnelle (TMP) promettait de libérer le média télévisuel du téléviseur fixe afin de le rendre davantage mobile. Lancée en 2005-2006 en Corée du Sud, au Japon et aux États-Unis, la TMP a fait l'objet de déploiements commerciaux dans plusieurs pays d'Europe, notamment en Italie, à partir de la norme européenne DVB-H. Mais la plupart de ces services ont été des échecs commerciaux, qui peuvent s'expliquer par l'effet de plusieurs facteurs, dont :

- des coûts élevés liés à la nécessité de

1/ Source : Médiamétrie, « 126 000 Radio » et « L'Année Radio 2012-2013 ».
2/ Source : Observatoire de l'équipement audiovisuel des foyers – 1er semestre 2013

déployer un tout nouveau réseau de diffusion plus adapté à la mobilité que le réseau TNT, sans perspective d'éteindre à terme un réseau plus ancien comme c'est le cas pour la RNT avec le réseau FM ;

- le manque de programmes adaptés à la mobilité (consistant essentiellement à la reprise de chaînes de télévision éditées pour la réception fixe) ;
- l'arrivée de l'internet en mobilité et des *smartphones*, pour la plupart non-compatibles avec les technologies de diffusion de la TMP.

Les premiers téléphones mobiles DVB-H (2006)

Le développement accéléré de l'internet mobile et de son usage pour les médias audiovisuels

L'arrivée du haut-débit mobile avec le déploiement de la 3G à partir de 2004 en Europe, puis le lancement des *smartphones* et des tablettes tactiles aux capacités multimédia avancées (l'*iPhone* en 2007 puis l'iPad en 2010), a permis de développer, en mobilité, les nouveaux usages de consultation des médias audiovisuels déjà apparus sur l'internet fixe : web radios, podcasts, vidéos à la demande, télévision de rattrapage, ...

Les débits médians descendants disponibles sur la 3G sont ainsi passés de moins de 2 Mbit/s en 2008 à 4 voire 10 Mbit/s en 2013 en fonction de l'opérateur[3], tandis que les réseaux 4G (LTE) naissants affichent des débits médians de près de 18 Mbit/s, ce qui est très confortable pour visionner des vidéos même en « Full HD »[4]. Quant aux nouveaux terminaux connectés, leur forte pénétration les rend aujourd'hui incontournables : 26 millions de Français possédaient un *smartphone* en 2013 et 8 millions une tablette[5].

Ainsi, de 2011 à 2014, la consultation de programmes de télévision (en direct et en rattrapage) sur mobiles et tablettes en France est passée de 6 à 49 millions de vidéos vues par mois (ces chiffres incluent le visionnage en wifi et en 3G/4G)[6].

Les limites de l'internet mobile pour la diffusion de contenus audiovisuels

Le haut-débit mobile fait toutefois face à une menace liée à son succès : sous l'effet de la consultation généralisée de contenus vidéo exigeants en débits, l'accroissement des capacités de l'internet mobile pourrait être rapidement compensé par l'accroissement des débits consommés. Le haut-débit mobile est en particulier peu efficace pour diffuser des contenus audiovisuels en mode linéaire tels que la télévision ou la radio en ce qu'il multiplie les transmissions de données avec le nombre d'utilisateurs (mode de transmission dit *unicast* ou *point-à-point*).

Aussi, certains équipementiers promeuvent la mise en place d'une offre « gérée » de distribution de services audiovisuels sur le haut-débit mobile (à l'instar des services IPTV sur le fixe) à partir de la technologie « *LTE Broadcast* »[7] qui permet aux opérateurs d'optimiser la transmission des flux envoyés simultanément à plusieurs usagers d'une même cellule LTE. Cette technologie est toutefois encore peu mature.

De nombreux acteurs de l'audiovisuel continuent de considérer que lorsque la demande en services linéaires mobiles sera forte, des réseaux dédiés tels que la RNT et la TMP resteront plus économiques que le haut-débit mobile actuel ou le LTE Broadcast, tant en quantité de spectre radioélectrique utilisé qu'en coûts opérationnels. En outre, l'utilisation de réseaux dédiés permettra aux éditeurs de continuer à s'auto-distribuer, gardant ainsi le contrôle des conditions économiques et techniques de leur diffusion, et de continuer à proposer un modèle d'accès entièrement gratuit aux services, ce qui reste essentiel en particulier pour les éditeurs du service public.

Quels réseaux pour quels services et quels terminaux ?

Si les réseaux haut-débit mobiles sont peu efficaces pour diffuser des contenus *mass-média*, les réseaux de radiodiffusion comme la RNT ou la TMP demeurent peu adaptés aux nouveaux usages non linéaires (podcasts, vidéo à la demande, ...). Des technologies existent pour pallier les lacunes de chaque type de réseau : pour le haut-débit mobile, le LTE Broadcast et ses prochaines évolutions ; pour la radiodiffusion, des stratégies de pré-stockage de contenus les plus demandés dans les terminaux, qui sont ensuite rendus accessibles à la demande (ce que l'on appelle la « Push VOD »).

Dans le modèle actuel de compétition des réseaux, le haut-débit mobile semble avoir pris l'avantage en raison de l'utilisation généralisée des nouveaux terminaux connectés. Certains acteurs de l'audiovisuel œuvrent cependant pour un modèle de coopération – voire de convergence technique – des deux types de réseau qui pourrait répondre aux différents enjeux à la fois des éditeurs et des opérateurs mobiles. Verra-t-on bientôt arriver la « paix » des réseaux ?

L'AUTEUR

Philippe de CUETOS (2003), est ingénieur en télécommunications (Télécom Bretagne 1999) et titulaire d'un doctorat dans le domaine des réseaux multimédia. Il a participé pendant plusieurs années à la standardisation dans le domaine de la diffusion des médias audiovisuels et à la gestion de projets R&D. Depuis 2010, il intervient dans l'élaboration et la mise en place des politiques publiques de modernisation des médias, d'abord au Ministère de l'industrie puis, aujourd'hui, au Ministère de la culture et de la communication au sein de la Direction générale des médias et des industries culturelles (DGMIC).

3/ Source : Enquête 2014 de l'ARCEP « La qualité des services mobiles en France métropolitaine ».
4/ Selon les paramètres de compression utilisés, une vidéo « Full HD » ou « HD 1080 p » codée en MPEG-4 AVC peut représenter un débit variant entre 7 et 10 Mbit/s.
5/ Source : Médiamétrie « l'année internet 2013 »
6/Source : Centre national du cinéma et de l'image animée (CNC) « l'économie de la télévision de rattrapage en 2013 ».
7/Aussi appelée eMBMS (« evolved - Multimedia Broadcast Multicast Services »)

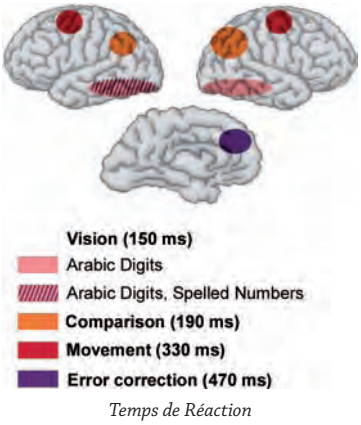
La performance applicative mobile
un problème complexe

Par Eric HORESNYI (1996)

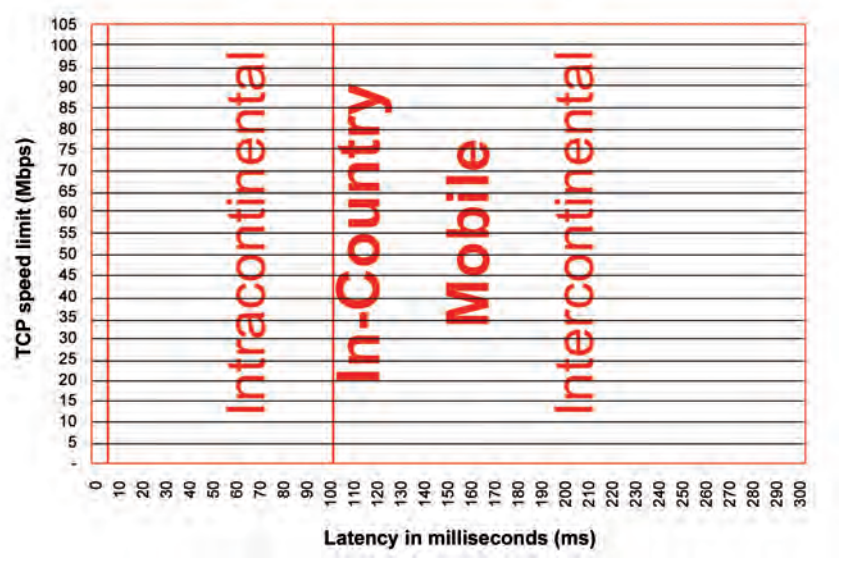
Pourquoi la rapidité est-elle si importante pour nous les humains ?

Lorsqu'elle s'adresse à des machines, la technologie peut imposer encore ses règles internes qui seront respectées. Mais lorsque la technologie sert des humains, nous devons respecter les règles héritées de notre fonctionnement interne. La physiologie, qui étudie le fonctionnement de notre corps à dessein médical, nous apporte des réponses.

Lorsqu'un humain interagit avec son smartphone (ou toute application à travers un objet connecté), il s'investit d'autant plus émotionnellement dans sa relation avec l'application que son comportement lui semble humain. Le temps de réaction humain se situe entre 150 et 470 ms suivant le sens sollicité et le traitement nécessaire. Donc **toute application réagissant avec plus d'une demi-seconde semblera artificielle.**



Temps de Réaction
Source : Public Library of Science



Effect of latency on maximum TCP throughput
Source : http://www.digitalsociety.org/2010/08/conflating-broadband-speed-with-internet-speed-is-misleading/

Google confirme ce chiffre dans ses recommandations aux développeurs, suite aux études continues du comportement des utilisateurs : 500ms est le délai à atteindre pour tout développeur d'application agréable.

Le problème du mobile avec la performance applicative

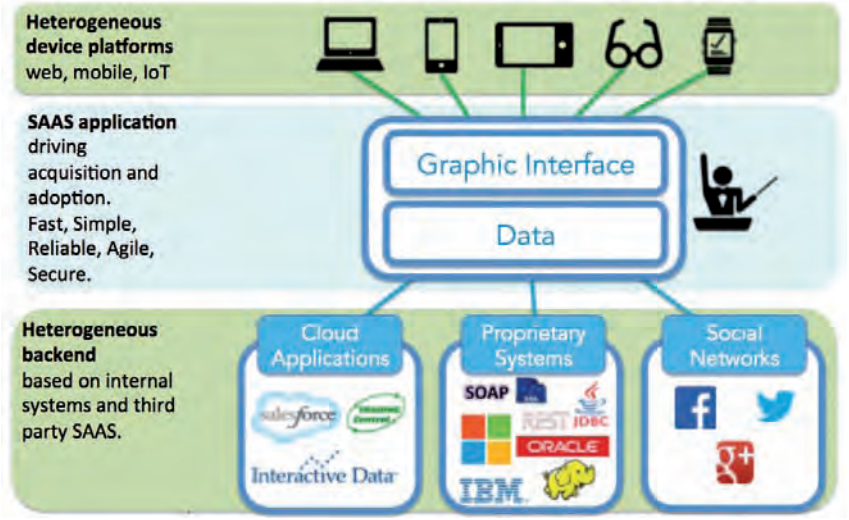
Pour atteindre ce benchmark de 500ms, un développeur sur mobile se retrouve dans une situation bien plus délicate qu'un développeur sur desktop : le temps de latence du sous-jacent réseau actuellement de 1 à 2 ms en réseau fixe, atteint 200ms sur réseau mobile ! Soit un budget temps multiplié par 100 pour la couche réseau.
Ceci ramène un développeur desktop aux années 1990 du web, ou à consulter (sans cache, donc un site très peu utilisé !) un site Chinois ou Indien. Le pire, c'est que ses utilisateurs ne sont plus les êtres patients que nous étions alors, les utilisateurs s'attendent à la même performance que sur le web.

Si nous voulons évaluer l'impact de la latence réseau sur la performance applicative, nous pouvons le résumer dans cette équation :
Latence Applicative pour un contenu affiché =
Nombre d'Applications Sollicitées (richness) x
(Nombre d'Aller-Retour par Application (chattiness) x
Nombre de paquets pour transmettre le volume de données (data volume) x
Latence Aller-Retour (round trip delay)

+Temps de Traitement Applicatif (CPU processing)).
Au delà de l'impact catastrophique d'un facteur réseau (round trip delay) x100 dans cette équation sur la latence applicative, les autres facteurs ne semblent pas aider. En effet, côté richness : avec l'adoption rapide du cloud pour la construction d'applicatifs SAAS, les données proviennent de plus en plus d'une ou plusieurs applications cloud en plus du système propriétaire, sans oublier les réseaux sociaux. Le data volume augmente également avec l'utilisation de plus en plus massive de vidéo, ou de contenus sophistiqués issus du big data, suivant la loi de Moore (doublement tous les 18 mois). Seule la chattiness peut être corrigée par une bonne discipline des développeurs, et le CPU processing suit la loi de Moore (divisé par 2 tous les 18 mois).
La 4G représente un espoir pour le round trip delay (round trip à 100ms), de même que les technologies qui lui succéderont. Malheureusement, l'augmentation de débit offert ne suit pas l'augmentation du volume de sources (richness), et encore moins le nombre de paquets transmis (data volume) qui suivent la Loi de Moore.

Existent-il des solutions pour ceux qui ne peuvent pas attendre ?

Les solutions utilisées pour le web « desktop » (CDN, Matériels, mémoire cache, ...) sont toujours disponibles mais ne suffisent plus face aux particularités du web mobile. Deux types de solutions s'imposent pour réduire, d'un côté, le facteur « richness » avec l'orchestration de données et, de l'autre côté, le facteur « Latence Aller-Retour » avec la confirmation des protocoles de communication bidirectionnelle.
A ce jour, une solution a émergé pour aider les développeurs à affronter ce défi : l'**orchestration de données**. Un agent logiciel représentant l'objet connecté s'insère dans le cloud et en face de l'équipement sans fil. L'agent représente l'objet connecté vis-à-vis des multiples sources cloud avant de n'envoyer à l'objet connecté que les informations essentielles pour sa présentation.
Par ailleurs, cette même architecture initialement prévue pour le sans fil distant traite les problèmes de wifi saturé, ou de bande passante Internet artificiellement faible, par exemple pour les éditeurs SAAS à travers le Great Firewall of China.



Orchestration de Données pour humains connectés. Source : Motwin

Le facteur « latence aller-retour » peut être réduit de moitié en supprimant l'aller (ou le retour !) avec **les protocoles de communication bidirectionnelle.** En reprenant nos cours Réseaux, nous pouvons constater que le protocole HTTP est en mode « Resquest-Answer ». Le mobile, pour avoir une information, doit poser une question au serveur. Ainsi la réactivité supporte le poids du temps de communication aller et retour. Les protocoles de communications bidirectionnelles en revanche permettent de créer un canal (un socket) de communication constant entre le mobile et le serveur. Si le serveur se rend compte qu'une donnée a changé de son côté, il peut pousser de lui-même des informations vers le mobile, sans attendre de question. Le plus connu de ces protocoles est Websocket, normalisé par l'IETF dans la RFC 6455 en 2011. Bien qu'il reste des éléments à spécifier, le protocole connait déjà un grand succès pour les applications les plus sensibles au temps (trading, betting, BtE, jeux à réalité augmentée, ...). L'intégration de plus en plus d'interactivité (chat, réseaux sociaux, news, ...) dans toutes les applications et les pages web forcera les développeurs à mieux maîtriser ce nouveau protocole.
L'orchestration et les protocoles bidirectionnels vont bientôt devenir une évidence pour tous car, non seulement ils permettent de réduire la latence applicative, mais ils luttent également contre le second plus gros ennemis de l'expérience web mobile : le manque de batterie ! En réduisant le nombre de paquet à envoyer et à recevoir, on réduit le besoin en énergie d'une application et on augmente son usage par ses clients ou ses employés. Et qui n'est pas confronté quotidiennement à cette terrible dernière petite barre rouge ?

Ressources :
- Public Library of Science : http://www.ncbi.nlm.nih.gov/pmc/articles/PMC548951/figure/pbio-0030051-g002/
- ENS Lyon : http://acces.ens-lyon.fr/acces/ressources/neurosciences/temps-de-reaction-investigation-variabilite-et-traitements-statistiques-des-donnees/comprendre-1/le-temps-de-reaction-quest-ce-que-cest/

L'AUTEUR

Eric HORESNYI (1996),
CEO, Motwin
Eric dirige Motwin, éditeur français d'APIs temps réel sécurisées pour une expérience utilisateur haut de gamme et multi-channel : mobiles, tablettes, web et objets connectés. Au préalable, Eric a développé la practice Finance de BT en France, les architectures de trading haute fréquence de Radianz aux USA après avoir travaillé comme consultant en performance applicative chez Equant. Eric est Ingénieur Télécom ParisTech 1996 et MBA NYU Stern.

Objets connectés
l'exemple de l'intégration automobile

Par Sophie DIALLO

Dès octobre 2015, le système d'appel d'urgence européen eCall sera opérationnel. Ce système permettant aux véhicules de communiquer en cas d'accident, rendant connectées les voitures par défaut.

De l'eCall à la voiture connectée

L'eCall est un système permettant à une voiture accidentée d'appeler instantanément les services d'urgence tout en envoyant sa position précise, que ses occupants soient conscients ou non, et quel que soit le pays de l'UE dans lequel elle se trouve. Avec l'arrivée de l'Ecall, la connexion des véhicules à un réseau mobile se standardise et demain l'ensemble de ces services ne seront plus uniquement réservés aux véhicules haut de gamme.

L'automobile devient donc un véritable objet communicant. L'enjeu est crucial tant pour les constructeurs automobiles que pour les opérateurs. En effet, pour les premiers cette connectivité permettra d'offrir de nouveaux services et prestations, pour les seconds cela génèrera une nouvelle source de revenus dans un marché qui vit principalement de renouvellement.

Les services envisagés tels que des systèmes de navigation, le divertissement, l'information sont très consommateurs en data. Le coût étant un élément essentiel dans le déploiement de ces nouveaux services, les constructeurs souhaitent pouvoir mettre en concurrence régulièrement les opérateurs.

Dans le modèle actuel, dès la conception, le constructeur automobile choisit un opérateur qui restera en place pendant toute la durée de vie du véhicule. La réalisation de nouveau appel d'offre le durée de vie du véhicule ne sera rendu possible seulement si les ont la liberté de changer d'opérateur durant la vie du véhicule.

Les évolutions de la SIM pour le marché Machine to machine (M2M)

En 2010, l'ETSI a standardisé le principe d'une carte SIM non extractible pour répondre aux contraintes industrielles émises par les constructeurs de modules dédiés au secteur du M2M.

Ces équipements doivent pouvoir supporter des conditions environnementales particulières: chocs, corrosion, températures extrêmes, vibrations ou encore humidité. Les caractéristiques physiques de la carte SIM ont dû être redéfinies.

Aujourd'hui, les cartes SIM sont personnalisées par leur fournisseur imposant au constructeur automobile le choix de l'opérateur pour toute une série de véhicules.

La seule solution aujourd'hui pour changer d'opérateur est de changer physiquement les cartes SIM ; tâche délicate car conditionnée par l'accessibilité et le nombre d'équipements sur lesquels l'intervention doit porter. C'est pourquoi, de nombreux d'industriels ont plaidé pour des procédures d'allocation a posteriori permettant le chargement ou la modification des données d'accès réseau d'un opérateur après installation de la carte SIM dans le module de communication du véhicule.

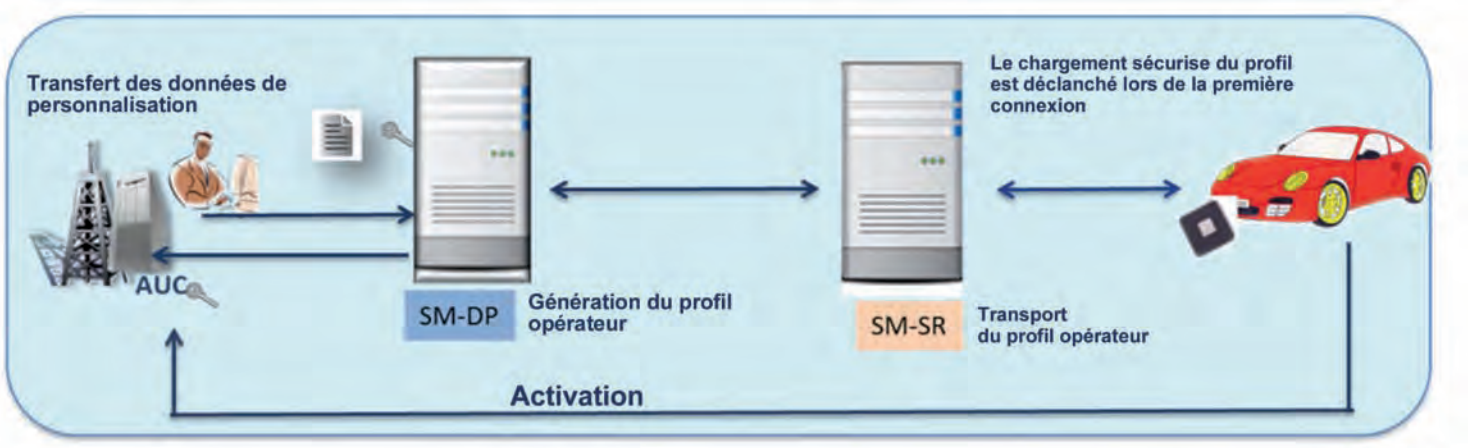
Ce besoin de post-personnalisation remet en cause le modèle économique et le cadre technologique existant des cartes SIM.

Un nouveau modèle de personnalisation

La post-personnalisation est en cours de standardisation dans deux organismes différents.

- L'ETSI, avec une vision globale du sujet : la solution sera dédiée au domaine M2M mais également aux objets connectés grand public,
- La GSM Association qui défend les intérêts des opérateurs et dont les spécifications s'adressent uniquement au domaine du M2M.

Les spécifications de la GSMA étant plus abouties (une première version est disponible depuis décembre 2013), c'est



le modèle actuellement à l'étude dans l'industrie automobile.

Initialement le fabricant de cartes à puce jouait un double rôle : il fournissait le de composant (matériel et logiciel) et prenait également en charge la personnalisation de la carte SIM selon les spécifications et données de son client : l'opérateur.

La solution proposée introduit un nouvel acteur : le « Subscription Manager ». Il s'agit d'un server en charge de la gestion des profils (des SIM) de l'intégration de ceux-ci à distance dans la carte. Ce nouvel acteur a deux rôles distincts et peut être séparé en deux entités :

- La préparation des données, cette entité « Subscription-Manager : Data Preparation » (SM-DP) est responsable de la préparation des données et du chiffrement des SIMs en fonction des caractéristiques de l'opérateur.

- Le transport des données, cette entité « Subscription-Manager : Secure Routing » (SM-SR) personnalise l'eUICC.Elle va donc gérer la communication sécurisée entre l'opérateur/le SM-DP et la carte SIM embarquée.

Pour permettre la première connexion et donc assurer le chargement des données de personnalisation du premier opérateur, l'eUICC est personnalisée en usine avec un opérateur de provisionning qui ne sera actif qu'au début du cycle de vie de celle-ci.

Dans ce nouvel écosystème, les rôles et responsabilités de chaque acteur (opérateur, fournisseur de modem et fournisseur de carte) sont modifiés. En effet, la propriété de la carte SIM rend l'opérateur légalement responsable de la connectivité. Dans ce nouveau modèle qui sera le propriétaire de la carte SIM avec les responsabilités légales associées ? Et surtout comment s'assurer des liens de confiance entre les différents acteurs ?

De la résolution de ces derniers éléments découlera le modèle économique de la connectivité des objets dont l'automobile.

L'émergence de nouveaux modèles économiques

Aujourd'hui, les premiers déploiements utilisent une solution basée sur une carte multi-profil mais les appels d'offres en cours portent sur la solution de post allocation.

À date, même si la majorité des fournisseurs de cartes proposent des solutions de post-personnalisation compatibles avec les spécifications GSMA, elles ne sont pas pour autant interopérables.

Plusieurs modèles économiques peuvent coexister dans la situation :

- Des grandes alliances entre opérateurs avec une solution propriétaire de post-allocation.

- Une solution de bout en bout fournit par de grands groupes (Vodafone, Orange, ...)

- Un modèle imposé par la régulation tel Denatran, organisme national brésilien en charge de la circulation pour lutter contre les vols de voiture.

L'AUTEUR

Sophie DIALLO est Responsable des Etudes et conception cartes SIM chez Bouygues Telecom. Elle y coordonne l'activité SIM sous l'ensemble des aspects (marketing, techniques, achats). Elle contribue également à des activités de standardisation au travers de l'ETSI (Smart Card Platform Technical Committee) où elle est rapporteur des spécifications relatives à la sécurité et au transport des données. Elle a exercé par le passé des responsabilités au sein de Global Platform, le forum dédié à la sécurité et l'administration à distance des cartes à puces.

Le monde connecté en mouvement, perspectives

Par Paul JOLIVET (1995)

Le monde de la téléphonie mobile a vu des technologies et des usages en évolution fulgurante et permanente depuis les années 1990. Nous vivons plus que jamais dans un monde mobile et connecté. Les outils créés et à venir permettent à la société de soutenir son besoin actuel de rapidité et d'immédiateté ...
Si les réelles révolutions sont rares, les évolutions et innovations justifient l'existence même du modèle de la mobilité. Florilège des évolutions du monde connecté.

Un essai rapidement transformé

Si les réseaux mobiles des années 1980 sont restés l'apanage des hommes d'affaires fortunés, des médecins et des agents secrets, le domaine a connu une évolution fulgurante par la suite. Il est devenu normal d'avoir un téléphone mobile et d'être toujours connecté.

Le téléphone est rentré dans les usages et y a rapidement pris sa place, annexant d'autres usages. Exit la montre, le navigateur GPS, le petit appareil photo compact, ... Tous les usages quotidiens ont tendance à intégrer le mobile, dont on ne se sépare plus : on oublie moins facilement son téléphone que son portemonnaie ou son passe de transport. Mieux, on fait plus facilement demi-tour sur le chemin du travail pour aller chercher son téléphone que pour autre chose.

Des époques et des tendances

Le téléphone mobile a été l'outil de communication « voix ». La première tendance est la miniaturisation des appareils, grâce à l'évolution des composants. Les mobiles deviennent petits au point d'être difficile à manipuler. Dans les années 1990 apparaissent les premières montres chez les Coréens LG Electronics puis Samsung. Il s'agit de téléphones miniaturisés et non comme maintenant le prolongement d'un téléphone.

Source : Ericsson

Le smartphone dont le succès marque la fin des années 2000 participe à l'inversement de cette tendance, disposant d'un grand écran sur toute la surface de l'appareil. La miniaturisation concerne maintenant les modules de communication des machines.

Technologies, tentatives et révolutions

Les évolutions technologiques se déclinent aujourd'hui en trois grands axes :

- **le réseau :** plus de capacité pour l'opérateur, plus de débit,
- **les écrans :** haute définition, écrans courbes ou souples,
- **les batteries :** plus d'autonomie à taille égale et optimisation de la charge.

Il est rare qu'une technologie pensée sans usage perce facilement. L'internet mobile a failli faire les frais de cet adage, inadapté au moment de son introduction au réseau et aux téléphones existants.

Le smartphone a été une vraie révolution pas forcément côté terminal mais surtout dans l'intégration de ce terminal à un écosystème d'applications sous-tendant aux usages.

Il faut aussi noter un grand nombre d'initiatives de l'industrie pour participer au renouvellement des appareils. Beaucoup se sont soldées par des échecs commerciaux. Ces tentatives ont pu prendre la forme :

- de phablettes, entre la tablette et le téléphone,
- de la télévision mobile que les opérateurs n'arriveront pas à lancer à côté de la télévision numérique,
- d'écrans 3D, qui ont buté sur le manque de contenus spécifiques.

Source : LG Electronics

S'habiller de téléphone, le top du moment

La tendance actuelle est le « wearable », ensemble des vêtements ou accessoires connectés portés au quotidien. L'exemple le plus évident est celui des montres ou des lunettes Google. Ces appareils sont conçus cette fois comme un prolongement du téléphone, voué à délivrer informations ou notifications, offrir un service amélioré (réalité augmentée, kit mains libres...). les grands acteurs du domaine investissent en tentant d'offrir simultanément un produit et des usages/applications.

Source : LG Electronics

Avec ces évolutions, le mobile et son utilisateur entrent de plein pied dans le monde connecté.

Les usages une évolution au quotidien

Le téléphone ne sert plus simplement à téléphoner. Il sert à rester connecté à son monde, au travers des messageries, des réseaux sociaux, et de la téléphonie.

Il faut rester connecté : les téléphones se dotent du wifi. Plus un restaurant, de moins en moins de lieux publics sans un accès internet souvent gratuit. On poste sur son réseau social en direct, on traduit la carte du restaurant prise en photo. Le téléphone se dote de modules GPS pour fournir la localisation. Il sert de moyen de navigation et trouve le magasin le plus proche.

Dans ce monde connecté, le téléphone multiplie les usages et les interactions qui facilitent la vie. La recharge d'un passe de transport sur une application dédiée plutôt que de faire la queue, le paiement par téléphone mobile chez le boulanger.

Des risques dans l'innovation ?

La concentration des applications et de leurs données soulève évidemment des inquiétudes liées au « Big Data » ; les utilisateurs prennent conscience du volume d'informations disponible. La notification rendue obligatoire récemment sur l'utilisation des cookies a attiré l'attention sur le fait que les fournisseurs de service exploite ces données. L'idée que le gratuit a ces contreparties commence à être acquise, personne n'étant prêt à sacrifier à la « gratuité » sur Internet.

Une autre source d'inquiétude est le regroupement des services dans un terminal, et le risque de perte ou de fraude. La répartition des responsabilités reste floue. Si la gestion à distance et la sauvegarde (cloud) résolvent le problème, elles ne rassurent pas complètement sur la sécurité des données. Un plus notable côté sécurité : on sait qu'on a perdu son téléphone très rapidement (au pire en heures)... dans le cas d'une carte bancaire ça peut prendre des jours selon l'utilisation.

Les risques sont souvent d'abord résolus par une kyrielle de mots de passe que l'utilisateur ne peut retenir facilement. La réponse biométrique a déjà montré des failles (le lecteur d'empreinte digitales a été pris en défaut immédiatement) et des limites (en cas de fraude, on peut changer un mot de passe, plus difficilement sa main).

Accepter l'innovation ...

L'innovation arrive toujours avec des changements, des inquiétudes. Les interactions avec les objets connectés doivent être comprises par l'utilisateur pour qu'il soit rassuré. La confiance dans les systèmes doit s'installer, on pense évidemment au cas des voitures qui parlaient dans les années 80 dont les conducteurs n'acceptaient pas les remarques. L'utilisateur doit avoir capacité à comprendre et participer à une décision plutôt que de simplement obéir, surtout à une machine.

Les entreprises innovantes (au sens de faire passer l'invention aux usages) sont celles qui savent créer du neuf, mais aussi intégrer dans le processus de création la dimension sociologique, ethnographique. Les plus grands acteurs du domaine ont tous investi cette dimension incontournable. L'innovation proposée doit avoir un sens. ▮

L'AUTEUR

Paul JOLIVET (1995) est Directeur Recherche et Standards en Europe de LG Electronics (téléphones mobiles). Son champ d'action est principalement l'innovation et la standardisation. Il est Président du 3GPP CT WG6 (Applications carte à puce) et de l'ETSI SCP TEC (Spécification de la plateforme carte à puce multi applicative). Il enseigne régulièrement dans plusieurs Ecoles dont Télécom ParisTech et Télécom Bretagne. Il étudie par ailleurs à l'Université Paris Dauphine dans le cadre d'un Doctorate of Business Administration sur le domaine de l'Innovation.

Dans la classe

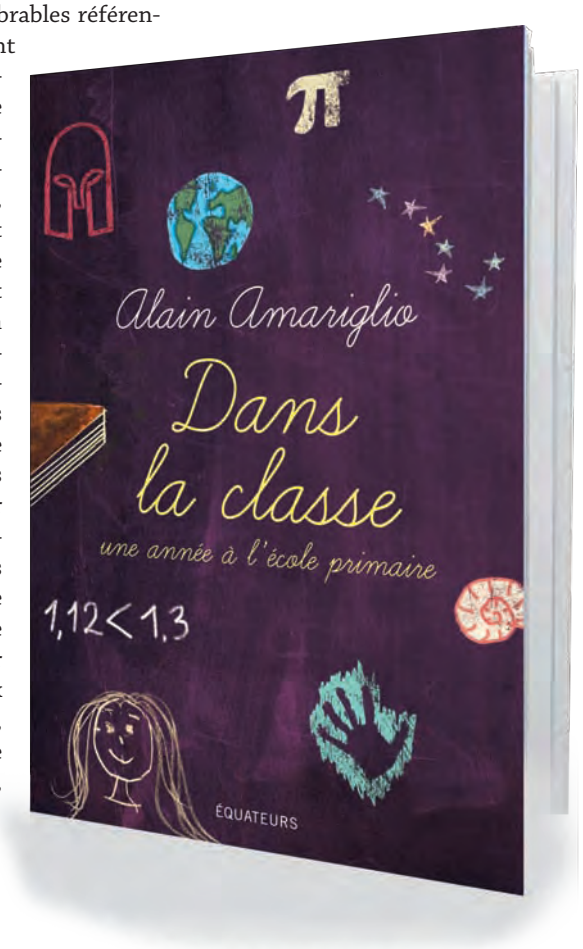
Par Alain AMARIGLIO (1988)

Dans son deuxième livre, Alain Amariglio nous raconte sa reconversion en instituteur, passant de l'univers des start-up à celui de l'école primaire.

Dans son premier livre, *Il était un petit navire*, il racontait son aventure d'entrepreneur. Le deuxième, Dans la classe, est consacré à son expérience d'instituteur et à ses élèves. Hamou Bouakkaz, également diplômé de la promo 88, ancien adjoint au maire de Paris et lui-même auteur de « *Aveugle, Arabe et homme politique, ça vous étonne ?* » l'a lu pour Télécom.

Qui n'a pas son avis à donner sur l'école ? Le plus immédiat, le plus brutal, souvent le plus certain de sa propre véracité ? C'est donc sur une crête redoutable que se positionne Alain Amariglio. Plutôt que de faire simplement résonner un discours sur des faits inconnus, ici l'enjeu premier est de montrer qu'un autre discours est tout simplement possible. Et quel discours. Alain Amariglio n'endosse ni un rôle d'expert, ni celui de professeur chevronné, lui qui assume d'être un nouveau venu dans le métier de prof. Il est encore moins l'un de ceux que l'on nomme «Grands Chefs» parés de dizaines de plumes d'aigle, cadres de haut niveau du ministère de l'Education Nationale. Il n'est pas non plus un de ces anciens élèves frustrés voulant en découdre. Sa démarche détonne. Elle est, en vérité, la plus naturelle qui soit. Celle que nous aurions dû d'emblée adopter. Alain a choisi l'enseignement après des années de vie bien remplie. Alors que sa carrière dans d'autres branches était déjà avancée. Les grands principes républicains, non seulement il les connaît, mais il les revendique. Il les met en acte. Un jour de rentrée donc ouvre le récit. Alain, nouveau prof, conte son sentiment d'irréalité face à ces deux douzaines de visages. Page après page défilent petits échecs, petites victoires, autant de moments de vie. Patiente mosaïque de l'humanité de demain, l'oeuvre d'Alain Amariglio est plus encore qu'un panorama anthropologique du petit d'homme. Elle est un laboratoire de convictions. Les innombrables références littéraires qui bercent le récit, autant de témoignages de l'érudition de l'auteur, sortis d'un cadre livresque que d'ordinaire on leur assigne, prennent subitement une autre lumière. Une apparence terriblement humaine. Se muent en témoignage d'humanité. Les trois cents pages défilent l'une après l'autre, sous l'oeil ou le doigt de plus en plus captivé du lecteur. Pour déboucher sur, merveille des merveilles, ces liens profonds entre le maître et ses élèves que tous pleurent le dernier jour de classe venu, eux que, au premier jour, tout séparait. «Le doute est l'école de la vérité», disait Francis Bacon, l'un des pères de l'esprit scientifique moderne. Merci, Alain, pour ce doute qui libère des carcans et prouve que la véritable école de la vie est ailleurs. Devant nous. ▮

Hamou Bouakkaz (1988)



Dans cet extrait, Alain raconte les premières minutes après la rentrée des classes.

La sonnerie comme dans un rêve.

S'avancer vers les élèves. Les saluer. Les compter. Exiger un rang parfait. Ne pas sourire. Ces conseils se bousculent dans ma tête pendant que mon pilote automatique a pris le relais. En ce premier jour les élèves, impressionnés, adoptent spontanément un comportement impeccable. Montons.

Dans l'escalier, puis tout au long de l'interminable couloir, l'irréalité demeure. Je suis le maître. Ces enfants marchant deux par deux vers la salle de classe sont mes élèves. Certains me regardent par en dessous, d'autres m'adressent des sourires timides. Deux ou trois, mal réveillés, bâillent. Celui-ci, visage fermé, m'inquiète. Il avance tête baissée.

J'ouvre la porte.

Tout est en ordre.

J'en suis presque surpris comme si je n'avais pas passé plusieurs heures hier à faire, défaire et recommencer. Tables et chaises sont maintenant alignées dans une géométrie savante exactement adaptée aux effectifs.

C'est une salle de classe.

Une vraie.

Regardons-la bien, elle n'aura plus jamais le même aspect.

Aussi propre. Aussi net. Sans une trace de pas, ni un grain de poussière.

Le tableau semble n'avoir jamais été utilisé.

L'éponge est neuve, l'eau du seau limpide, le chiffon propre.

Ça sent la cire.

Je n'ai pas eu le temps d'accrocher la moindre affiche. Outre les couleurs du ciel et des arbres que l'on voit par la fenêtre, seule une carte du monde offerte par Médecins Sans Frontières égaie un peu les murs presque nus.

Mais les élèves arrivent.

Avec eux, les couleurs.

- Entrez. Prenez une place temporaire, je réorganiserai la classe plus tard. Les CE2 à gauche, les CM2 à droite. Sans bousculade, s'il vous plaît.

Ils entrent sans bruit, avec leurs gros cartables, puis attendent debout derrière les chaises.

- Asseyez-vous.

Je marche vers la porte, la referme lentement. On l'entend grincer dans le silence revenu.

À l'oral du concours, le jury m'a donné 20/20.

La vraie épreuve vient de commencer.

Dans la classe, Editions des Equateurs

L'AUTEUR

Alain AMARIGLIO (1988) est ingénieur, entrepreneur, instituteur.
Diplômé de Télécom ParisTech en 1988, il crée SLP avec Jean Schmitt (1988), Jérôme Pujol (1988) et Thierry Delbecque (INT), dès leur sortie de l'école. La première partie de sa carrière est consacrée au développement de cette start-up, dont les clients sont les opérateurs de télécommunications. Vite apparue sur les radars des analystes, SLP fait en 2001 l'objet d'une acquisition par Gemplus, leader mondial des cartes à puces, pour laquelle Alain continue à travailler un temps.
Après quoi il revient à un projet de toujours : l'enseignement. Il présente le concours à Paris, passe un an à l'IUFM puis enseigne dans plusieurs écoles primaires parisiennes, souvent en ZEP. Il est sans doute le seul ancien à avoir enseigné au pied de la Butte-aux-Cailles, rue de la Providence...

Les rencontres des alumni d'Orange : 3e édition

C'est devenu « le rendez-vous » annuel pour les alumni en poste chez Orange. Yves Poilane (1984), directeur de l'école, a introduit la soirée par l'actualité de l'école et de son enseignement, les partenariats avec les entreprises et notamment Orange, la présentation du projet architectural de la nouvelle école sur le plateau de Saclay. A la suite de Jean Philippe Vanot (1977), Mari-Noëlle Jégo-Laveissière (1995), nouvellement nommée directrice exécutive Innovation, Marketing et Technologies du Groupe Orange auprès de Stéphane Richard qui a repris le flambeau de ces « Rencontres Télécom ParisTech alumni d'Orange » ce 10 juin à Orange Campus. Organisée avec le concours de Christine Chardon (1995), administratrice de l'association et attachée à la Direction de la Communication d'Orange France et avec le soutien de l'association et de la Fondation Télécom, l'invité d'honneur de la soirée était Antonio Casilli. Enseignant-chercheur en sociologie numérique à Télécom ParisTech, au département des sciences économiques et sociales, Antonio Casilli a proposé une conférence issue de sa publication « contre l'hypothèse de la fin de la vie privée » interrogeant la question de la vie privée sur les réseaux sociaux. Mari-Noëlle Jégo-Laveissière a animé les échanges posant le sujet de la sécurité des données en miroir du contexte d'Orange, avant de répondre avec spontanéité aux diverses questions des quelques 150 diplômés venus se retrouver pour l'occasion.

A suivre pour l'édition 2015 !

1


2


3


4

1 *Mari-Noëlle Jégo-Laveissière (1995)*

2 *Antonio Casilli, enseignant-chercheur en sociologie numérique à Télécom ParisTech*

3 *Christine Chardon (1995)*

4 *Yves Poilane (1984) et Antonio Casilli*

Suivre l'actualité d'Antonio Casilli sur Twitter @antoniocasilli ou ses chroniques sur France Culture.

Journée de l'Innovation étudiante et diplômée de Télécom ParisTech

retour sur l'édition 2014

Le 19 juin, 10 projets d'étudiants et 5 start-up ont concouru pour 3 prix « coup de cœur » décernés par le jury composé de Michel Paulin (Meditel, ex-Neuf Cegetel), François Paulus (co-fondateur de Breega Capital), Jean-Luc Vaillant (co-fondateur de LinkedIn) et Jacques Veyrat (fondateur du repreneur d'affaires Impala).

Bravo aux 3 réalisations primées !

- **Projet étudiant Plume :** géolocaliser des objets à l'intérieur des bâtiments.
- **Projet étudiant Qubble :** jouer de la musique autrement avec une table interactive, destinée notamment aux enfants.
- **Start-up FocusMatic :** ce qui se dit de sa marque et celles de ses concurrents sur les réseaux sociaux.

Retrouvez la Journée de l'Innovation sur www.Télécom-paristech.fr/journee-innovation/

FocusMatic, start-up primée à la Journée de l'Innovation 2014

Deux nouveaux Masters créés avec l'École Polytechnique

Le Master **Mathématiques pour la science des masses de données**, créé par l'École Polytechnique et Télécom ParisTech pour la rentrée 2014, vise à optimiser le « Big Data » afin d'extraire l'information la plus pertinente. Son responsable est Éric Moulines, professeur au département Traitement du Signal et des Images.

Télécom ParisTech et l'École Polytechnique, en partenariat avec l'Inria, ouvrent le Master **ACN (Advanced Communication Networks)**, dont la première promotion fait sa rentrée le 1er octobre. Cette formation d'excellence vise à former des chercheurs et des ingénieurs de haut niveau dans le domaine des réseaux.

Université Paris-Saclay : une avancée importante

Télécom ParisTech vise à devenir le collège de l'innovation par le numérique de l'Université Paris-Saclay. Une avancée importante a eu lieu le 8 juillet avec l'adoption par les 19 membres fondateurs des statuts de la nouvelle COMUE (COMmunauté d'Universités et d'Etablissements).

Distinctions recherche

Quatre doctorants ont été primés par Télécom ParisTech dans le cadre de l'initiative « 5 minutes Pour Ma Thèse - PhD Pitch »
Ce nouvel événement qui a eu lieu le 26 juin vise à exercer les doctorants à synthétiser efficacement leurs travaux à destination d'un public large et à faire connaître la diversité et la richesse des thèses menées à Télécom ParisTech ou avec nos partenaires.

- **Antoine Saillenfest, 1er prix :** Modélisation de l'intérêt dans le récit fictionnel - Application au récit automatique.
- **Xavier Pons Masbernat, 2e prix :** Green Concept appliqué aux Réseaux Radiomobiles 4G de type PMR.
- **Samuel Goeta, 3e prix ex aequo :** Les coulisses de l'open data - sociologie de la production et de la libération des données publiques.
- **Marwa Meddeb, 3e prix ex aequo :** codage vidéo conceptuel pour un système de vidéoconférence bas débit.

Retrouvez leurs prestations filmées sur http://www.Télécom-paristech.fr/recherche/doctorat/5-pour-ma-these-phd-pitch.html

Prix du Poster au congrès SFIPP 2014 (Société Française d'Imagerie Pédiatrique et Prénatale)
Prix du poster pour « Étude de la reproductibilité des interprétations d'IRM cérébrales néonatales » (B. Morel, S. Kemel, S. Dahdouh, C. Adamsbaum et I. Bloch) lors du congrès de la SFIPP (Société Française d'Imagerie Pédiatrique et Prénatale) en juillet 2014 à Lyon. Isabelle Bloch est professeure au département Traitement du Signal et des Images.

La doctorante Nausikaa Geeraert reçoit un Best Paper Award à la conférence RPM 2014
Nausikaa Geeraert, doctorante à Télécom ParisTech, en cotutelle avec l'université KUL de Leuven (Belgique) et en CIFRE avec General Electric, a eu le prix du meilleur article à la conférence RPM 2014 (International Conference on Radiation Protection in Medicine) du 30 mai au 2 juin à Varna (Bulgarie).

Deux Best Paper Awards pour le groupe Systèmes Électroniques Numériques de Télécom ParisTech
Le groupe Systèmes Électroniques Numériques (SEN) du département Communications et Électronique a reçu deux Best Paper Awards au printemps 2014 :

- Best student paper award à la conférence IEEE - Symposium on Hardware Oriented Security & Trust (HOST), 6-7 mai, Arlington (États-Unis) pour Daisuke Fujimoto (Kobe University) pour lequel le groupe de recherche SEN est co-auteur (projet ANR Spaces).
- Best paper award à la 12e International Conference on Applied Cryptography and Network Security (ACNS '14), 10-13 juin, Lausanne (Suisse) pour Annelie Heuser, dont les directeurs de thèse sont Sylvain Guilley et Olivier Rioul (elle est aussi lauréate en 2013 d'une bourse de recherche Google).

Rentrée : bienvenue à Télécom ParisTech !

L'accueil de nos nouveaux étudiants par la direction le 8 septembre a été marqué par le témoignage fraternel de **Corentin Raux (1999)**, fondateur de **Pretty Simple**, l'entreprise à l'origine du jeu **Criminal Case** au succès mondial. Les nouveaux intégrés ont aussi pu, grâce à des démonstrations d'enseignants-chercheurs et d'étudiants, s'imprégner de la qualité et de la diversité des activités de l'École.

A voir sur www.telecom-paristech.fr/rentree/

Retour sur le programme FIRST 2014

Le 16 septembre dernier, la première saison du nouveau programme FIRST s'est achevée avec la présentation au public des projets d'open-innovation des trente-six étudiants engagés dans l'aventure.
Pour cette nouvelle formule, le programme FIRST, programme de formation ouvert aux étudiants de deuxième année des écoles Télécom ainsi qu'à des élèves de l'école de design de Reims, a porté six projets innovants en lien avec le domaine du numérique.
Les six équipes se sont retrouvées à trois reprises dans des lieux phares de l'innovation, Orange Labs, NUMA, le Cube, SFR, pour travailler lors de séminaires résidentiels de deux jours sur tous les aspects de leurs projets : business models, développement technologique, communication et prototype. C'est enfin au cours d'une école d'été de 10 jours passée au sein de l'incubateur de l'Université Technologique de Tampere en Finlande qu'ils ont pu mener à bout leur projet et pitcher devant un public averti (professeurs, ingénieurs de l'université, start-upers et institutionnels). Entre visites d'entreprises innovantes, laboratoires de recherche, conférences en lien avec leurs thématiques de travail et incitation à l'innovation, les étudiants ont pu développer leur esprit d'entrepreneur. Et certains envisagent de poursuivre à l'issue de leurs études sur la création d'entreprise…

Témoignage d'un étudiant du programme FIRST 2014

Le programme FIRST est une occasion unique pour un élève ingénieur de découvrir le monde de l'entrepreneuriat. A travers les différents séminaires proposés, on est réellement plongé dans le monde des start-up. Pouvoir me rendre dans un lieu comme NUMA, lieu hautement prestigieux dans l'entrepreneuriat, m'a permis de réaliser qu'aujourd'hui, monter sa start-up et réussir n'est plus seulement un rêve mais bien une réalité.
Pour ma part, ce monde m'était totalement inconnu jusqu'alors. Grace au programme FIRST, j'envisage très sérieusement de lancer un jour ma start-up.
Plus qu'un simple projet scolaire, le programme FIRST est une expérience professionnelle enrichissante qui permet d'avoir une vision globale sur le monde de l'entrepreneuriat.

Viktor Jarry, Télécom ParisTech (2015)

Les six projets FIRST 2014

- **ChampiMix :** un jeu interactif de création musicale.
- **EZmove :** une application munie de capteurs permettant un apprentissage gestuel guidé pour les archers.
- **Orientago :** une plateforme innovante qui permettra aux jeunes de découvrir des métiers
- **SensPlin :** a pour objectif de fournir une nouvelle approche sensorielle au monde du spectacle en enrichissant le show à travers une synesthésie des sens.
- **Smartbus :** une application collaborative qui s'adresse aux voyageurs réguliers des bus, tramways et lignes de métro aériennes.
- **WhatsOn :** WhatsOn est une application android destinée à faire le lien entre des contenus numériques (vidéo, texte, musique,…) en relation avec votre humeur du moment.

SensPlin

Soutenez Télécom ParisTech à votre rythme et en toute simplicité

Depuis peu, la Fondation Télécom met à votre disposition un nouvel outil pour soutenir Télécom ParisTech : le prélèvement automatique. Une manière simple et pratique d'apporter à votre école le soutien dont elle a besoin de la part de ses diplômés.

Vous avez désormais la possibilité de soutenir Télécom ParisTech au rythme qui vous convient et pour le montant que vous choisissez. De même, à vous d'affecter vos dons à la cause de votre choix : bourses d'excellence, soutien aux start-up des incubateurs des écoles, bourses internationales, aide à l'aménagement de Télécom ParisTech à Saclay, fonds annuel, etc.

Si cette option vous intéresse ou si vous souhaitez plus d'informations à ce sujet, n'hésitez pas à contacter Charlotte Gonnord (charlotte.gonnord@mines-telecom.fr – 01 45 81 74 27) afin que nous puissions répondre à vos questions et vous faire parvenir le document à remplir afin de mettre en place le procédé.

Que vous ayez choisi ou pas le prélèvement automatique, notez qu'il est bien évidemment toujours possible de réaliser des dons ponctuels soit par chèque, soit en vous rendant sur **www.fondation-telecom.org.**

Un très grand merci de votre soutien !

Rappel

Pour bénéficier de réductions fiscales sur votre impôt sur le revenu 2014, n'hésitez pas à concrétiser votre don à Télécom ParisTech en vous rendant sur le site de la Fondation Télécom www.fondation-telecom.org puis « Faire un Don », avant le 31 décembre 2014.

COMMANDER LA REVUE TELECOM

À compléter et à nous retourner, accompagné de votre règlement à :
Télécom ParisTech alumni - La Revue TELECOM - 46 rue Barrault, 75634 PARIS cedex 13 ou sur contact@telecom-paristech.org
Aucune commande ne sera prise en compte sans règlement joint.

VOS COORDONNEES

Nom, Prénom.....
Société.....
Adresse .....
Code postal .....Ville .....
Pays .....
e-mail .....
tél .....

Adresse de facturation *(si différente de l'adresse de livraison)*

Nom, Prénom.....
Société.....
Adresse .....
Code postal .....Ville .....
Pays .....
e-mail .....
tél .....

VOTRE ABONNEMENT

☐ Je m'abonne à la revue TELECOM 53 €
pour une année civile (4 numéros)

☐ Je commande un numéro unique 21 €
Numéro :

☐ Je commande plusieurs exemplaires de la revue TELECOM
Nous contacter

Mode de règlement (factures sur demande)

☐ Par virement (voir les informations ci-dessous)
Date du virement : / / Référence du virement :

☐ Par chèque : à l'ordre de l'AIST

☐ En espèce ou par carte bancaire au bureau de l'association au 46 rue Barrault, 75013 PARIS

Informations complémentaires pour les virements : IBAN FR76 1027 8033 0000 0280 2554 590 - BIC CMCIFR2A
Merci d'intituler votre virement « achat de la revue ____ » et de retourner ce document à contact@telecom-paristech.org

LES REVUES TELECOM DISPONIBLES A LA VENTE

N° 174 Cybersécurité – La mobilité
N° 173 Les industries de contenus à l'ère digitale – Finance et sécurité
N°172 Prix des technologies Numériques 2014 – La performance énergétique
N°171 50 ans de la revue Télécom
N°170 Les systèmes de transport intelligents : vers une nouvelle mobilité
N°169 BIG DATA Nouveaux défis
N °168 Le Prix des Technologies Numériques 2013
N°167 Le conseil vocation ou nouvelle vie
N°166 Divertissement numérique : la fiction dépassera-t-elle la réalité ?
N°165 Le Prix des Technologies Numériques 2012
N°164 CLOUD Le tout Internet

COMMENT AVEZ-VOUS CONNU LA REVUE TELECOM ?

☐ Dans votre entreprise
☐ Suite à un événement. Lequel ?.....
☐ Par le site Internet de Télécom ParisTech alumni
☐ Pendant votre scolarité à Télécom ParisTech
☐ Autres ?.....

Important Les diplômés de Télécom ParisTech cotisants peuvent souscrire un abonnement à la revue TELECOM à un tarif préférentiel. Pour plus d'informations : contactez-nous !

Contact contact@telecom-paristech.org - Tél. 01 45 81 74 77 - **www.telecom-paristech.org**

La Communication
dans tous ses états

Site Internet
Supports multimédia
Brochures
PUBLICATIONS
Salons
Edition
Annuaires
CATALOGUES
Régie publicitaire
Identité Visuelle

Régie publicitaire
Annuaires
BANNIERES
Edition
Impression-Routage
REVUES THEMATIQUES
Site Internet
Catalogues
Supports multimédia
ANNUAIRES
Brochures

EM-COM

Partenaire de Télécom ParisTech alumni

- Fédérations
- Grandes Ecoles de Commerce
- Grandes Ecoles d'Ingénieurs
- Salons et Congrès
- Sociétés Savantes
- Universités
- Associations
- Web

ENSEMBLE,
atteignons votre cible...
pour la réalisation de vos supports de communication

EM-COM
11, rue Chevreul
94100 SAINT MAUR DES FOSSES
Tél. : 01 43 97 40 82
contact@em-com.fr

www.em-com.fr

EI TELECOM

Découvrez **EI Telecom**, un **opérateur innovant** sur un marché compétitif

350 millions d'euros

CHIFFRES D'AFFAIRES

EI Telecom, un opérateur particulièrement innovant :

- Une architecture performante avec cœur de réseau de dernière génération
- Une structure de coût optimisée
- Une capacité unique à apporter des solutions aux autres opérateurs : agrégation de trafic, services hautement résilients, approvisionnement multi-opérateurs

1.3 millions de clients

SOUS 5 MARQUES DISTINCTES :

Crédit Mutuel Mobile · CIC Mobile · nrj mobile · Auchan telecom · Cofidis Mobile

4.600 CAISSES /AGENCES BANCAIRES

UN RÉSEAU DE DISTRIBUTION UNIQUE

Si vous souhaitez participer à son développement contactez : **nrjrh1@e-i.com**

Pour en savoir plus, découvrez l'**article de Philippe Sikora**,
Directeur de la Stratégie et du Contrôle Interne