SOMMAIRE

Pages

SOMMAIRE 3

PRÉAMBULE 9

INTRODUCTION – L'ACTUALITÉ DE LA SÉCURITÉ DU NUMÉRIQUE 19

CHAPITRE PREMIER – LE CONTEXTE INTERNATIONAL DE LA SÉCURITÉ NUMÉRIQUE DES ENTREPRISES 25

I. LA GOUVERNANCE TECHNIQUE DU NUMÉRIQUE À L'ÉCHELLE MONDIALE 26

A. LA GOUVERNANCE MONDIALE DE L'INTERNET 26

B. LA GOUVERNANCE MONDIALE DE LA SÉCURITÉ 28

II. LA GESTION MONDIALE DES INCIDENTS DE SÉCURITÉ NUMÉRIQUE 30

A. LES SERVICES DE VEILLE 30

B. LES INQUIÉTUDES GRANDISSANTES DES ÉTATS FACE AU NUMÉRIQUE 33

C. LES RAPPORTS DE FORCE ENTRE LES GÉANTS DE L'INTERNET, LES ÉTATS, LES ENTREPRISES ET LES CITOYENS 35

III. LE PROJET D'ACCORD DE LIBRE ÉCHANGE ENTRE LES ÉTATS-UNIS D'AMÉRIQUE ET L'UNION EUROPÉENNE 37

IV. VERS UNE EUROPE DU NUMÉRIQUE COHÉRENTE ? 39

V. SOUVERAINETÉ ET NUMÉRIQUE 41

A. UNE COLONISATION NUMÉRIQUE ? 41

B. LES LEÇONS TIRÉES PAR LES ÉTATS-UNIS D'AMÉRIQUE DES EXCÈS DE LA NSA 43

CHAPITRE II – LE CADRE NATIONAL DE LA MISE EN ŒUVRE DE LA SÉCURITÉ NUMÉRIQUE 45

I. NUMÉRIQUE ET LIBERTÉS 45

A. LE RAPPORT DU CONSEIL D'ÉTAT SUR LE NUMÉRIQUE ET LES DROITS FONDAMENTAUX 45

B. LIBERTÉ DE L'USAGE DU NUMÉRIQUE ET LIBERTÉS DE SES USAGERS 51

II. LA MISE EN ŒUVRE OPÉRATIONNELLE DE LA SÉCURITÉ NUMÉRIQUE 54

A. LA DIRECTION GÉNÉRALE DE L'ARMEMENT (DGA) 54

B. LE LABORATOIRE DE HAUTE SÉCURITÉ DU LABORATOIRE LORRAIN DE RECHERCHE EN INFORMATIQUE ET SES APPLICATIONS (LORIA) 56

C. L'AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (ANSSI) 57

D. LA GENDARMERIE NATIONALE 59

E. LES INDUSTRIELS 60

III. ORGANISATION DE LA SÉCURITÉ NUMÉRIQUE 60

A. LES INVESTIGATIONS DES OBSERVATOIRES PUBLICS ET PRIVÉS 61

B. L'INVESTIGATION POLICIÈRE 62

C. L'ASSURANCE CONTRE LE RISQUE CYBER 63

IV. LES OPÉRATEURS D'IMPORTANCE VITALE (OIV) 64

A. LA PROBLÉMATIQUE GÉNÉRALE 65

B. L'EXEMPLE DU SECTEUR DES TÉLÉCOMMUNICATIONS 66

C. L'EXEMPLE DU SECTEUR DE L'ÉNERGIE 68

CHAPITRE III – LA COMPLEXITÉ DU NUMÉRIQUE REND SA SÉCURITÉ POUR LES ENTREPRISES DIFFICILE À CONCEVOIR 71

I. VERS UNE REPRÉSENTATION DU NUMÉRIQUE DE NATURE À FACILITER SA CONNAISSANCE 72

A. L'ÉCHANGE ET LES COMMUNICATIONS HUMAINES 74
1. Le processus « vertical » ou interne de production des messages en vue de l'échange 74
2. Le processus « horizontal » ou externe de transport du message 77
3. Le niveau virtuel ou global de l'échange interindividuel et sociétal 78

B. L'ÉCHANGE ET LES COMMUNICATIONS NUMÉRIQUES 84
1. Le message comme objet de l'échange numérique 86
2. Le processus « vertical » ou interne de production de message numérique 88
3. Le processus « horizontal » ou externe de transport de message numérique 90

II. LES INFRASTRUCTURES DU NUMÉRIQUE 105

A. INFRASTRUCTURES DE SERVICES MUTUALISÉS POUR LES ÉCHANGES NUMÉRIQUES 105
1. Infrastructure de noms de domaine (DNS) 105
2. Infrastructure de routage et de messagerie 107
3. Infrastructure de navigation : les moteurs de recherche 108

B. INFRASTRUCTURES GLOBALES POUR LES SERVICES : LE NUAGE NUMÉRIQUE 110
1. Les quelques étapes clés 110

2. L'informatique en nuage comme changement de paradigme 111
3. Les modèles de services offerts par le nuage numérique 112
4. Les modèles de déploiements 112
5. Enjeux de sécurité du nuage numérique 114

CHAPITRE IV – FORCES ET FAIBLESSES DU SYSTÈME D'INFORMATION DE L'ENTREPRISE 117

I. LES TROIS NIVEAUX DE L'ENTREPRISE 117

A. LE RÔLE DU SYSTÈME DE DÉCISION 118

B. LE SYSTÈME D'INFORMATION ET DE COMMUNICATION 121
1. Le système d'information 121
2. Le système de communication 122

C. LE SYSTÈME DE PRODUCTION DE L'ENTREPRISE 123
1. Le concept d'industrie 4.0 123
2. Le Manufacturing Execution System (MES) 124
3. Le Supervisory Control And Data Acquisition (SCADA) 124
4. Les capteurs et actionneurs 125

II. ANALYSE CRITIQUE DU SYSTÈME D'INFORMATION DE L'ENTREPRISE 127

A. MODÉLISATION D'UN SYSTÈME D'INFORMATION EN VUE DE SON ÉLABORATION 128

B. LE SYSTÈME DE COMMUNICATION 129
1. Le Réseau Local d'Entreprise (RLE) 129
2. Le réseau local « radio » de l'entreprise ou Wi-Fi 132
3. L'interconnexion du système d'information de l'entreprise avec son système d'information industriel 134
4. Objets connectés dans l'entreprise 135

C. LES SERVICES 136
1. La relation client / serveur numérique 136
2. Les services réseaux 137
3. Les services applicatifs collaboratifs 138
4. Les services applicatifs liés aux métiers de l'entreprise 142

CHAPITRE V - LA SÉCURISATION DU SYSTÈME D'INFORMATION D'UNE ENTREPRISE 145

I. PRINCIPES DE SÉCURITÉ D'UN SYSTÈME D'INFORMATION 145

A. D'UNE VISION STRATÉGIQUE À UNE VISION OPÉRATIONNELLE 145

B. LES TROIS PROPRIÉTÉS FONDAMENTALES DE L'ÉTAT DE SÉCURITÉ 146

C. LES FONCTIONS DE SÉCURITÉ 148

D. ORGANISATION DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS 148

E. L'IMPÉRATIF D'AMÉLIORATION CONTINUE 149

II. MISE EN ŒUVRE DE LA PRÉVENTION DANS LE SYSTÈME D'INFORMATION D'UNE ENTREPRISE 151

A. POLITIQUES DE SÉCURITÉ DE L'ÉTAT ET DES ENTREPRISES 152

B. MISE EN PLACE D'UNE ARCHITECTURE POUR LA SÉCURISATION DU SYSTÈME D'INFORMATION 154
1. La ligne de défense périmétrique traditionnelle 154
2. Le pare-feu comme pièce maîtresse 155
3. Les zones d'accès selon la sensibilité des ressources 156
4. Les antivirus 157

C. CARACTÈRE DE L'AUTHENTIFICATION FORTE 158
1. Le mécanisme d'authentification 159
2. L'identification 160
3. La gestion des identités 162
4. Le protocole d'authentification 163
5. Les principaux protocoles d'authentification 165

D. HABILITATIONS 170
1. La définition des habilitations 171
2. L'accès aux répertoires 173

E. ARCHITECTURES ET PROTOCOLES POUR DES TUNNELS D'INTERCONNEXION SÉCURISÉS 175
1. Les architectures pour des tunnels d'interconnexion sécurisés 175
2. SSL : le maintien de la connexion sécurisée sur TCP/IP 176

CHAPITRE VI – LES FAILLES ET LES ATTAQUES NUMÉRIQUES COMPROMETTANT LA SÉCURITÉ DES ENTREPRISES 179

I. UN MILIEU HOSTILE 179

A. LES VULNÉRABILITÉS 180
1. Les vulnérabilités et menaces 181
2. La veille comme processus d'analyse des vulnérabilités 183
3. La vulnérabilité dite « zero-day », à corriger en zéro jour 189

B. ANALYSE GLOBALE DES RISQUES DANS LES ÉCHANGES NUMÉRIQUES 190
1. L'identification des éléments pour l'analyse des risques 192
2. L'évaluation des risques 196
3. L'analyse des vulnérabilités 197
4. L'analyse de nouvelles vulnérabilités pour une informatique en nuage (cloud computing) 201
5. Les vulnérabilités des protocoles d'authentification 203

II. LES ATTAQUES CONTRE LE SYSTÈME D'INFORMATION 203

A. LA CLASSIFICATION DES ATTAQUES 205
1. Les modes opératoires de base 205
2. Les modes opératoires combinés 206
3. Les attaques sur la confidentialité et l'intégrité 207

B. LES ATTAQUES COMPLEXES ET CIBLÉES 208
1. Les attaques complexes 208
2. Les attaquants chevronnés 213

3. Les caractéristiques d'une cyberattitude 216
4. La cybercriminalité 217

III. LA FONCTION DE SURVEILLANCE DE LA SÉCURITÉ 219

A. RECOURS À LA CARTOGRAPHIE DES RISQUES 219

B. ACTIVITÉS DE SÉCURITÉ POUR LA DÉTECTION, L'ÉVALUATION ET LA REMÉDIATION DES INCIDENTS 221
1. La sécurité opérationnelle 222
2. L'audit de sécurité 225
3. L'investigation liée aux incidents 226

B. RÉACTION AUX ATTAQUES 226
1. L'analyse des flux 226
2. Le contrôle comme point fondamental, vers un contrôle multi-échelle 228

CHAPITRE VII – LA CULTURE DU NUMÉRIQUE ET L'ÉDUCATION À SA SÉCURITÉ 229

I. TEMPS ET CONTRETEMPS DE LA SÉCURITÉ NUMÉRIQUE 229

A. HYPERCONNEXION ET HYPORÉFLEXION 229

B. DES PRIORITÉS QUI RALENTISSENT 232

II. LES ACTEURS DE LA SÉCURITÉ NUMÉRIQUE 233

A. LES CONSEILS DE SÉCURITÉ DISPENSÉS AUX INDUSTRIELS PAR L'ANSSI 233
1. L'infogérance 233
2. Une forme particulière d'infogérance : l'informatique en nuage 236

B. LES INITIATIVES DES INDUSTRIELS EN MATIÈRE DE SÉCURITÉ NUMÉRIQUE 237

III. FAIRE DE L'ÉCONOMIE AVEC DU DROIT ? 239

CONCLUSION 243

RECOMMANDATIONS 245

RECOMMANDATIONS D'ORDRE GÉNÉRAL 247

I. Développer une culture du numérique : former et informer massivement toutes les classes d'âge à l'informatique, dans tous les milieux sociaux 247

II Assurer les conditions d'une autonomie numérique pour préserver la souveraineté 248

III. Se donner les moyens de la sécurité numérique par une meilleure coopération entre les acteurs 249

IV. À partir de dispositions et de pratiques nationales vertueuses, Construire un droit européen 249

V. Assemblées parlementaires, collectivités territoriales et administrations 250

***VADE-MECUM* DE RECOMMANDATIONS DE SÉCURITÉ NUMÉRIQUE À L'USAGE DES ENTREPRISES** 251
1. Les préalables à la sécurité numérique de l'entreprise : 252
2. La construction de la sécurité numérique de l'entreprise 252
3. L'appréciation critique continue de la structure numérique mise en place 254
4. Le parc informatique de l'entreprise 255
5. Les trois séries de distinctions à opérer 256
6. Les principes propres à l'utilisation de chaque réseau ou matériel numérique 257
7. Les réflexes de sécurité numérique à acquérir 258
8. L'évaluation de la sécurité numérique de l'entreprise 260
9. La construction d'une résilience de l'entreprise après une attaque numérique 260

ANNEXES 263

LETTRE DE SAISINE DE L'OPECST 265

EXTRAITS DES RÉUNIONS DE L'OPECST DU 17 DÉCEMBRE 2014 ET DU 28 JANVIER 2015 : ADOPTION DU RAPPORT 267

SCHÉMA DE LA SÉCURITÉ NUMÉRIQUE : INSTANCES PUBLIQUES OU PRIVÉES EN CHARGE DE LA SÉCURITÉ NUMÉRIQUE POUVANT CONCERNER LA FRANCE 295

EXEMPLE DE BULLETIN DE L'ANSSI (26 JANVIER 2015) 297

LA SÉCURITÉ NUMÉRIQUE PAR LE JEU : SCÉNARIO D'UN *SERIOUS GAME* – OCTOBRE 2013 RAPPORT DU CIGREF - RÉSEAU DE GRANDES ENTREPRISES 303

BIBLIOGRAPHIE 331

GLOSSAIRE 339

LEXIQUE DES SIGLES 363

PRÉAMBULE

Le 16 avril 2014, vos rapporteurs ont présenté à l'OPECST leur étude de faisabilité sur la saisine de la commission des affaires économiques du Sénat, transmise à l'Office, le 26 juin 2013, d'un rapport sur « Le risque numérique » (voir, en annexe, la lettre de saisine).

La raison même de l'étude de faisabilité précédant les rapports de l'Office parlementaire d'évaluation des choix scientifiques et technologiques conduit notamment à vérifier si une étude analogue récente existe concernant la sécurité des réseaux numériques utilisés par les entreprises, à recenser les multiples colloques traitant de la sécurité numérique et à apprécier la portée des choix à opérer.

Dans le cadre de la présente étude, vos rapporteurs ont organisé trois journées d'auditions publiques retracées, comme l'ensemble de la centaine d'auditions, dans le tome II du présent rapport.

C'est ainsi que **trois auditions publiques ont été organisées**.

En avril 2014, trois tables rondes sur l'éducation au numérique et à sa sécurité ont d'abord tenté de repérer les moments et les moyens de nature à **favoriser, tout au long de la vie, l'apprentissage des outils numériques, une connaissance des avantages et des risques induits par leurs usages et une conscience de leurs faiblesses** ; l'omniprésence et le développement rapide de ces outils devant être accompagnés par une accélération de l'acquisition d'une véritable culture numérique par la population.

Il deviendrait ainsi possible d'analyser l'évolution en cours et de se demander si elle conduit à une humanité augmentée (plus connectée, plus performante, plus généreuse…) plutôt qu'à une humanité diminuée (plus dépendante, plus influençable, plus soumise, etc.).

Ce questionnement est contenu dans l'analyse de M. Éric Sadin sur l'évolution actuelle de l'humanité conduisant à une administration numérique du monde : « *C'est l'apparition d'un couplage inédit entre organismes physiologiques et codes numériques qui se tisse* ».[1]

Le 19 juin 2014, une audition publique a permis aux intervenants à deux tables rondes de se pencher sur le cadre juridique, les risques et les aspects sociétaux de la sécurité des réseaux numériques.

Enfin, le 26 juin 2014, une audition publique a réuni deux tables rondes sur le risque numérique à travers la sécurité des réseaux

[1] *Voir la bibliographie en annexe du présent rapport.*

informatiques, le stockage des données personnelles ou industrielles et leur exploitation. La première table ronde a rassemblé des opérateurs d'importance vitale des secteurs de l'énergie et des télécommunications ; la seconde a permis d'entendre les entreprises proposant des solutions de sécurité numérique.

Comme déjà envisagé par le Gouvernement en avril 2014, le thème du numérique, enjeu économique voire stratégique, devrait donner lieu au dépôt d'un projet de loi pour la fin du premier semestre 2015.

Il est d'ailleurs probable qu'un tel projet de loi, nécessaire, ne règle, ni en une fois ni une fois pour toutes, les questions posées par le numérique et qu'il faille le compléter, l'approfondir à plusieurs reprises. D'une part, car bien des aspects de cette technique omniprésente ne sont pas encore entrevus, et, d'autre part, parce que l'utilisation du numérique ne cesse de se déployer à travers le monde, notamment du fait de l'évolution des supports (de l'ordinateur au téléphone portable, de la puce *RFID*[1] aux compteurs individuels dits intelligents).

Ce projet de loi s'inscrit dans un ensemble d'initiatives gouvernementales relatives au numérique incluant une **concertation sur le numérique**, organisée par le Conseil national du numérique (CNN) et comprenant une plate-forme en ligne recueillant des contributions de la société civile (d'octobre 2014 à février 2015), la publication de la stratégie numérique de la France, en mars 2015, laquelle, outre le projet de loi, devrait inclure un **plan de mesures concrètes à caractère national** et un **plan stratégique à déployer au niveau européen**.

Mme Axelle Lemaire, Secrétaire d'État chargée du numérique, a eu l'occasion d'évoquer ce dispositif devant l'Assemblée nationale lors du **débat d'orientation pour la stratégie numérique de la France**, le 14 janvier 2015.

Ce sur quoi la commission des affaires économiques du Sénat a souhaité être éclairée, à travers la présente saisine de l'Office sur le **risque numérique**, ce sont aussi **les aspects de la sécurité numérique qui seraient de nature à favoriser ou, au contraire, à entraver l'activité économique des entreprises.**

En effet, en quelques années, un nouvel espace économique est apparu, s'est déployé commodément, y compris dans le nuage numérique, utilisé par les individus comme par les entreprises. Cet espace semble avoir toujours existé ; il paraît sans limite au point que sa mise en cause ne vient pas à l'esprit même si le numérique parfois inquiète.

Au-delà des peurs comme du laisser-faire, ces préoccupations ont conduit vos rapporteurs à établir certains constats puis à opérer des choix.

---

[1] *Un glossaire des termes techniques et un lexique des sigles figurent en annexe du présent rapport.*

Les constats des rapporteurs au début de leur étude :

Certains constats découlent directement de la spécificité du numérique, à la fois familier et inconnu.

- Constat n° 1 : **une représentation mentale des frontières du numérique est difficile, voire impossible à imaginer** et, alors même qu'il faudrait pouvoir connaître les limites du numérique pour mesurer la confiance à placer en lui, ses failles, son degré de sécurité et les moyens de la garantir. **Ces limites, fluctuantes, ne correspondent pas aux frontières des États, elles sont inconnues du grand public, voire de beaucoup de professionnels du numérique**.

En réalité, fixer et surveiller les frontières du numérique ne relève pas des États mais de contrats, de rapports de force qui prennent la forme de contrats de gré à gré. C'est ainsi que **le droit nord-américain trouve, de fait, à s'appliquer partout dans le monde** et que les autres droits nationaux ne parviennent plus à appréhender, donc à maîtriser, la réalité juridique de relations qui concernent pourtant les nationaux de chaque État sur son propre territoire.

Ces frontières sont méconnues. Qui sait, par exemple, que la France a une frontière numérique commune avec l'Inde et qu'elle passe sous le site de La Défense ?

Ces frontières fluctuent, éventuellement plusieurs fois par jour, en fonction de l'état des techniques et des liens juridiques tissés.

- Constat n° 2 : **les approches traditionnelles des évolutions techniques et économiques peinent à cerner la réalité du numérique** car le contenu de notions comme celles de frontières, de confiance, de productivité et même de sécurité a évolué. Elles sont réinterprétées de façon extrêmement rapide tant par les usagers que par les fournisseurs de produits et/ou d'accès numériques.

Ces approches traditionnelles sont aussi remises en cause par les usages malveillants qui se développent sur la toile (ou *web*) : si les entreprises sont des cibles évidentes en dépit de leurs efforts de sécurité, il convient de prendre acte que les réseaux sociaux se réclamant de l'élan démocratique, empreint de bienveillance, associé à l'image de l'Internet, sont aussi, de plus en plus, utilisés par des individus malveillants et dangereux pour des échanges d'informations nuisibles et également pour des commerces illégaux comme ceux des armes et des substances illicites.

- Constat n° 3 : **l'existence de failles de sécurité du numérique est inhérente à cette technologie**. Elles sont inévitables à chaque degré d'évolution de la technique et à chaque niveau des systèmes informatiques. Ces failles sont multiples et souvent utilisées d'abord par les pirates qui les exploitent bien avant qu'elles soient explicitées par des analyses théoriques.

Ces failles peuvent être inhérentes aux logiciels, aux systèmes d'exploitation ou résulter de connexions entre réseaux (internes ou internes/externes).

Ces faiblesses intrinsèques peuvent se trouver à l'intérieur d'un matériel, d'un composant, d'un cœur de réseau mal conçu ou conçu volontairement avec une faille appelée « porte dérobée » permettant au constructeur, à l'instigation ou non d'un utilisateur, de pénétrer volontairement le réseau qu'il a contribué à construire ou d'y dérober des données de la manière la plus discrète et la plus durable possible – ou, plus simplement, à l'intérieur d'un logiciel, le plus souvent introduit lors d'un téléchargement ou *via* une clé *USB* non sécurisée.

L'existence de ces failles est souvent constatée par les utilisateurs d'un réseau avec plusieurs mois, voire plusieurs années, de retard ou n'être jamais ni constatée ni révélée – les entreprises répugnant à donner de l'écho à leurs mésaventures informatiques. Il semble cependant que le rythme de découverte des intrusions s'accélère, soit grâce à la vigilance accrue des entreprises soit en raison de l'augmentation du nombre des intrusions.

- Constat n° 4 : **les utilisateurs du numérique, généralement mal informés des risques de celui-ci, négligent trop souvent la sécurité, par faiblesse de leurs connaissances ou oubli des précautions à prendre, et/ou ignorance des moyens pour y parer**. En effet, la vigilance des services informatiques des entreprises est parfois perçue par les utilisateurs professionnels du numérique – même au plus haut niveau – comme un frein à l'activité et à la croissance de leur entreprise.

Ces failles, involontaires ou volontaires, ne sont pas exclusivement techniques ou malveillantes mais sont d'autant mieux mises à profit qu'elles sont amplifiées par la légèreté des utilisateurs. Il convient donc de prôner l'hygiène informatique.

- Constat n° 5 : **la sécurité du numérique doit être réinventée chaque jour** puisqu'elle est, par nature, impossible à penser à partir des risques avérés et des procédés de sécurité antérieurs mais doit prendre en compte, à la fois et également, les risques présents et ceux qui pourraient caractériser le futur.

- Constat n° 6 : **la dépendance au numérique des individus comme des entreprises et de la société en général ne cesse de s'accroître**.

Tant dans les usages individuels que professionnels du numérique, le perfectionnement des outils, la fascination qu'ils peuvent exercer par leurs facultés et leur apparence familière, pratique et esthétique, sont de nature à entraîner une accoutumance qui peut se transformer en dépendance voire en addiction.

Cela est particulièrement frappant chez les jeunes mais s'observe à tout âge. Dans les loisirs comme dans le milieu professionnel, **nul ne saurait**

plus se passer du numérique d'autant que celui-ci se fait nomade dans la plupart de ses outils et peut donc accompagner partout et en permanence.

Les facilités offertes par les ordinateurs portables, les messageries électroniques, la téléphonie mobile, les clés *USB* données et/ou échangées, permettent de travailler n'importe où et à n'importe quelle heure, ce qui ouvre évidemment des opportunités, mais ne laisse pas d'inquiéter.

- Constat n° 7 : **l'omniprésence du numérique rime parfois avec l'ignorance de ses possibilités comme des risques pris**.

La dépendance au numérique des individus comme des entreprises et de la société tout entière, ne cesse de s'amplifier et le décalage s'accroît entre les possibilités techniques des outils numériques et les connaissances nécessaires à leur maîtrise.

En effet, il n'est nullement nécessaire de maîtriser l'informatique pour utiliser un logiciel, un téléphone portable ou un ordinateur, pour stocker des images et des données dans un nuage numérique ou envoyer des photos et des fichiers à un tiers ou sur un site de partage en ligne, etc. La faible connaissance que nombre d'usagers ont de leur matériel devient plus inquiétante quand **cette ignorance empêche de suspecter l'existence de failles de sécurité dans les outils numériques utilisés**.

Il est singulier d'observer que, désormais, **la quête de la connexion permanente l'emporte sur toute autre considération** : chacun est attiré par la prise de courant, la connexion *Wi-Fi*, la clé *USB* prêtée ou offerte, et néglige le temps de recul, l'instant de réflexion qui permettrait, peut-être, de se demander si ces multiples possibilités ne masquent pas un fait essentiel : un flux de données peut toujours s'écouler en sens contraire à celui espéré par l'heureux possesseur de ces merveilles technologiques et ce, totalement indépendamment de sa volonté.

C'est ainsi que nombre de commerciaux emportent à l'étranger leur ordinateur professionnel avec toutes ses données, se connectent de nombreuses fois au cours de leur voyage puis s'étonnent sincèrement de voir les marchés escomptés leur échapper. Il en va de même pour nombre d'ingénieurs, pourtant mieux avertis, qui transportent des données sensibles.

Dans ce contexte, au printemps 2014, déjà éclairés par près d'une quarantaine d'auditions, vos rapporteurs ont jugé utile de proposer à tous les membres de l'Office **une séance de démonstration de la vulnérabilité des outils numériques** dont l'usage s'accroît à proportion, par exemple, de l'exploitation croisée des données massives (*big data*).

Désormais, une masse considérable de données peut être stockée et exploitée, dès à présent ou dans le futur, sur des serveurs dispersés dans le monde, dont les nuages numériques. La mobilité et la multitude des opérateurs rendent possible la collecte massive et durable de données disparates et éparses relatives à une personne ou à une entreprise.

Cette collecte ne prenant éventuellement sens qu'au regard de sa mise en ordre par l'opérateur de données massives ou par la personne à laquelle il aura transmis ces informations.

Les données massives, même éparses, prennent ainsi, progressivement, une valeur marchande, économique, pour l'opérateur, à l'insu de son client et en l'absence de tout contrôle.

Le client, dont l'être se réduit ainsi à une série de données, devient le produit : l'exploitation économique du « *petit tas de secrets* » évoqué par André Malraux débute. Personne ne l'avait prévu ; tout le monde en est l'objet.

Ce phénomène, qui s'intensifie, entraîne la création de nouveaux modèles d'affaires, attrayants mais insidieux.

En effet, l'exploitation de ces données peut ne pas être conforme à la volonté initiale de celui qui les a confiées – le plus souvent sans avoir conscience de cet acte lui-même – au fournisseur du service de stockage.

C'est ainsi qu'une photo déposée dans un espace « privé », par exemple *Facebook, Twitter ou Google*, peut être utilisée, modifiée, détournée à des fins totalement étrangères à la volonté initiale de la personne ayant placé sa confiance en cet opérateur.

Des décisions récentes ont été prises par certains opérateurs en matière d'effacement de données et ce, sous la pression de la Commission nationale informatique et libertés (CNIL) et des médias… mais toutes les questions d'ordre privé n'ont pas pour autant été résolues.

Entre angélisme et paranoïa, il est donc nécessaire de trouver une voie, non point médiane mais appropriée à chacun, personne physique ou morale, dans l'intérêt bien compris du développement économique comme de la sécurité publique et privée.

Ce qui conduit à se demander si le changement de monde, vécu actuellement, que l'on voudrait créateur d'emplois et d'activités, peut se satisfaire, pour sa sécurité, du seul outil de l'autorégulation ?

- Constat n° 8 : **la nécessité de recourir à des tiers de confiance s'impose** pour aborder ces questions sur le numérique, ses frontières, son caractère évolutif et sa complexité.

Cela ne va d'ailleurs pas sans paradoxe : le Centre de sécurité de *Thales* – comme bien d'autres – recrute des *hackers*, des pirates de la toile, agiles à déjouer les attaques informatiques menaçant les opérateurs d'importance vitale et à remédier à leurs effets. Ces pirates se muent alors en corsaires du XXIe siècle.

En complément, quand un individu, une entreprise, une administration souhaite placer tout ou partie de ses données dans un nuage de stockage numérique, il doit s'assurer que le fournisseur est **un partenaire**

de confiance apte à garantir la disponibilité, l'intégrité, la confidentialité (DIC) et la réversibilité du stockage des données et des services rendus. Ces critères objectifs de confiance peuvent d'ailleurs être exigés par contrat.

Cette notion de confiance, au temps des pirates et des nuages numériques, illustre les limites de la sécurité du numérique puisque, faute de pouvoir appréhender le degré de sécurité de tels matériels, logiciels, réseaux, centres de stockage, etc., il sera choisi de n'évaluer que le degré de fiabilité de ce tiers de confiance qui est supposé, lui, être à même d'expertiser en permanence le degré de sécurité de tout ce qu'il propose à ses clients.

Pour autant, les critères d'octroi de la confiance demeurent personnels et subjectifs. Ce qui conduit certains acteurs à faire appel à plusieurs opérateurs de confiance – qui, dans le même esprit, dupliquent eux-mêmes les données pour en mieux garantir la sécurité.

- Constat n° 9 : **la sécurité des entreprises face aux risques du numérique apparaît insuffisamment garantie**, ce qui est d'autant plus regrettable qu'elle peut être un facteur de croissance économique.

C'est l'objet même des interrogations de la commission des affaires économiques du Sénat d'estimer l'ampleur des risques encourus par les entreprises du fait du numérique.

En effet l**es failles énumérées ci-dessus rendent vulnérables toutes les entreprises** et, en particulier, celles classées parmi les opérateurs d'importance vitale.

De leur côté, les jeunes entreprises innovantes constituent des proies intéressantes pour des entreprises plus matures, à la recherche d'innovations, tout comme les entreprises de taille intermédiaire (ETI) qui tentent de développer massivement et au plus vite leurs marchés au niveau mondial.

- Constat n° 10 : **la vie quotidienne des entreprises est maintenant rythmée par des attaques informatiques** de plus ou moins grande ampleur comme par des moments de crise liés à une attaque ciblée.

L'examen du dispositif de crise prévu pour impulser une réaction immédiate et cohérente jusqu'à la fin des effets de l'attaque numérique comprend ou non le recours à une équipe spécialisée.

La prise de conscience de l'importance des questions de sécurité peut devenir un facteur de croissance pour l'économie en favorisant l'émergence d'entreprises spécialisées en sécurité numérique (encodage, cryptage, algorithmique, groupage, dégroupage, transports, duplications, etc.). La sécurité est ainsi devenue un enjeu citoyen et un intérêt économique.

- Constat n° 11 : **la vulnérabilité des opérateurs d'importance vitale (OIV) peut résulter de celle de leurs nombreux sous-traitants, clients, et personnels et être aussitôt mise à profit par leurs concurrents**.

De la sorte, **nombre d'opérateurs d'importance vitale se tournent souvent vers des sociétés propres à leur assurer une sécurité totale de leurs données comme celle du fonctionnement de l'ensemble de leurs outils numériques**. **De plus, ces tiers peuvent également, à leur tour, faire appel à des sous-traitants**. Or, comme toujours, la solidité d'une chaîne dépend de celle de son maillon le plus faible. Aussi, la sécurité des opérateurs d'importance vitale peut-elle être compromise par un sous-traitant qui n'a pu ou su veiller à sa propre sécurité numérique.

Il peut arriver aussi que la défaillance provienne d'un affaiblissement des barrières habituelles, un stagiaire, un visiteur, etc.

- Constat n° 12 : la confiance n'excluant pas le contrôle, pas plus que l'information n'exclut la formation, **la sécurité informatique doit être un enjeu de performance dans toutes les entreprises**.

Il importe que les processus internes et externes de sécurité numérique soient placés au cœur de la vie de l'entreprise impliquant l'ensemble de la hiérarchie, toutes les instances de direction, et qu'ils ne soient plus laissés à la seule charge du service informatique, bien souvent peu écouté.

- Constat n° 13 : **les conditions de la sécurité de l'informatique en nuage semblent peu développées en France**, et même les opérateurs les plus performants ne sont pas exempts de failles de sécurité, y compris internes.

Le déploiement de services en propre ou le recours aux traditionnels ressources et services associés (service de paiement électronique, gestion de la paye, puissance de calcul, etc.) peut en effet entraîner des failles massives de sécurité. Tout comme le peu de confiance accordée aux propres services des entreprises et des administrations souvent marginalisés ou au mieux perçus comme rétifs à la modernité.

Le développement rapide des solutions partagées dans les infrastructures en nuage et leur médiatisation pourraient laisser penser que l'externalisation de la sécurité informatique serait la solution miracle. Il n'en est évidemment rien et nombre d'entreprises préfèrent continuer à disposer de serveurs classiques (hébergés ou non) pour maîtriser l'ensemble de leurs informations et données. Les faiblesses sont d'ailleurs souvent davantage d'ordre humain que d'ordre technique, et c'est à cela aussi que l'entreprise doit prendre garde.

Il convient donc de déployer, dans tous les cas, une solidité de bon aloi dans l'entreprise pour que le recours à des prestataires externes soit performant, et que l'ensemble du personnel de toutes les entreprises comprenne ces questions de sécurité, notamment grâce à une information et une formation continues.

Enfin, au-delà de ces nécessaires ajustements internes à l'entreprise, il importe qu'elle connaisse de manière explicite les lieux de stockage de ses

données et qu'elle maîtrise les garanties de disponibilité, d'intégrité, de confidentialité et de réversibilité offertes par l'opérateur choisi, puisque ce sont les objectifs mêmes d'une sauvegarde de données satisfaisante s'inscrivant dans une démarche-qualité opérationnelle, validée au plus haut de la hiérarchie.

Des constats qui précèdent, vos rapporteurs ont déduit quelques choix pour orienter leurs travaux.

Choix n° 1 : **focaliser l'étude sur les acteurs publics ou privés classés comme opérateurs d'importance vitale (OIV)**.

Près de deux cents entreprises sont reconnues comme étant des opérateurs d'importance vitale en fonction de leur rôle crucial au sein de l'économie et de la société en général. Selon les sources, le nombre de ces opérateurs varie assez sensiblement mais il s'agit toujours d'entreprises dont le fonctionnement ne saurait être interrompu par quelque événement que ce soit sous peine de compromettre sévèrement le fonctionnement économique du pays.

Choix n° 2 : après avoir procédé à un tour d'horizon de ces entreprises, vos rapporteurs ont estimé que **les opérateurs d'importance vitale des secteurs des télécommunications et de l'énergie méritaient une attention particulière**.

En effet, le secteur des télécommunications est doublement sensible : d'abord en lui-même et comme support du maillage nécessaire au fonctionnement et au développement du numérique.

Quant au secteur de l'énergie, il est évident que sa sauvegarde est particulièrement cruciale puisqu'il inclut aussi bien les centrales nucléaires que les raffineries, les oléoducs, les gazoducs, les éoliennes, les centrales solaires ou encore les barrages, les transformateurs, les lignes à haute tension et même, tout simplement, le réseau « cuivre », servant d'ailleurs aussi de réseau de transport « numérique ».

C'est pourquoi, dès le stade de l'étude de faisabilité, vos rapporteurs avaient procédé à l'audition de plusieurs opérateurs d'importance vitale, parmi lesquels *Total* et la *Fédération française des télécommunications*.

Choix n° 3 : après avoir rappelé et analysé le contexte et l'organisation de la sécurité numérique, **la compréhension, même faible, du risque numérique impose l'étude détaillée de la technique de la transmission du message, du système d'information de l'entreprise pour en déduire les conditions de sa sécurisation au vu des failles constatées et des attaques subies par les entreprises**.

INTRODUCTION – L'ACTUALITÉ DE LA SÉCURITÉ DU NUMÉRIQUE

Au début des investigations de vos rapporteurs, le thème de la sécurité numérique n'occupait pas autant qu'actuellement le devant de l'actualité.

Puis il y eut l'affaire Snowden et ses rebondissements en cascade, mais pas seulement. Et, tout récemment, à la suite des attentats perpétrés à Paris, les attaques contre des sites Internet à très grande visibilité se sont multipliées et l'opinion publique a pris conscience de l'émergence d'un nouveau type de guerre dont l'arsenal comprend les atteintes à la sécurité numérique.

Avant cela, depuis quelques mois, **les incidents révélant des failles de la sécurité numérique, de plus en plus spectaculaires, se sont multipliés** : vols de fichiers de données personnelles et de numéros de cartes de crédit chez de grands distributeurs (*Target* aux États-Unis d'Amérique, etc.), chez de grands opérateurs (*Orange*, etc.) au point que la Commission nationale de l'informatique et des libertés (CNIL) a affirmé qu'il ne s'agissait pas de fatalité mais bien d'incidents mettant en cause la responsabilité de celui qui détient des données personnelles.

Mais, au-delà de ce qui peut être imputé à des attaques, il est apparu que **de grands opérateurs coopéraient avec des États pour livrer des données personnelles et, plus grave encore, se livreraient au commerce des données personnelles soit à la suite d'une information très lacunaire des droits de leurs clients, soit à leur insu**.

Ces incidents à répétition, ces stratégies délibérées commencent à émouvoir l'individu, le citoyen qui comprend, peu à peu, qu'il n'est pas l'usager bienheureux de techniques perfectionnées tendant à faire de lui un homme augmenté mais plutôt la cible, le produit des pourvoyeurs de ces techniques qui l'entourent d'objets dits intelligents au moment même où il est pris pour un sot.

La confiance dans les acteurs du numérique et dans la sécurité numérique s'érode.

Mais ces doutes n'auraient-ils pas des effets positifs dans la mesure où la nécessité n'est perceptible que dans la crise ?

Il serait permis de le penser au vu de l'indifférence de la population, des entreprises et des gouvernements à la sécurité numérique avant que les révélations de M. Edward Snowden, à l'occasion de l'affaire *Prism* ne viennent réveiller – partiellement – ces différents acteurs.

Désormais, il est possible d'évoquer certaines failles majeures de la sécurité numérique, certaines attaques, sans être suspecté d'imagination

débridée ou de perfectionnisme technique entravant l'efficacité, ce qui permet au discours des personnes entendues par vos rapporteurs d'être écouté avec davantage d'attention. Cela devrait faciliter l'imposition de nouvelles exigences de sécurité aux personnels des entreprises et un meilleur respect des consignes des services de sécurité édictées par les spécialistes placés auprès des responsables politiques ou économiques de haut niveau.

Pourtant, jusqu'alors, l'accent était plutôt mis sur la séduction au service des extensions des usages du numérique au travers d'un mécanisme toujours identique : possibilités d'augmenter ses capacités, de soigner des maladies incurables, etc.

Selon M. Fabrice Vézin, consultant e-santé et ancien responsable de la stratégie Internet de la filiale française de ***Glaxo Smith Kline (GSK),*** citant le cabinet d'études américains *Gartner*, « ***l'utilisation d'objets connectés dédiés à la santé pourrait nous faire gagner six mois d'espérance de vie*** *dans les prochaines années* ». Dans cet entretien, il reconnaît que l'automédication se développe mais refuse d'y voir les conséquences du développement de la numérisation de la santé.

De même, *Google* entreprend maintenant un tour de France des petites et moyennes entreprises françaises, dont seuls 42 % ont un site *web* actif, en arguant d'un rapport *McKinsey* de 2011 qui montrait que **les entreprises les plus actives en ligne pouvaient croître et exporter « *jusqu'à deux fois plus* » que la moyenne.**

Sans connaissances spécifiques avérées sur les nanobiotechnologies, *Google X* entend désormais se lancer dans un projet de recherche sur les nanoparticules pour diagnostiquer des maladies comme le cancer.

Au passage, *Google X* ne manquera probablement pas de collecter un maximum de données personnelles sur l'état de santé des utilisateurs potentiels de son diagnostic médical. Et cette découverte-là est certaine, proche et monétisable.

En effet, parfois, des visées autres transparaissent : « *Ce que veut Google avec la génération des voitures autonomes, c'est* ***capter le temps que les automobilistes passent dans leur voiture*** » (M. Thierry Vadieu, directeur de programme des services de mobilité chez *Renault*). Et capter les données personnelles qui vont avec ?

Mais cela n'est encore rien comparé aux objectifs de l'un des patrons de la recherche de *Google*, M. Anet Singhal, qui anticipe « *l'essor du savoir à la demande,* ***l'information parvenant aux gens avant même qu'ils ne la recherchent*** ». Pour lui, le moteur de recherche du futur sera « *le parfait assistant personnel qui vous fera bénéficier de tous les savoirs techniques****, améliorant votre processus de pensée*** ».

Pour les réticents, il ajoute : « ***Nous devons apprendre aux gens à nager avec le courant de la technologie et non à lutter contre*** ». D'autant que « *Internet a rendu les gens plus productifs* ».

Quand ce n'est pas l'amélioration de la santé ou des capacités humaines, ce sont les économies résultant de la réduction des consommations d'eau, d'électricité, de gaz, de carburant qui sont mises en avant. Ou encore la réduction des gaspillages et des déchets.

L'économie pourrait également profiter du développement de villes connectées supposées offrir un nouveau marché de 1 500 milliards de dollars en 2020 et de 3 300 milliards en 2025 (étude du cabinet *Fost & Sullivan*).

D'autres fois, la révolution numérique se pare des couleurs de la révolution industrielle et sociétale.

M. François Bourdoncle, copilote du plan « *big data* » lancé par le Gouvernement en 2013, recommande aux entreprises en tête de leurs marchés respectifs « *d'être capable de se vampiriser soi-même plutôt que de se faire vampiriser par d'autres* ». Steve Jobs, fondateur d'*Apple*, l'avait d'ailleurs parfaitement compris, et théorisait même cette autocannibalisation.

Faute d'y procéder, il pourrait advenir ce qui se dessine dans les transports urbains où le mouvement d'ouverture des données publiques (*open data* avec *Etalab*) a conduit *Google* à s'intéresser à ce secteur et signer des accords de partenariat avec des municipalités.

Dès lors, les services futurs répondront-ils réellement à l'intérêt des usagers séduits par les métamorphoses du numérique ou plutôt aux logiques commerciales ?

Et *Google*, ou autre, deviendra-t-il pour le transport ce que l'incontournable *Booking* est devenu pour l'hôtellerie, se glissant entre l'usager et les transporteurs au détriment de la relation client du professionnel du secteur et aux frais de ce dernier ?

Encore au-delà de ces nouvelles possibilités, l'espoir est mis dans l'intelligence dont seraient animés de nouveaux objets citoyens.

Au moment où le citoyen, devenu consommateur, se transforme lui-même en produit, comment refuserait-il de se revaloriser en utilisant des objets intelligents dans des logements intelligents au sein de villes intelligentes ?

Ne prévoit-on pas près de cinq cents objets connectés et communiquant entre eux dans un logement intelligent en 2022 (étude du cabinet *Gartner*) pour un coût d'environ un dollar par objet ?

Pour ceux que cela inquiéterait, Mme Sophie Breton, présidente d'*Ignes* (groupement des industries du génie numérique énergétique et sécuritaire), directrice générale de *Hager France* se veut rassurante : « *il faut* ***mettre le consommateur au cœur de la démarche et lui permettre d'être***

acteur au sein de son logement*… l'assister au sein de son habitation pour y vivre plus longtemps* ».

Peu étonnant, dans ces conditions, qu'il faille rassurer le consommateur peu enclin à utiliser le paiement mobile – moins de 5 % des paiements dans le monde et 22 % des Français seulement estiment que leur argent est en sécurité lors de paiements utilisant la technologie du sans contact. Ce qui a conduit certains banquiers à proposer : 1° des données bancaires cryptées stockées au sein d'une puce sécurisée qui se trouve dans les *Iphone* 6 et *6 Plus*, 2° la validation de chaque transaction par un code de sécurité unique, 3° la vérification de l'identité de l'auteur de la transaction au moyen du capteur biométrique *Touch ID*. D'où la naissance de nouveaux marchés.

De son côté, *Keypasco*, société suédoise, utilise deux sources d'authentification pour sécuriser un paiement : 1° l'empreinte numérique des équipements du porteur de la carte (la combinaison unique de leurs composants) et 2° la localisation géographique du porteur. À cela s'ajoute une **analyse de risque** à travers l'identification des transactions inhabituelles : en cas d'achat effectué loin de la localisation de l'intéressé ou grâce à un ordinateur inhabituel, 3° un SMS est adressé au porteur pour recueillir son accord avant paiement.

L'économie du numérique attend beaucoup de telles innovations porteuses de marchés prometteurs : **sécurité et économie peuvent converger**.

C'est dans ce contexte ambivalent de méfiance accrue et d'espoirs renouvelés face au numérique, que depuis l'année 2013, la préoccupation autour du numérique s'est traduite dans nombre de rapports, notamment parlementaires, abordant cette question sous divers angles.

Parmi ces rapports, on relève, à l'Assemblée nationale :

- « *La stratégie numérique de l'Union européenne* » par Mme Axelle Lemaire et M. Hervé Gaymard (2013)**.**

Au Sénat :

- « *La cyberdéfense : un enjeu mondial, une priorité nationale* » rapport d'information de la commission des affaires étrangères, de la défense et des forces armées du Sénat, par M. Jean-Marie Bockel (2012) ;

- « *Le numérique, le renseignement et la vie privée : de nouveaux défis pour le droit* » par M. Jean-Pierre Sueur (2014);

- « *La protection des données personnelles dans l'open data : une exigence et une opportunité* » par M. Gaëtan Gorce et M. François Pillet (2014) ;

- « *L'Europe au secours de l'Internet : démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique industrielle européenne* » par Mme Catherine Morin-Desailly (2014).

Et, au Conseil d'État :

- « *Le numérique et les droits fondamentaux* » (2014).

Aucun de ces rapports n'avait comme objectif unique la sécurité numérique alors que les questions qu'ils abordaient étaient, bien évidemment, sous-tendues par l'existence voire l'exigence de ladite sécurité.

Cependant certains de ces rapports reposent sur des raisonnements dans l'air du temps mais faisant trop peu de cas des exigences de la sécurité numérique.

C'est ainsi que, dans le rapport sénatorial sur l'*open data*, il est dit que, nonobstant les incertitudes liées à cette ouverture et les dangers que celle-ci ferait courir aux individus, il était nécessaire « *d'y aller* » puisque cela s'inscrit dans un élan général :

« ***Ces failles ne remettent pas en cause la pertinence de l'ouverture des données publiques, mais la façon dont elle est conduite.*** *Loin de trouver là des raisons de freiner un mouvement dont l'utilité sociale est acquise, la mission d'information y a vu plutôt l'opportunité de donner un nouvel élan à l'ouverture et au partage des données publiques, en définissant une doctrine et une méthode qui garantissent la meilleure protection des données personnelles possible. Car,* ***une fois cette protection assurée, aucun obstacle au déploiement de l'*****open data** ***n'est plus légitime****.* ».

De même, dans le rapport sur « *Agir pour une France numérique : De l'audace, encore de l'audace, toujours de l'audace…* » des députées Corinne Erhel et Laure de la Raudière, le modèle américain est pris comme référence et le seul avenir possible serait l'imitation en tout point de ce précédent – pourtant inimitable par bien des aspects – dans l'espoir d'un miracle économique réalisé automatiquement par l'imitation de la Silicon Valley, soulignant que :

« *l'avenir est exaltant si l'on accepte aujourd'hui de pleinement basculer dans l'âge du numérique* » ;

« *Il faut prendre conscience que l'économie numérique se nourrit des failles qui existent dans nos systèmes, notre économie et nos politiques publiques : le numérique s'engouffre là où le XXIe siècle n'a pour l'instant pas su apporter de réponse pertinente* ».

Toutefois, ce rapport reconnaît que : « ***La cybersécurité est un enjeu essentiel*** *et* ***il faut traiter le plus en amont possible les risques de vulnérabilité des réseaux et des entreprises critiques et stratégiques*** ». Mais le rapport ne développe pas ce thème.

Malheureusement, aucune des personnes entendues par vos rapporteurs n'a semblé croire que le pas en avant au bord du gouffre de l'*open data* ou des *big data* ne serait de nature à permettre de marcher dans le vide. Pas davantage, la possibilité d'imiter les États-Unis d'Amérique n'a été indiquée comme l'unique piste à suivre.

Bien au contraire, les spécificités françaises et européennes ont toujours été soulignées et les suggestions de recommandations impliquant à la fois des efforts dans les comportements, des innovations, de la clairvoyance et beaucoup d'investissement n'ont jamais été présentés comme des voies aisées à suivre.

Le rôle de l'OPECST est précisément de souligner, dans tous leurs aspects, les problématiques scientifiques et technologiques sous-tendant les choix à effectuer pour que, dans la durée, soit menée **une analyse exigeante permettant de sensibiliser, d'éduquer, de concevoir une sécurité numérique fondée sur une défense dans la profondeur**, à peine esquissée aujourd'hui.

C'est donc une construction réfléchie plus qu'un acte de foi que vos rapporteurs proposent à l'OPECST à travers leurs propositions de recommandations tendant à n'utiliser qu'à coup sûr l'outil numérique puisque l'outil numérique ne saurait être sûr à tout coup.

Après avoir évoqué, dans un premier temps, le contexte international, les règles européennes et nationales régissant l'Internet, une plongée dans le numérique au service de l'entreprise sera effectuée pour montrer comment le numérique structure et fragilise ces acteurs économiques, *a fortiori* lorsque des attaques exploitent les failles existantes.

Mais ces failles ne pourraient-elles, aussi, constituer des opportunités de construire des systèmes d'information plus solides, avec des acteurs de confiance, sans remettre en cause les droits fondamentaux ni compromettre les bases d'un développement durable ?

CHAPITRE PREMIER – LE CONTEXTE INTERNATIONAL DE LA SÉCURITÉ NUMÉRIQUE DES ENTREPRISES

Pour situer la problématique de la sécurité numérique des entreprises, il est indispensable de replacer l'évolution du numérique dans le contexte mondial, européen, national, caractérisé par des rapports de force politiques, économiques, juridiques s'appuyant sur des techniques.

Les vitesses d'évolution de ces rapports de force comme de ces techniques et leurs interactions mutuelles rendent difficile l'appréhension des mesures à prendre pour assurer une meilleure sécurité numérique aux entreprises et, en particulier, aux opérateurs d'importance vitale et à leurs sous-traitants.

L'organisation de la sécurité numérique résulte de régulateurs officiels et d'une autorégulation. Elle est à la fois mondiale et nationale et doit concilier libertés et efficacité opérationnelle – figure en annexe un « *schéma de la sécurité numérique : instances publiques ou privées en charge de la sécurité numérique pouvant concerner la France* ».

Au cœur de la sécurité numérique de l'entreprise, se trouve la nécessité d'**évaluer cette sécurité** selon l'approche responsable propre au monde de l'entreprise.

Cependant, des cas les plus spectaculaires jusqu'au chantage au coin du clavier, les entreprises sont exposées, leurs savoir-faire menacés. Les constats sur la mise en œuvre des solutions de sécurité ne sont donc pas satisfaisants.

Cela provient-il d'un manque de connaissance ? De l'ampleur du problème ou d'une renonciation fataliste ? De la difficulté récurrente d'obtenir, pour décider, les chiffres précis sur les risques encourus ? De l'incapacité d'évaluer les enjeux de valeurs ou d'informations immatérielles ? Du manque d'outils pour les appréhender ?

Ou l'importance des coûts de la sécurité numérique, en personnes et moyens matériels, est-elle dissuasive ? La confiance dans le numérique doit-elle être favorisée plutôt par des acteurs privés que par des acteurs publics ? L'accompagnement juridique ou technologique fait-il défaut ? L'inconsistance des règles et lois relatives au maintien de la conformité en matière de sécurité numérique est-elle nocive ?

Les États ont-ils abdiqué leur rôle ou, au contraire, surjoué celui-ci au détriment des libertés ? Des obligations nouvelles doivent-elles être imposées ? L'innovation numérique s'oppose-t-elle aux savoir-faire de l'entreprise ?

Selon les entreprises et les incidents considérés, ces facteurs se combinent pour faire de la sécurité numérique une question clé.

Dans ce contexte, l'organisation que la société met en place pour assurer ou faciliter la protection des entreprises face au risque numérique joue un rôle essentiel dont la cohérence peut s'apprécier à partir de l'analyse des incidents, des données recueillies par des observatoires spécialisés, de l'articulation entre les normes techniques et juridiques.

I. LA GOUVERNANCE TECHNIQUE DU NUMÉRIQUE À L'ÉCHELLE MONDIALE

L'Internet s'est insinué dans la vie de chacun, peu à peu ou très rapidement, sans que la question de sa gouvernance ne vienne par priorité à l'esprit.

L'Internet a d'abord été perçu comme un espace de liberté, d'accès à des connaissances – intellectuelles ou sociales.

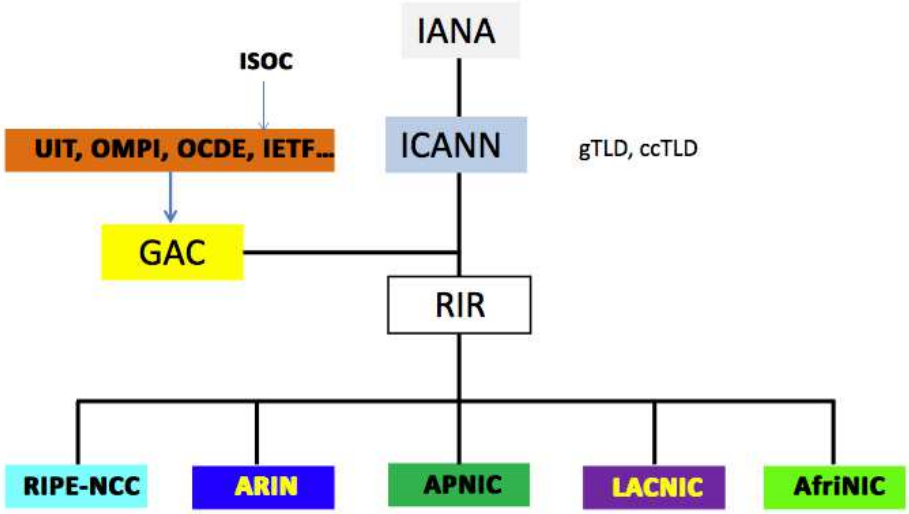
Et pourtant, comme l'Internet supposait une organisation, celle-ci, quoique peu visible, se trouvait forcément dans certaines mains.

A. LA GOUVERNANCE MONDIALE DE L'INTERNET

Compte tenu de la taille considérable de l'Internet, lorsque deux interlocuteurs géographiquement distants, situés dans des pays éloignés, souhaitent échanger, **il a été nécessaire de définir des zones de routage et d'adressage**. Avec plus de 440 000 routes en 2013, des zones de routage ont été définies et hiérarchisées pour former des zones de relais. Le gigantisme d'un tel ensemble a posé la question de sa gestion d'où la décision de proposer une gouvernance technique à l'échelle mondiale.

À l'heure actuelle, **l'attribution des zones d'adressage *IP* est organisée par continent** comme le présente l'organigramme ci-après.

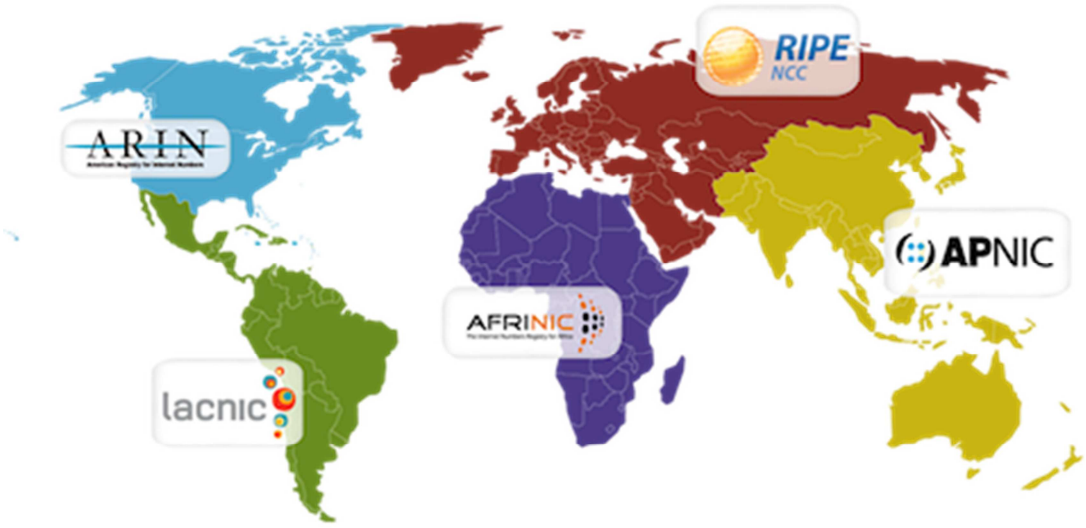
Schéma n° 1 : Les zones d'adressage *IP* de la gouvernance mondiale de l'Internet



Source *: ICANN*

La gouvernance de l'Internet est indispensable pour répartir les adresses *IP*, les noms des domaines *DNS* et d'autres éléments qui contribuent au fonctionnement du protocole Internet.

Actuellement, **l'organisation de cette gouvernance ne résulte d'aucun texte international**.



Source *: ICANN*

B. LA GOUVERNANCE MONDIALE DE LA SÉCURITÉ

Dans sa résolution 65/41 du 8 décembre 2010 intitulée « *Les progrès de l'informatique et de la télématique et la question de la sécurité internationale* », l'Assemblée générale des Nations Unies s'est déclarée préoccupée par le fait que **les « *technologies et les moyens [informatiques] risquent* *d'être utilisés à des fins incompatibles avec le maintien de la stabilité et de la sécurité internationales et* *de porter atteinte à l'intégrité de l'infrastructure des États, nuisant ainsi à leur sécurité dans les domaines tant civils que militaires*** ».

Aujourd'hui, la question de la gouvernance mondiale de l'Internet est posée, la nécessité de sa réforme admise mais ni les objectifs ni le calendrier ne s'imposent d'eux-mêmes car d'importants enjeux sont en cause.

La toile d'araignée qui enserre le monde, le *Net*, l'*Internet*, le *web*, est en contact avec tous les domaines.

Les règles discrètes de sa mise en place et de son organisation ont bénéficié à des sociétés commerciales et à leur État d'origine tandis que la population mondiale se prêtait avec ardeur et inconscience à cette mainmise mondiale sur les esprits comme sur les objets.

Le tissage de la toile d'araignée mondiale a été effectué par quelques acteurs inconnus comme :

- l'*IAB*, l'*Internet Architecture Board*, désigné par l'*Internet Society*, comité chargé de la surveillance et du développement de l'Internet ;

- l'*ICANN*, l'*Internet Corporation for Assigned Normes and Numbers*, qui gère le fichier racine du système des noms de domaine assurant la correspondance entre les noms de domaine et les adresses *IP* ; de droit californien, **cette association est supervisée par le Département du commerce américain** ;

- l'*IETF*, l'*Internet Engineering Task Force*, en charge de l'ingénierie de l'Internet, qui participe à l'élaboration de normes pour l'Internet ;

- l'*ISOC*, l'*Internet Society* ;

- le *W3C*, *Worldwibe web consortium*, qui est l'organisation pour le réseau mondial.

La gouvernance actuelle de l'Internet résulte de l'action conjuguée de l'ensemble de ces acteurs, tous américains, dont les instances de direction comprennent notamment des géants américains du numérique.

C'est seulement depuis une dizaine d'années qu'une réflexion a été engagée sur cette curieuse structure à travers la création, en 2005, de l'*Internet Governance Forum* (*IGF*), espace de dialogue multiparties prenantes mais non interétatique.

Il a fallu l'affaire Snowden, en 2013, c'est-à-dire la révélation publique de l'identité de l'araignée en attente au cœur de sa toile, la *National Security Agency* (*NSA*), pour que se tienne, en avril 2014, au Brésil, une conférence mondiale sur la gouvernance de l'Internet dont **la déclaration finale a condamné la surveillance en ligne et affirmé des principes fondateurs pour un Internet libre et démocratique**.

Pour conserver le maximum de leurs prérogatives actuelles, **les États-Unis d'Amérique ont proposé, en mars 2014, d'entamer une privatisation de la gouvernance de l'Internet, probablement afin d'éviter la création d'une organisation intergouvernementale ou l'influence de tout autre État**. À noter que le contrat liant l'*ICANN* au département du commerce américain expire en septembre 2015.

Face à cette situation, la mission commune sénatoriale d'information sur la démocratisation de la gouvernance de l'Internet[1] a proposé une nouvelle architecture reposant sur :

- l'élaboration d'un traité international consacrant les principes fondateurs du *Net* mondial de São Paulo de 2014 et entraînant la **globalisation de la gouvernance de l'Internet** ;

- la création d'un Conseil mondial de l'Internet (résultant de la transformation du Forum pour la gouvernance de l'Internet ou *IGF*) ;

- la transformation de l'*ICANN* en une *WICANN* (*WorldICANN*) de droit international ou de droit suisse tout en organisant une **supervision internationale du fichier racine des noms de domaine** ;

- l'instauration d'un mécanisme de recours indépendant et accessible permettant la **révision d'une décision de la *WICANN*** ;

- l'établissement d'une séparation fonctionnelle entre la *WICANN* et les fonctions opérationnelles d'attribution des noms de domaine de premier niveau (la racine), des adresses *IP* et des numéros des systèmes autonomes (ASN) aux registres Internet régionaux et la définition des paramètres des protocoles Internet (liste des numéros de ports, etc.) ;

- la définition de critères d'indépendance pour les membres du bureau de la *WICANN* afin d'**éliminer les conflits d'intérêts**.

La nouvelle architecture de la gouvernance de l'Internet proposée par la mission d'information sénatoriale ne rencontre évidemment pas l'enthousiasme de l'***ICANN*** qui **entend bien s'autoréformer à sa manière**.

La Commission européenne a présenté plusieurs communications sur ce sujet appelant à une **gouvernance de l'Internet plus transparente,**

---

[1] « L'Europe au secours de l'Internet : démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne » *présidée par M. Gaëtan Gorce et dont le rapporteur était Mme Catherine Morin-Desailly (Sénat, n° 696, 2013-2014).*

responsable et inclusive mais tous les membres du Conseil européen sont loin d'être sur la même ligne. En fait, l'alignement sur les États-Unis d'Amérique séduit encore le Royaume-Uni, la Suède, la Pologne, l'Estonie, la République Tchèque et les Pays-Bas, sans compter l'Allemagne, en dépit de l'espionnage avéré des communications privées de la Chancelière par les États-Unis.

Toutefois, **à São Paulo, l'Union européenne a affirmé son soutien à un Internet unique, ouvert, libre, sûr, fiable et non fragmenté**.

Devant le Sénat, le 23 octobre 2014, Mme Axelle Lemaire, secrétaire d'État chargée du numérique, a indiqué que **la France souhaite que le Conseil de l'Union européenne prenne position en faveur de : « *la liberté d'expression, la liberté d'association, la liberté d'information, le droit au respect de la vie privée, l'accessibilité, l'architecture ouverte d'Internet, une gouvernance multipartite, ouverte, transparente, redevable, un système qui soit inclusif, équitable et qui promeuve des standards ouverts* »**.

Face aux États-Unis d'Amérique, soudain favorables à une privatisation de la gouvernance de l'Internet, l'Union européenne s'oriente vers une moralisation incluant le droit de regard des États – et non plus d'un seul - sur la gouvernance de l'Internet.

Si vos rapporteurs ont tenu à effectuer ce rappel de la réalité et de l'évolution souhaitable de la gouvernance de l'Internet, c'est pour montrer que **les enjeux de la sécurité des réseaux numériques se situent dans un cadre qui est lui-même construit comme un lieu d'insécurité**.

Dès lors, placer ses informations, ses intérêts dans une toile d'araignée implique l'acceptation d'être une proie. Une prise de conscience de cette réalité par les individus comme par les entreprises ne peut que stimuler leur réflexion.

On ne surfe sur le *Net* que si l'araignée veut bien, momentanément, octroyer cette liberté étroitement surveillée.

II. LA GESTION MONDIALE DES INCIDENTS DE SÉCURITÉ NUMÉRIQUE

A. LES SERVICES DE VEILLE

Depuis les années 1990, des services de veille à l'échelle institutionnelle ont été proposés ; la plupart de ces services résultent d'initiatives nord-américaines.

Le *National Institute of Standards and Technology (NIST)* dépend du département américain du commerce, il est aujourd'hui l'entité organisationnelle et opérationnelle chargée de **favoriser la compétitivité des entreprises confrontées à l'usage de technologies complexes**. À son origine, en 1901, laboratoire de sciences physiques, le *NIST* a étendu son périmètre, depuis la fin des années 1980, à la **normalisation des technologies de l'information**.

Le *NIST* est chargé par le gouvernement nord-américain d'héberger et de gérer la base de connaissance des vulnérabilités au niveau national (*National Vulnerability Database*), le *NIST* est un institut puissant à l'origine de l'emploi ou du développement de la plupart des normes à des fins de veille en sécurité (bulletins *OVAL*, *CVE*, *CVSS*).

Il en résulte que **toute la connaissance de la majorité des vulnérabilités est aujourd'hui concentrée et fédérée sur le *Security Content Automation Protocol (SCAP)*, la plate-forme du *NIST***, née de l'idée d'une mise en réseau de connaissances de sécurité entre la recherche scientifique et industrielle. **Au travers de la plate-forme *SCAP*, le *NIST* centralise et diffuse les événements de sécurité considérés comme dangereux afin de favoriser la coopération des efforts au niveau national et international.** *SCAP* permet également de produire une connaissance unique et commune sur les vulnérabilités. Dans son standard, *NIST* SP800-126, le *NIST* propose une normalisation des vulnérabilités afin de les exprimer sous un même format.

Vers la fin des années 1980, à la suite d'une vulnérabilité qui avait touché plus de 10 % des ressources Internet, l'État nord-américain s'est également doté d'un centre de traitement des incidents informatiques, le *CERT/CC* (*Computer Emergency Response Team Coordination Center*).

Le *CERT/CC* fut créé par le *SEI*, sous l'impulsion de la *DARPA (Defense Advanced Research Projects Agency*) et du *DoD (United States Department of Defense*), installé au cœur de la *Carnegie Mellon University*. Après cet incident fondateur, la mission du *CERT/CC* a été de fédérer des équipes mixtes, industrielles et scientifiques, pour **freiner la multiplication des failles des systèmes**. Cette stratégie devait préserver la compétitivité des entreprises utilisatrices de logiciel en opposant un acteur de poids aux éditeurs à l'origine des failles de sécurité toujours plus nombreuses.

C'est pourquoi, dès 1993, l'une des missions du *CERT/CC* a été de **diffuser ces vulnérabilités au grand public sous forme des bulletins « *bugtraq* », mettant en quelque sorte les éditeurs de logiciels en demeure de corriger leurs failles**. Depuis cette date, **60 000 vulnérabilités ont fait l'objet d'une analyse fine du *CERT* sur plus de 27 000 logiciels conduisant pour la majorité à des correctifs**. **Le *CERT/CC* est devenu une référence, publiant gratuitement au quotidien une liste des vulnérabilités accompagnées d'une analyse détaillées.**

Le *SCAP* et l'*US-CERT* font partie de ces initiatives nord-américaines de nature communautaire soutenues par le *Departement of Homeland Security* (*DHS*), au lendemain des attentats du 11 septembre 2001. En septembre 2003, le *DHS* a annoncé la création de l'*US-CERT,* résultant d'un effort conjoint avec le Centre de coordination *CERT*. *US-CERT* s'appuie sur les capacités *CERT/CC* pour aider à prévenir les cyberattaques, protéger les systèmes et répondre à ces agressions.

Schéma n° 2 : Page d'accueil de l'*US-CERT*



Source *: Internet*

Le succès du *CERT/CC* a entraîné le développement d'un réseau à l'échelle mondiale permettant de fédérer les connaissances de sécurité scientifiques et industrielles et d'**offrir un service aux usagers du monde entier**.

Le *CERT/CC* a mis en place un mécanisme de certification ; chaque État ou entité, désireux d'être acteur de sa sécurité, peut rallier ce réseau.

Le *CERT/CC* délivre la certification à tous les *CERT*.

En France, une vingtaine de *CERT* sont actuellement en service, certains sont des *CERT* d'État comme l'*ANSSI* dont la page d'accueil figure ci-après, d'autres dépendent de secteurs professionnels.

L'intérêt opérationnel de tous ces *CERT* est d'être reliés entre eux à différents niveaux, national et international afin d'échanger leurs informations sur la découverte de nouvelles vulnérabilités. Toutes celles-ci sont centralisées par le *CERT/CC* et identifiées par le *SCAP* ; le rôle de ce

dernier, à l'image de l'*ICANN*, est d'en dresser une identification unique à l'échelle mondiale.

Dans un contexte où le numérique constitue un enjeu stratégique, on peut s'interroger sur la neutralité et sur la pérennité du *SCAP*.

Schéma n° 3 : Page d'accueil de l'ANSSI



***Source** : Internet*

B. LES INQUIÉTUDES GRANDISSANTES DES ÉTATS FACE AU NUMÉRIQUE

Du côté des nations, la situation est également inquiétante, celles-ci sont exposées à des attaques à l'échelle des pays, les attaquants à la solde d'États s'organisent en véritable armée.

La Commission européenne a adopté une communication afin d'améliorer la protection des infrastructures critiques de l'UE (IC) contre le terrorisme, l'arrêt de ces infrastructures pourrait provoquer des pertes en vies humaines et en biens matériels ainsi que l'effondrement de la confiance des citoyens dans l'Union européenne. Un train de mesures est engagé.

L'*Organisation du traité de l'atlantique nord* (OTAN) est également partie prenante dans la lutte contre le terrorisme. Elle *n'est pas restée inactive en matière de cybersécurité puisque, en 2008, à la suite de la cyberattaque qui a paralysé l'Estonie en 2007, un* ***centre d'analyse et d'expertise en matière de cybersécurité*** *a été mis en place à Tallinn. Ce centre* est d'ailleurs régulièrement la cible de violentes attaques en déni de service.

En 2008 également, l'OTAN créait la ***Cyber Defense Management Authority (CDMA)****, autorité politique ayant pour mission de* ***lancer et coordonner des « mesures immédiates et efficaces de cyberdéfense chaque fois que les circonstances l'exigent*** *» et, également, d'organiser des exercices de simulation de cyberattaque à grande échelle.*

Un élément de l'approche de l'Alliance atlantique a été d'encourager une plus grande coopération entre les nations pour faire face aux cyberattaques. L'Union européenne est devenue désormais partie prenante dans la mise en œuvre de la confiance dans les systèmes d'échange électronique. **La prise de conscience de la dangerosité des menaces sur l'Internet et *via* les modes d'échanges électroniques modernes constitue l'enjeu de la prochaine décennie.**

Les mesures les plus avancés semblent avoir été prises au Danemark où, afin d'instaurer la confiance dans les systèmes de paiement électronique, une infrastructure de paiement sécurisé étatique a été déployée. De même, pour répondre au besoin de sécurité du citoyen, une campagne a été menée sous forme de trois cent trente-trois initiatives différentes au travers du pays sous le nom de *NetSafe Now !*, ce qui constitue une avancée considérable.

Ce qui était évoqué à mots couverts ou comme des hypothèses de réflexion sur les développements éventuels d'affrontements cybernétiques entre États, l'est maintenant ouvertement, notamment depuis le 24 novembre 2014, lorsqu'est survenu le piratage informatique du studio *Sony Pictures*, attribué à la Corée du Nord en représailles de l'annonce de la diffusion d'un film intitulé *The Interview* ou « *L'interview qui tue* », qui montre l'assassinat du chef d'État sud-coréen Kim Jong-un par des journalistes recrutés par la *CIA*.

Bien plus, dès le 5 décembre, des employés de *Sony Pictures* ont été la cible directe de menaces des pirates. Puis, le 16 décembre, il s'est agi de menaces d'attentat contre les salles qui projetteraient ce film, ce qui a entraîné, dès le lendemain, la renonciation de *Sony Pictures* à sortir son film, les milliers d'exploitants de salle désirant éviter tout risque.

Le 19 décembre, le *FBI* a directement désigné la Corée du Nord comme le pilote de cette attaque et le président nord-américain a promis une réponse « *proportionnée en lieu et temps voulus* » et a qualifié d'erreur la renonciation de *Sony Pictures*.

C'est la première fois que les États-Unis d'Amérique accusent nommément une nation étrangère d'avoir mené une cyberattaque.

Finalement, plus de trois cents salles ont décidé, au nom de la liberté d'expression, de projeter le film qui a été également disponible, dès le 24 décembre, sur l'Internet.

Techniquement, le *FBI* a révélé que la signature nord-coréenne serait exprimée par des **lignes de code informatique**, un **cryptage des algorithmes**, des **méthodes d'expression des données** analogues à celles utilisées par le régime nord-coréen lors d'une attaque contre des banques et des médias sud-coréens en mars 2013. De plus, **des adresses *IP* associées à des infrastructures nord-coréennes** auraient communiqué avec celles identifiées comme responsables du piratage.

À noter que, dès juin 2014, la Corée du Nord avait qualifié la réalisation de *The Interview* d'« *acte de guerre* » et menacé de représailles « *fortes et sans pitié* ».

À son tour, M. John McCain, sénateur républicain, a qualifié d'« *acte de guerre* » le piratage informatique dont *Sony Pictures* a été victime.

Dans le même temps, la Russie et la Corée du Nord ont multiplié les signes de leur rapprochement, notamment avec l'invitation lancée au dirigeant nord-coréen de se rendre à Moscou en mai 2015.

Parallèlement, le 22 décembre 2014, pendant près de neuf heures, la liaison Internet entre la Corée du Nord et le monde – qui passe par la Chine –a été interrompue. Cela a-t-il été l'œuvre de la Chine, des États-Unis d'Amérique, de la Corée du Nord elle-même pour prévenir les effets d'une cyberattaque nord-américaine ? Ou de la Corée du Sud victime, le 9 décembre 2014, du piratage des plans de certains réacteurs nucléaires et de leurs circuits de refroidissement, ainsi que des données personnelles de près de 11 000 employés – cyberattaque attribuée par la Corée du Sud à la Corée du Nord ?

Dans le même temps, le 25 décembre 2014, même si cela est passé davantage inaperçu, une panne géante a affecté les serveurs *Xbox live* de *Microsoft* et *Playstation live* de *Sony*, menacés début décembre d'une cyberattaque par un groupe ambitionnant de mettre définitivement hors ligne ces deux réseaux.

Ces événements récents montrent que, **de la cybersécurité à la cyberguerre, les frontières séparant les risques civils des risques militaires, et celles séparant les risques des dangers, sont de plus en plus impossibles à discerner** et que la recherche d'un niveau élevé de sécurité numérique pour les entreprises doit être, plus que jamais, et dans les plus brefs délais possibles, une réelle priorité des États comme de leurs acteurs de la sécurité civile dont chaque utilisateur du numérique.

C. LES RAPPORTS DE FORCE ENTRE LES GÉANTS DE L'INTERNET, LES ÉTATS, LES ENTREPRISES ET LES CITOYENS

Là où le droit devrait énoncer les règles applicables, ce sont actuellement des rapports de force qui priment.

Pendant que le droit tarde à s'élaborer, des situations de fait se créent, risquant de limiter les marges de créativité des législateurs.

L'exemple de *Google* dans l'Union européenne illustre bien ces contradictions.

Premièrement, tandis que l'Union européenne s'interroge depuis cinq années sur l'existence de l'**abus de position dominante** dont le moteur de recherche *Google* serait coupable aux dires d'une trentaine de plaignants, le Parlement européen a voté une motion appelant au démantèlement de *Google* et l'Espagne a voté une **taxe *Google***, pour protéger la propriété intellectuelle des outils des éditeurs de presse utilisées gratuitement par *Google Noticias*, devant entrer en vigueur au 1er janvier 2015.

À propos de ces initiatives, il faut d'abord relever que poursuivre *Google* pour ces abus de position dominante, en raison du recours au poids de ses 90 % de parts de marché européen pour promouvoir l'ensemble de ses services au détriment de ceux de ses concurrents, suppose de communiquer à *Google* les griefs retenus contre lui et d'entamer une procédure qui durera des années… au cours desquelles l'abus supposé perdurera ou s'aggravera. D'où la préférence pour la conciliation du commissaire européen à la concurrence, M. Joaquin Almeira, en fonction de 2009 à 2014.

Quant à la **motion votée par le Parlement européen**, au-delà de son écho médiatique, d'ailleurs assez limité en dépit de l'audace de ce texte, il est permis de se demander, à ce stade, si sa portée n'est pas plus symbolique que réelle.

Enfin, la simple annonce de la **taxe *Google* espagnole** a déjà conduit *Google* à annoncer la fermeture de son service d'actualités, ce qui a entraîné le recul immédiat des éditeurs de presse que la taxe devait protéger des emprunts gratuits de *Google*.

Face à cette situation, une réaction européenne ne semble pas envisageable, ne serait-ce que parce que la France a obtenu de *Google*, depuis 2013, le financement du fonds pour l'amélioration numérique de la presse.

Deuxièmement, aucun pays n'a semblé en mesure de mettre en place un impôt obligeant *Google* à s'acquitter d'un quelconque paiement proportionnel aux profits réalisés dans chaque pays considéré.

Tout au plus, une directive devrait permettre le versement de la **taxe sur la valeur ajoutée** dans le pays où une œuvre cinématographique ou une chanson est achetée sur *Apple* ou *Google*.

Troisièmement, la mise en place par *Google*, en 2014, des **modalités du droit à l'oubli**, à la suite de la décision de la Cour européenne de justice, laisse *Google* seul juge de la pertinence des quelque 200 000 demandes de suppression de liens formulées.

De plus, dans un proche avenir, à savoir au cours de l'année 2015, l'Union européenne devrait adopter un **règlement sur les données personnelles** afin de soumettre ces derniers à la loi du pays où se trouve la personne concernée, quelle que soit la localisation des serveurs hébergeant ces données.

Enfin, **les six CNIL européennes sont en contentieux avec *Google*** à qui elles reprochent d'avoir modifié unilatéralement sa **politique de confidentialité**, qu'il s'agisse de messagerie, de recherche ou de stockage.

À en juger par le test que viennent d'imposer à *Booking* trois instances nationales de régulation française, italienne et suédoise, agissant de concert contre les clauses imposées par ce site de réservation en ligne aux hôteliers, ce type d'action concertée pourrait être une voie plus rapide et efficace que des solutions institutionnelles européennes.

Mais l'image d'un face à face entre *Google* et les États doit être complétée par la faculté de la coopération entre ceux-ci.

Depuis des années, *Google* accède aux demandes de gouvernements souhaitant obtenir les données privées des internautes détenues par cet opérateur.

Depuis 2010, www.google.com/governmentrequests/ permet de connaître, État par État, le nombre de requêtes gouvernementales adressées à *Google*, soit pour disposer de données privées, soit pour supprimer des contenus.

Cela consiste à préciser que ***Google* détient les lieux de connexion, la configuration des ordinateurs connectés, l'historique de la navigation, le contenu des recherches effectuées, le contenu des messages électroniques**, etc.

Les entreprises n'échappent pas à ce système.

De la sorte, ***Google* détient bien plus d'informations sur des individus et des entreprises que la plupart des États et une puissance financière surpassant également celle de nombre d'entre eux**.

À ce niveau, cela fait de cette entreprise privée nord-américaine – comme de toutes celles à son niveau – **un acteur politique**.

III. LE PROJET D'ACCORD DE LIBRE ÉCHANGE ENTRE LES ÉTATS-UNIS D'AMÉRIQUE ET L'UNION EUROPÉENNE

En février 2013, ont été lancées des négociations relatives à la conclusion d'un accord transatlantique global sur le commerce et les investissements entre les États-Unis d'Amérique et l'Union européenne.

À ce jour, déjà quatre cycles de discussion ont été conclus traduisant la volonté des deux parties d'avancer à un rythme extrêmement rapide en

vue de « *créer un grand marché transatlantique déréglementé au sein duquel seraient substitués la volonté et les intérêts économiques aux lois votées par les parlements nationaux et à la législation européenne* »[1].

Il est envisagé que, une fois adopté cet accord, son champ puisse être étendu sans qu'il soit besoin de rouvrir les négociations en fonction des nouveaux domaines de convergence identifiés.

Depuis fin 2013, il est publiquement établi que les États-Unis d'Amérique ont espionné à grande échelle les télécommunications et les réseaux informatiques de tous les Européens en charge de la négociation de cet accord international.

C'est pourquoi **vos rapporteurs tiennent, pour deux raisons, à évoquer la négociation de cet accord dans la mesure où il peut porter sur le numérique – dont la sécurité est pourtant un enjeu de souveraineté nationale – et où l'insécurité du numérique vient parasiter sa négociation, voire démontrer le danger de sa conclusion**.

L'Union européenne va-t-elle exiger le respect du droit européen en matière de respect du droit à la vie privée et de protection des données personnelles par le texte final de cet accord ?

Va-t-elle exiger l'exclusion de la protection des données personnelles de ces négociations commerciales ?

Va-t-elle exiger que les citoyens européens jouissent du même niveau de protection que les citoyens nord-américains ?

Qui se souvient de la déclaration, en juin 2013, de Mme Viviane Reding, commissaire chargée de la justice dans la précédente Commission européenne, selon laquelle « *on ne peut pas négocier sur un grand marché transatlantique s'il y a le moindre doute que nos partenaires ciblent des écoutes vers les bureaux des négociateurs européens* » ?

En évoquant cette négociation en cours, vos rapporteurs tiennent à insister sur l'existence de **quatre chronologies parallèles intéressant l'avenir du numérique** : celle de la mise en place d'une gouvernance internationale de l'Internet, celle de la négociation de l'accord de libre-échange transatlantique, celle de l'élaboration d'un nouveau règlement européen relatif au numérique et, enfin, celle d'une nouvelle loi française sur le numérique.

Il est essentiel que des garanties européennes et internationales s'imposent dans la protection des données personnelles et la gouvernance de l'Internet avant que ne soient adoptées des clauses de l'accord de libre-échange relatives au numérique.

---

[1] *M. André Chassaigne, député, rapporteur pour la commission des affaires étrangères de l'Assemblée nationale du projet d'accord de libre-échange entre les États-Unis d'Amérique et l'Union européenne. Assemblée nationale, rapport n° 1938, XIVe législature.*

Bien plus, **le numérique ne devrait pas être inclus dans l'accord commercial car le numérique englobe le commercial et non le contraire**.

Il conviendrait donc de **considérer le numérique comme justifiant une exception numérique à l'instar de l'exception culturelle. En conséquence, ce secteur serait exclu des négociations commerciales**.

Et ce d'autant plus que **les modalités d'arbitrage envisagées dans l'accord de libre-échange soumettent les États signataires à la volonté des entreprises dominantes du marché** à travers le recours à un tribunal supranational privé dénommé « *panel d'arbitrage* ».

Même en l'absence de cet accord, cette situation est déjà celle observée dans le domaine du numérique ; il est urgent de la modifier en **évitant de transformer cette situation d'infériorité momentanée, de fait, de l'Union européenne dans le domaine du numérique en situation de droit définitive**.

IV. VERS UNE EUROPE DU NUMÉRIQUE COHÉRENTE ?

Dès 2010, l'Union européenne a publié « *Une stratégie numérique pour l'Europe* » figurant parmi les sept initiatives phares de la stratégie Europe 2020, révisée en 2010 : « *Une stratégie numérique pour l'Europe : faire du numérique un moteur de la croissance européenne* ».

En 2013, l'affaire Poison a montré que les fournisseurs de services en ligne disposaient de moyens de cybersurveillance pouvant être utilisés pour contrôler les données personnelles au détriment des individus voire des États.

Face à cela, **vos rapporteurs se sont interrogés sur la place accordée à la sécurité dans ces ambitions européennes de développement du numérique**.

La proposition de directive du Parlement européen et du Conseil du 7 février 2013 concernant « *des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union* » ambitionne de **renforcer la coopération intra-européenne pour affronter les crises dépassant la dimension nationale**.

Ce projet de texte envisage d'**imposer à chacun des États membres d'accorder des moyens à des autorités compétentes en matière de sécurité des réseaux et de l'information**.

Cela se concrétiserait par :

- la mise sur pied d'**équipes d'intervention en cas d'urgence informatique** ;

- l'élaboration de stratégies et de **plans de coopération nationaux** ;

- l'amélioration des **échanges d'informations** et des **capacités de détection** ;

- la création d'une **culture de gestion des risques** ;

- l'**obligation pour les administrations et les secteurs critiques de procéder à une évaluation des risques et d'adopter des mesures appropriées et proportionnées pour garantir la sécurité de leurs réseaux et de leurs systèmes informatiques** ;

- **la signalisation aux autorités compétentes de tout incident de nature à compromettre sérieusement les réseaux et les systèmes informatiques et à avoir un impact significatif sur la continuité des services critiques et la fourniture de biens**.

Mais d'après Mme Fleur Pellerin, alors ministre déléguée chargée de l'économie numérique, en octobre 2013, « ***la vision de la Commission européenne***, *assez peu stratégique, n'embrasse pas les enjeux de l'économie numérique. Elle* ***omet en particulier les mesures qui dessineraient un environnement favorable à l'émergence de champions européens*** ».

Elle estimait que « ***les entreprises européennes sont mal protégées. L'enjeu est d'intelligence économique et de souveraineté mais aussi industriel*** : la France compte de belles entreprises spécialisées en cybersécurité, qui trouveraient là un marché et des débouchés ».

Cette position était également exprimée dans la contribution française sur l'Europe numérique élaborée en vue du Conseil européen des 24 et 25 octobre 2013 qui résumait ainsi la situation :

« *Aujourd'hui,* ***ce sont essentiellement des acteurs non européens de l'Internet qui détiennent les positions centrales dans le monde numérique****. Incontournables, ils captent l'essentiel de la valeur et détiennent la capacité d'influer sur le fonctionnement même d'Internet.*

L'Europe ne doit pas devenir un simple espace de coordination de services numériques développés ailleurs, **via** ***des technologies, des matériels et des normes qu'elle ne maîtriserait pas*** *; elle doit veiller au renforcement de son autonomie stratégique dans ce domaine. Elle doit garantir qu'Internet fonctionne comme un espace public ouvert à tous et respectueux des droits de chacun, un levier de développement économique, un instrument de liberté et d'émancipation politique* ».

En conséquence, à l'occasion du Conseil européen des 24 et 25 octobre 2013, consacré en partie à l'économie numérique – et ce, pour la première fois – **la France a élaboré une contribution écrite autour de trois priorités principales**.

D'abord, développer une stratégie industrielle européenne du numérique permettant l'**émergence d'acteurs européens innovants**, créateurs de croissance et d'emplois notamment en privilégiant le développement de technologies avancées (informatique en nuage, objets

connectés, traitement de masses de données), en facilitant le développement de services (villes et réseaux de transport et d'énergie intelligents, plates-formes ouvertes d'éducation), en soutenant le développement d'infrastructures de réseaux (haut et très haut débit, 4G) et en développant le numérique dans le secteur éducatif et dans la formation continue.

Ensuite, garantir un **accès ouvert** aux services et utilisateurs de l'Internet et permettre l'**émergence d'acteurs européens de niveau mondial**.

Enfin, **renforcer les règles visant à assurer la protection de la vie privée des citoyens européens** grâce notamment à l'encadrement des transferts de données en direction des États tiers, à la mise en place d'un guichet unique de défense des droits des individus et des entreprises face au numérique, à la coopération entre autorités de contrôle nationales sur les décisions relatives au traitement des données personnelles.

Ces règles devraient déboucher sur une proposition législative européenne concernant l'identification, l'authentification et la signature électronique, à l'étude depuis 2012, afin de **garantir des niveaux de sécurité harmonisés et la possibilité, parmi les États membres, d'adopter des règles mieux-disantes en ce qui concerne la sécurité des systèmes d'information**.

Il s'agit, en fin de compte, d'aspects de souveraineté qui méritent une plus ample analyse.

V. SOUVERAINETÉ ET NUMÉRIQUE

« ***La capacité de se protéger contre les attaques informatiques, de les détecter et d'en identifier les auteurs est devenue un des éléments de la souveraineté nationale.*** *Pour y parvenir, l'État doit soutenir des compétences scientifiques et technologiques performantes.* »

Livre blanc sur la Défense et la sécurité nationale, 2013

A. UNE COLONISATION NUMÉRIQUE ?

Après avoir élaboré plusieurs rapports sur le numérique pour la commission de la culture, de l'éducation et de la communication du Sénat, Mme Catherine Morin-Desailly, sénateur, a été chargée d'un rapport d'information intitulé « *L'Union européenne, colonie du monde numérique* » (rapport n° 443, 2012-2013) publié en mars 2013, dans lequel elle a choisi de « *sonner le tocsin avant qu'il ne soit trop tard* ». Elle y affirme que « ***l'Europe est sous-développée dans le monde numérique*** » et qu'« ***elle est menacée de sous-développement global demain****, puisque le numérique prend progressivement le contrôle de toute l'activité* ».

Ce rapport identifie bien les menaces pesant sur la maîtrise des données par l'Union européenne, son « *or noir du futur numérique* », mettant en cause son indépendance et sa liberté.

Pour y remédier, ce rapport propose **d'assurer à l'Union européenne la maîtrise effective des données des citoyens européens** notamment face à l'informatique en nuage, aux objets communicants et aux emprises multiples des États-Unis d'Amérique qui, au nom de la lutte contre le terrorisme, ne cessent d'étendre à grande échelle leur collecte de données sur les citoyens non-américains situés hors du territoire nord-américain.

Dans ce domaine, **les citoyens non-américains se voient reconnaître moins de droits que les citoyens américains tandis que l'Union européenne applique, elle, à tout individu, des textes de portée universelle** comme la Convention européenne des droits de l'homme et la Charte des droits fondamentaux de l'Union européenne (droit à la vie privée, au respect de la correspondance, à la protection des données personnelles).

Il serait évidemment souhaitable que l'Union européenne mette en avant le respect de ces droits dans le développement de l'informatique en nuage mais les diverses hésitations manifestées à l'occasion de la préparation de la proposition de règlement européen laissent craindre une forte influence nord-américaine dès ce stade.

Comment alors garantir la protection de la vie privée, des données personnelles par des fournisseurs de services du nuage numérique relevant, ou pouvant relever d'un jour à l'autre, du droit nord-américain au gré des variations d'identité des propriétaires de leur capital ?

Cette dérive une fois survenue, **quelle protection opposer au développement de l'Internet des objets** dont les règles devraient être conçues dès aujourd'hui ?

D'autant que nombre de ces objets connectés concerneront la quantification de soi, domaine d'élection de la vie privée.

À l'abandon de leur souveraineté numérique par les États risque de répondre l'abandon par les États de la protection des droits de leurs citoyens menacés par le numérique contrôlé depuis l'étranger.

C'est dans ce contexte mouvant et fragile qu'**il importe de sécuriser les réseaux numériques objets d'attaques**.

Devant l'ampleur possible des dégâts provoqués par de telles attaques, **les États se doivent de concevoir la protection des infrastructures critiques de la société, celle des opérateurs d'importance vitale (OIV) comme des citoyens reliés à eux de manière critique**.

Les notions de vulnérabilité et de résilience, face et à la suite d'attaques numériques, prendront alors tout leur relief.

C'est pourquoi la France s'est dotée, en 2009, de l'Agence nationale de la sécurité et des systèmes d'information (ANSSI) pour prévenir les attaques informatiques et aider les opérateurs d'importance vitale à réagir en cas de crise.

Comme il peut être indispensable d'étendre cette prévention et cette assistance aux sous-traitants, aux clients et aux personnels de ces opérateurs, il apparaît aussitôt que **c'est davantage l'échelon national que l'échelon européen qui peut tisser ce maillage préventif et curatif**.

Cela passe par le recours à des **matériels fiables** (fabriqués en France, dans l'Union européenne ou labellisés par l'ANSSI), à des **contrôles** systématiques, à des **règles juridiques** plaçant très haut les impératifs de la sécurité numérique et à des **comportements responsables** face aux risques du numérique.

À l'échelon communautaire, cela suppose de reconnaître la nécessité de la mise en place d'une **préférence communautaire pour les marchés de sécurité d'équipements numériques hautement stratégiques**.

Cette notion devant primer sur la liberté de la concurrence dans les secteurs d'importance vitale.

B. LES LEÇONS TIRÉES PAR LES ÉTATS-UNIS D'AMÉRIQUE DES EXCÈS DE LA NSA

À la suite des divulgations effectuées par M. Edward Snowden, une commission d'enquête en charge de la réforme du système de surveillance de la *NSA* (*National Security Agency*) a élaboré **quarante-six propositions** à partir de l'idée que « ***Les nations libres doivent se protéger et les nations qui se protègent doivent demeurer libres*** » afin de garder un équilibre entre les nécessités de la sécurité nationale, les intérêts économiques et le maintien de la vie privée garantie par la Constitution américaine.

Dans ce cadre, **la *NSA* cesserait de stocker systématiquement l'ensemble des métadonnées téléphoniques** (dates et heures des appels, origines, destinataires, etc.) ; elle ne pourrait les obtenir des opérateurs de télécommunications qu'au cas par cas et sur décision d'un juge.

De plus, **ces experts ont également proposé que les fabricants américains de matériels et de programmes informatiques n'y intègrent plus systématiquement des portes dérobées**.

Les experts ont également recommandé d'**accorder la même protection aux non-Américains qu'aux citoyens nord-américains**. En application du *Privacy Art* de 1974, les Américains ont droit à l'accès aux données personnelles les concernant collectées par les administrations ou divulguées publiquement.

Enfin, **la surveillance des personnalités politiques devrait être contrôlée par le Parlement et non par les dirigeants du renseignement**.

Quel sera le sort de ces propositions ? Ne sont-elles, comme les modifications de la gouvernance de l'*ICANN*, qu'un nouveau faux-nez destiné à masquer le visage de l'escamoteur ?

CHAPITRE II – LE CADRE NATIONAL DE LA MISE EN ŒUVRE DE LA SÉCURITÉ NUMÉRIQUE

En complément des normes techniques, les normes juridiques continuent de jouer un rôle majeur en imposant des cadres évolutifs dans le respect des libertés.

I. NUMÉRIQUE ET LIBERTÉS

Face aux conséquences du numérique pour les libertés, à ses imperfections, la nécessité de légiférer est souvent évoquée. Mais l'amélioration de toutes les composantes de la sécurité informatique passe-t-elle par l'adoption de nouvelles règles juridiques ?

En matière de protection des droits fondamentaux, la section du rapport et des études du Conseil d'État a jugé nécessaire et urgent de répondre, en 2014, de manière très approfondie, à cette interrogation.

De leur côté, la CNIL et l'ANSSI conjuguent leurs efforts, complémentaires plutôt que concurrents, pour assurer la protection des entreprises comme celle des personnes.

A. LE RAPPORT DU CONSEIL D'ÉTAT SUR LE NUMÉRIQUE ET LES DROITS FONDAMENTAUX

Pour le Vice-président du Conseil d'État, M. Jean-Marc Sauvé, « *Les technologies de l'Internet et les espaces numériques qu'elles ont engendrés n'invitent pas seulement les juristes à l'exploration et à la conquête d'une nouvelle* terra incognita *; ils transforment de l'intérieur, voire dérèglent, les conditions d'exercice des droits fondamentaux et les mécanismes traditionnels de leur conciliation* ».

Le droit à l'oubli, le déréférencement, très souvent cités comme des avancées notables, ne sont pas de véritables garanties de sécurité.

L'étude annuelle du Conseil d'État de 2014 a porté sur « *Le numérique et les droits fondamentaux* » et a constaté que **le numérique représente à la fois un atout et une menace pour les droits fondamentaux**.

Les rapporteurs, M. Jacky Richard, rapporteur général de la section du rapport et des études, et M. Laurent Cytermann, rapporteur général adjoint, ont noté que le numérique permettait à la fois le **développement de certaines libertés** (d'expression, d'association ou d'entreprendre, par exemple) **tout en menaçant la vie privée et la sûreté en général**, compte tenu du développement rapide de la cybercriminalité.

Ils ont relevé plusieurs **spécificités du numérique qui rendent difficile son encadrement par la règle de droit**.

C'est ainsi que **la gouvernance de l'Internet n'est pas régie par un texte international** mais par des rapports de négociations qui ne résultent même pas de la confrontation d'États mais d'équilibres de pouvoirs au sein d'une fondation de droit privé américain , l'*ICANN*, où les États sont peu représentés – même si un rééquilibrage de cette gouvernance a été envisagé depuis la réunion de São Paulo d'avril 2014.

La règle de droit, qui se caractérise d'abord par la territorialité de la norme, semble ne pas avoir prise sur le numérique qui se trouve, de fait, **régi par le droit nord-américain**.

Il est à noter également que, si **la circulation des données est de la compétence européenne**, **la sécurité nationale est régie par la loi des États membres**. Toutefois, les rapporteurs ont souligné que, dans ce domaine, **le droit dur devrait être largement associé au droit souple** pour permettre l'organisation de transitions conduisant à de bonnes pratiques.

Ils ont rappelé aussi le rôle fondamental de la CNIL qui a su faire prospérer les principes fondamentaux issus de la loi de 1978 devenus aujourd'hui **communs aux États européens**.

Parmi ces principes figure l'encadrement de la collecte des données qui doit avoir une **finalité déterminée** et lui **être proportionnée** ou encore l'idée qu'**une autorité indépendante doit surveiller la mise en œuvre de la législation**.

Les rapporteurs ont toutefois relevé que la question du stockage et du traitement des données massives était difficilement conciliable avec ces principes de finalité déterminée et de proportionnalité d'où l'intérêt de **reconnaître une grande liberté de réutilisation des données à des fins statistiques mais sans transiger sur le respect des données des personnes privées**.

Parmi les cinquante recommandations de ce rapport, vos rapporteurs ont retenu particulièrement celles relatives à la réduction du risque numérique dont celles consistant à :

- **promouvoir la démocratisation de l'*ICANN*** en créant une assemblée générale rassemblant l'ensemble des parties prenantes et pouvant mettre en cause la responsabilité du conseil d'administration ; renforçant les mécanismes de recours internes, par exemple, en dotant d'une portée contraignante le mécanisme d'*Independant Review Panel* permettant au comité représentant les gouvernements (*GAC*) d'adopter des résolutions contraignantes ;

- **diversifier la composition des instances de gouvernance de l'Internet**, par des critères de sélection imposant une réelle diversité linguistique et géographique et la mise en place de stratégies d'influence au

niveau de la France et de l'Union européenne incluant notamment l'obligation de traduction simultanée lors des travaux de ces instances.

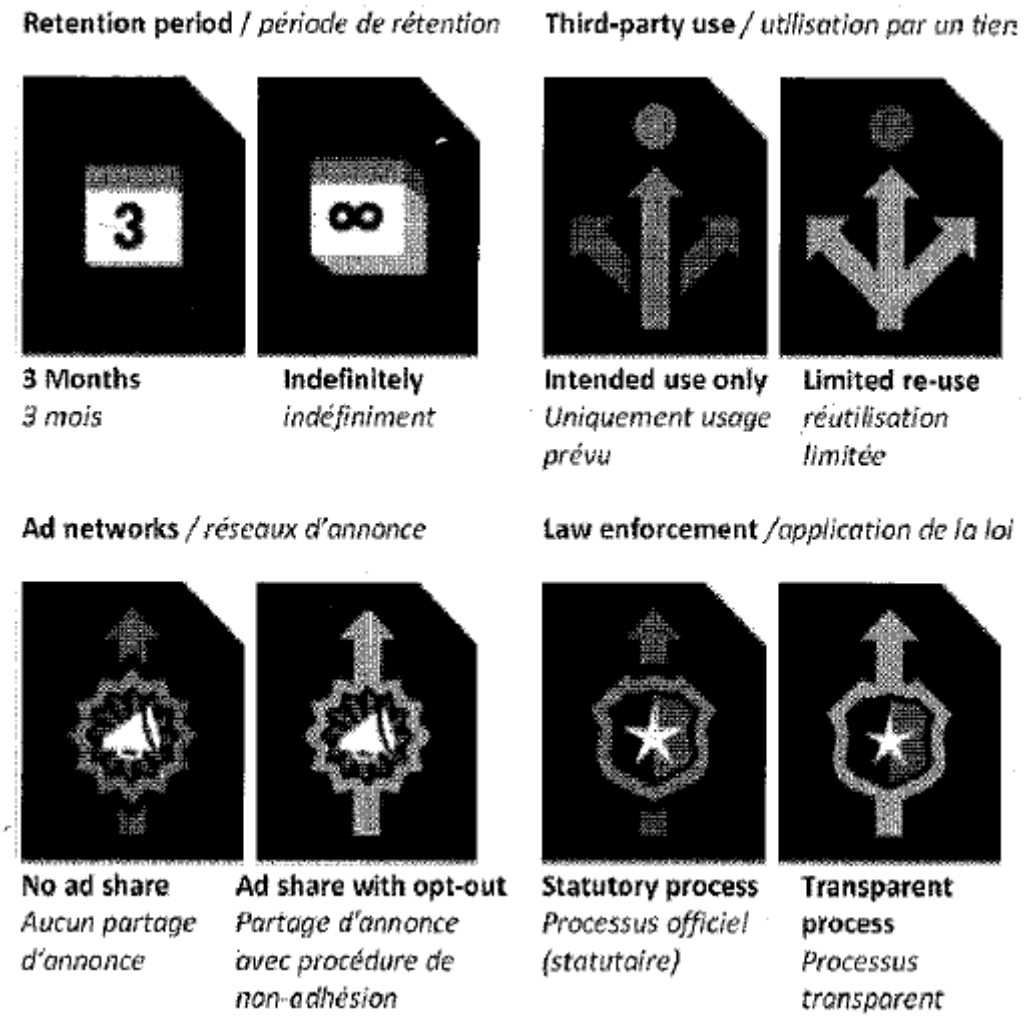
En effet, **une partie du risque numérique provient du contrôle de l'Internet par un État étranger**.

Dans ce rapport du Conseil d'État est également préconisée une profonde transformation des instruments de protection des données avec, par exemple, l'utilisation de technologies permettant de **rendre les données moins accessibles aux tiers** et de **renforcer la capacité des personnes à contrôler l'utilisation de leur données**. À ces fins, l'ensemble des technologies de **cryptologie** ou encore l'usage du **réseau *TOR***, qui permet de rendre anonymes des échanges sur l'Internet, pourraient être optimisés.

Il existe déjà la possibilité de bloquer l'enregistrement de fichiers ou *cookies* sur un terminal, d'exprimer ses préférences en matière de traçage de ses données, ou encore de permettre à un individu de recourir à une plate-forme d'accès à toutes les données personnelles détenues par un ensemble de partenaires. Cela est peu connu.

Ce rapport estime qu'il serait souhaitable de mettre en place un affichage généralisé des politiques d'utilisation des données personnelles suivies par chaque site en faisant figurer sur l'écran de l'ordinateur, dans un format simple et lisible, **une signalétique appropriée** dont, par exemple celle préconisée par la Fondation *Mozilla* **indiquant la durée de la période de rétention des données, la possibilité de leur utilisation par un tiers, leur partage d'annonce, la transparence du processus** au moyen des icônes ci-après.

Schéma n° 4 : Signalétique d'information sur l'utilisation des données personnelles développée par la fondation *Mozilla*



***Source** : Mozikko Wiki, Privacy Icons project (beta release), Owner : Ben Moskowitz, Mozilla ; Aza Raskin (initiator), Designs by Michael Nieling & Ocupop, designers of the official HTMLS logos, Updated : June 15, 2011, https://wiki.mozilla.org/Privacy_Icons*

Vos rapporteurs sont très favorables au développement de ce type d'icônes pour renseigner utilement et immédiatement les utilisateurs sur la confiance à accorder aux outils et applications qui leur sont proposés.

En conclusion de son étude, le Conseil d'État a estimé que les quatre grandes hypothèses de travail formulées au commencement de ses travaux avaient été validées.

Mais il y a une nuance entre son affirmation de 1998 selon laquelle il n'y aurait eu nul besoin d'un droit spécifique de l'Internet et des réseaux et ce qui a été observé depuis, à savoir le **décalage entre le rythme des innovations dont le numérique est porteur et le temps d'adaptation du**

régime juridique des droits fondamentaux s'est manifesté à de nombreuses reprises.

C'est pourquoi le Conseil d'État recommande aujourd'hui de s'engager dans la reconnaissance du droit et de devoirs pour les individus de protéger leurs données personnelles, ce qu'il désigne par l'expression « ***autodétermination informationnelle*** ».

Il reconnaît aussi la nécessité :

- de la définition d'une catégorie juridique de **plates-formes respectant le principe de loyauté** à l'égard de leurs utilisateurs ;

- d'un **droit au déréférencement** sur les moteurs de recherche assorti d'une décision unique de déréférencement ;

- de la définition d'un **droit des algorithmes prédictifs** ;

- de la **réforme du régime de la concentration en matière de presse d'information** ;

- de la **conciliation entre la protection de la vie privée et la conservation des métadonnées** à des fins de prévention des atteintes à la sécurité nationale.

Autant d'aspects qui, selon le Conseil d'État, nécessiteraient une législation adaptée.

Il est important de noter – et cela rejoint nombre d'observations de vos rapporteurs – que, selon le rapport cité, **le numérique « *n'est pas un outil docile aux mains de son maître* » puisqu'« *il porte en lui-même des conséquences qui échappent à la volonté de ses utilisateurs* »**. Il ne s'agirait donc pas du tout d'un outil ni bon ni mauvais en lui-même, comme cela a été plusieurs fois affirmé au cours des auditions menées par vos rapporteurs, mais d'**un outil à la fois bon et mauvais**.

Il est intéressant de relever aussi que **le Conseil d'État attache une grande importance au développement d'un droit souple**, par opposition à un droit dur, pour fournir des solutions juridiques praticables fondées sur le recours aux **recommandations**, aux **guides de bonnes pratiques**, à l'homologation des **codes de conduite professionnelle**, à la **certification** ou à la **médiation**, soit un droit ajustable et réversible en fonction de l'usage.

Il rejoint en cela les positions défendues par le Professeur honoraire au Collège de France, Mme Mireille Delmas-Marty lors des auditions.

« Derrière la *soft law*, nous avons à la fois un **droit flou**, ou imprécis, fait de principes généraux qui ne sont pas définis de façon rigoureuse et un **droit mou**, facultatif, non obligatoire (le droit des recommandations), enfin le **droit doux,** qui n'est pas sanctionné. Le flou, le mou et le doux peuvent aller de pair ou séparément.

[...] Le droit flou [...] **Un droit qui n'uniformise pas, mais qui permet de pluraliser la régulation**, me paraît une perspective très intéressante [...] Il est utile aussi, et on l'a déjà dit, de faire appel au **droit mou, non obligatoire, comme manière d'amorcer un processus de régulation.** Il est plus facile de commencer par des recommandations que directement par un texte de loi. Le droit mou est peut-être un moyen d'**éviter que le cadre juridique soit en retard par rapport aux innovations technologiques.** »

Mme Mireille Delmas-Marty
Membre de l'Institut de France (Académie des Sciences morales et politiques)
Professeur honoraire au Collège de France (études juridiques comparatives et internationalisation du droit)
19 juin 2014
Auditions. Tome II du présent rapport

Le rapport du Conseil d'État a également retenu comme hypothèse que « ***les internautes européens doivent se voir appliquer en priorité des règles européennes*** **»** et noté que **l'Union européenne constitue, en opportunité, le niveau pertinent d'action**.

Le rapport note que la proposition de règlement européen en cours de préparation prévoit, avec le G29 et avec la Commission européenne, un ensemble de mesures incluant le **droit au référencement linéaire**.

Toutefois, compte tenu des délais excessivement longs de mise au point d'une directive ou d'un règlement, **le Conseil d'État estime que plusieurs propositions pourraient être portées en priorité par les autorités nationales même si des textes européens sont en préparation** – et alors que les négociations du traité transatlantique de libre-échange (*TTIP*) sont bien engagées, ajoutent vos rapporteurs. En effet, la protection des données personnelles, les garanties offertes aux organes de presse, la réglementation de la responsabilité des plates-formes numériques ont besoin d'un encadrement rapide ; de même, pour la question de la conservation des métadonnées de communication à des fins de prévention ou de répression qui touche aux intérêts nationaux fondamentaux.

Enfin, le rapport du Conseil d'État relève que si l'Europe a été distancée quant à la génération actuelle de plates-formes, **il est souhaitable que s'y développent des entreprises liées au numérique**.

Mais l'enjeu n'est pas seulement économique car le numérique doit prendre plus largement en compte « *les enjeux de la connaissance, de l'éducation de la culture* » pour faire contrepoids aux pratiques de l'Internet.

Le rapport du Conseil d'État recommande fortement **que l'Union européenne affirme ses valeurs sans imposer des règles désavantageant ses propres citoyens, ses propres entreprises et donc en affirmant la territorialité de la norme**.

B. LIBERTÉ DE L'USAGE DU NUMÉRIQUE ET LIBERTÉS DE SES USAGERS

> « *Un peuple prêt à sacrifier un peu de sa liberté pour un peu de sécurité ne mérite ni l'une ni l'autre, et finit par perdre les deux.* »
>
> *Benjamin Franklin*

À la liberté des débuts de l'Internet, de la multiplication des outils de communication, de la créativité des logiciels ont répondu, après septembre 2001, une surveillance accrue des libertés à travers ses expressions numériques : le *Patriot Act*, le *Foreign Intelligence Surveillance Act (FISA)* et l'activisme de la *NSA* en sont autant d'illustrations.

Dès lors, la fragmentation de l'Internet en des Internets s'est accélérée et un étrange jeu de cache-cache dans les réseaux s'est mis en place.

Il a été rappelé aux plus inattentifs que le *net* signifiait la toile et qu'était de moins en moins anonyme l'araignée à l'affût des informations individuelles, commerciales ou culturelles qui s'y prenaient.

Araignée boulimique, ascendant fourmi, qui réclame de plus en plus de données et stocke même celles qu'elle ne sait pas encore déchiffrer pour les analyser un jour avec des algorithmes encore plus performants.

> « Ouvrir un compte sur *gmail*, c'est accepter de voir ses informations livrées à l'administration américaine si elle en fait la demande ».
>
> ***Me Christiane Féral-Schuhl,***
> ***Avocat, ancien bâtonnier du barreau de Paris***
> *Rapport d'information :*
> *« Numérique, renseignement et vie privée : de nouveaux défis pour le droit*
> *Journée d'étude du 22 mai 2014*
> *Sénat, n° 663, 2013-2014*

En France, dès 1978, la Commission nationale de l'informatique et des libertés (CNIL) a été érigée en gendarme vigilant des libertés face aux fichiers. Mais l'accélération des évolutions technologiques a fait naître des menaces excédant le seul contrôle des fichiers. La CNIL a évolué et a été complétée par l'ANSSI.

Les auditions ont montré la coopération et la complémentarité entre la commission et l'agence nationales.

> « Les actions de la CNIL et de l'ANSSI sont complémentaires. En général, en matière de sécurité des systèmes d'information, **on s'intéresse aux risques pour l'entreprise, alors qu'en matière**

de protection des données, on s'intéresse aux risques pour les personnes. Les mesures techniques à mettre en place dans chacun de ces cas sont souvent similaires. Par exemple, le chiffrement des données garantit la confidentialité des échanges, ce qui protégera la personne mais aussi l'entreprise. »

M. Gwendal Le Grand
Directeur des technologies et de l'innovation, CNIL
12 février 2014
Auditions. Tome II du présent rapport

La CNIL ne protègerait pas seulement les personnes tandis que l'ANSSI ne protègerait par uniquement les entreprises.

En réalité, existent des préconisations de la CNIL aux entreprises – comme celles sur le **stockage de données dans les nuages informatiques**, le **guide à destination des PME** publié par la CNIL en 2010 ou encore, en 2012, le **guide avancé de gestion des risques** élaboré grâce à une méthode mise au point par l'ANSSI ou, enfin, les **pactes de conformité** permettant aux entreprises d'intégrer la préoccupation de protection de la vie privée dès la conception des produits.

« Concrètement, nous devons apporter une réponse de « sécurité en réseau ». En effet**, aucun acteur n'a l'ensemble des clés pour piloter à lui seul la sécurité de cet univers.** En revanche, si l'on s'adresse à l'ensemble des acteurs concernés, et que chacun d'entre eux a une action, une responsabilité particulière en termes de sécurité, alors nous pouvons collectivement garder cet univers sous contrôle, en tout cas au niveau de la sécurité de celui-ci.

Qu'est-ce que signifie avoir une « sécurité en réseau » ? Le premier axe, ce sont les entreprises. Vous l'avez dit, madame Le Dain, c'est le cœur de votre préoccupation d'aujourd'hui. L'objectif est de **responsabiliser ces acteurs** professionnels et ces entreprises, afin qu'ils intègrent dans leur propre fonctionnement cet objectif de garantie de la sécurité des réseaux, et pour nous, à la CNIL, de la sécurité des données personnelles. »

Mme Isabelle Falque-Pierrotin
Présidente, Commission nationale de l'informatique et des libertés (CNIL)
19 juin 2014
Auditions. Tome II du présent rapport

La CNIL comme l'ANSSI doivent s'adapter sans cesse. Cela a été illustré récemment par la CNIL face à *Google* mais le niveau des amendes qu'elle peut infliger devrait se situer dans une gamme propre à dissuader réellement les auteurs d'atteintes aux libertés individuelles par le numérique.

« L'action menée récemment par la CNIL vis-à-vis de *Google*, en partenariat avec ses homologues au niveau européen, a conduit à conclure que **la politique de confidentialité de *Google* n'était pas conforme aux règles européennes** ; l'information donnée aux personnes lors de l'utilisation de ces services, était insuffisante, les utilisateurs ne disposant pas d'un contrôle suffisant sur les combinaisons des données ; enfin, *Google* ne précisait pas la durée de conservation comme demandé, dans la loi informatique et libertés.

C'est la raison pour laquelle, au début de l'année 2014, la formation restreinte de la CNIL a prononcé une sanction financière contre *Google* qui a interjeté appel de cette sanction. Non pas pour son côté financier mais pour l'obligation de publier cette sanction sur le site de *Google* : www.google.fr. Un référé suspension contre cette obligation a été rejeté par le Conseil d'État la semaine dernière et, cette semaine, samedi et dimanche derniers, sur le moteur de recherche un avis indiquait que *Google* avait été condamné à publier le fait qu'il avait été sanctionné pendant quarante-huit heures. »

M. Gwendal Le Grand
Directeur des technologies et de l'innovation, CNIL
12 février 2014
Auditions. Tome II du présent rapport

Pour sa part, l'**ANSSI s'attache à la fiabilité des matériels et accorde des labellisations à ceux-ci**.

Face à la rapidité et aux aspects techniques sans cesse renouvelés des attaques numériques, il est souvent proposé d'accroître de manière significative les effectifs de l'ANSSI toujours davantage sollicitée.

La loi de programmation militaire de 2013 a encore chargé l'ANSSI de nouvelles missions. Cependant, **en dépit de la prévention que l'ANSSI développe et de ses indispensables interventions, cette agence ne saurait voir sa mission s'étendre de tous les opérateurs d'importance vitale et des points d'importance vitale à tous les sous-traitants, fournisseurs et clients de ces opérateurs. Pas davantage à l'ensemble des entreprises situées sur le territoire national qui sont, pourtant, toutes menacées par l'insécurité numérique.**

Comme l'ont souligné plusieurs personnes entendues, **la protection, la défense numérique des entreprises doivent se construire dans la profondeur, avec des couches successives de sécurité**.

« Comme les antivirus ne couvrent pas tous les risques du numérique, la protection assurée par les antivirus doit être complétée par l'importante défense en profondeur. Il s'agit de **l'empilement de briques de sécurité** qui permet d'accorder un certain niveau de sécurité aux outils et aux usages que l'on en fait. L'outil informatique comprend des mises à jours de sécurité des briques matérielles et logicielles car **les composants ne sont pas développés de façon suffisamment sécurisée et comportent des failles de sécurité**. Tout un écosystème vit de la détection, de la production et de la vente de ces failles de sécurité. »

M. Philippe Le Bouil
Direction de la protection et de la sécurité de la défense (DPSD)
6 mars 2014
Auditions. Tome II du présent rapport

II. LA MISE EN ŒUVRE OPÉRATIONNELLE DE LA SÉCURITÉ NUMÉRIQUE

A. LA DIRECTION GÉNÉRALE DE L'ARMEMENT (DGA)

Au sein de la Direction générale de l'armement (DGA), qui est le premier acteur de la recherche de défense en Europe, l'établissement DGA Maîtrise de l'information est l'expert technique du ministère de la défense pour les systèmes d'information et de communication, la cybersécurité, la guerre électronique et les systèmes de missiles tactiques et stratégiques.

Cette expertise technique va **du composant électronique jusqu'aux systèmes de systèmes**, **de la conception des composants ou d'algorithmes cryptographiques jusqu'aux évaluations d'architectures sécurisées de systèmes complets**.

Dans ce cadre, **la DGA développe et évalue des produits de cybersécurité**.

Elle coopère tant avec le Centre d'analyse en lutte informatique défensive (CALID), qu'avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI) pour analyser les attaques numériques les plus complexes détectées sur les réseaux et les menaces potentielles les plus dangereuses.

La perception aiguë des exigences de la cyberdéfense a conduit la DGA à prévoir le **recrutement accru d'experts**, à savoir des ingénieurs de très haut niveau, spécialisés dans l'analyse et la prévention des attaques informatiques (effectif accru de 160 % de 2012 à 2017) et un **appui substantiel aux études amont** (financement en progression de 200 % de 2012 à 2017) menées par les laboratoires de recherche sur les petites et moyennes entreprises.

La DGA Maîtrise de l'information travaille, par exemple, à des **systèmes de chiffrement pour réseaux *IP*** aptes à traiter des informations classifiées « confidentiel défense » ou « secret défense ».

De plus, la DGA constitue, depuis sa création, **un pont entre les armées et les industriels** y compris au-delà de la défense nationale.

Le centre de Bruz compte près de **huit cents ingénieurs et techniciens dont 25 % en charge de la sécurité des systèmes d'information** ; il recrute une quarantaine de personnes chaque année.

Il développe les **algorithmes de chiffrement gouvernementaux**, effectue de plus en plus de la simulation numérique et contrôle les matériels à l'exportation quant au respect des autorisations délivrées.

La croissance prévisible de la cyberdéfense jusqu'en 2017 va conduire à recruter de plus en plus d'ingénieurs qui constitueront près de 70 % des personnels.

La convergence croissante entre les technologies civiles et militaires dans le domaine du numérique conduit à l'emploi de composants identiques dans le monde entier mais sur des systèmes très différents, voire des systèmes de systèmes – comme sur un navire de combat – d'où un risque de pénétration infiltrant tout.

Dans ce contexte, les barrières entre les systèmes ne suffisent plus et l'interconnexion peut, en elle-même, introduire des risques, d'où la **nécessité de disposer de capteurs d'attaques dans les systèmes d'armes, dans les systèmes d'information et de communication et dans les systèmes industriels (SCADA)**.

La cybersécurité résulte de l'addition de la cyberprotection avec la cyberdéfense – qui revient à poster l'équivalent de sentinelles dans un système d'information.

La DGA intervient à trois niveaux :

- **la conception** d'éléments qui suppose la maîtrise de la partie critique et donc le contrôle des composants ;

- **l'évaluation** des composants, des équipements et des systèmes dans la durée ;

- **l'anticipation** de la menace qui conduit à se mettre dans la peau de l'attaquant pour tester les systèmes.

La DGA et l'ANSSI travaillent en commun, notamment pour certaines études cofinancées.

Compte tenu des nombreuses failles de sécurité numérique possibles, investir dans la cybersécurité ne saurait être un surcoût même si cela peut sembler être le cas dans l'immédiat.

B. LE LABORATOIRE DE HAUTE SÉCURITÉ DU LABORATOIRE LORRAIN DE RECHERCHE EN INFORMATIQUE ET SES APPLICATIONS (LORIA)

Le laboratoire de haute sécurité du LORIA (CNRS, INRIA, Université de Lorraine) constitue une **plate-forme académique unique en France pour la recherche en sécurité numérique** depuis 2010. Son activité porte à la fois sur l'expertise en sécurité, la défense proactive contre les programmes malveillants et la formation afin de pouvoir **garantir la confidentialité des données ou de leur traitement local pour des recherches sensibles**.

Ce laboratoire fait partie du maillage européen des laboratoires de haute sécurité mais n'a pas d'équivalent réel en Europe.

Le laboratoire analyse à large échelle le trafic sur le réseau pour y repérer des menaces, les canaux de communication entre les machines zombies et ceux qui les contrôlent, les tentatives d'hameçonnage (*phishing*) à travers de faux sites de confiance.

Le défi à relever consiste à sécuriser l'Internet en temps réel à travers l'élaboration d'une structure de supervision en coopération avec les forces de l'ordre, par exemple dans la lutte contre la pédophilie (40 % des fichiers de recherche d'un dessin animé sont pollués). Un pare-feu a été mis au point par l'INRIA qui travaille également sur la recherche anticipée des réseaux pédophiles de demain.

Concernant les entreprises, le laboratoire étudie les moyens de **détecter les intrusions sur les systèmes *SCADA*** dont certains peuvent être accessibles par Internet, ce qui permet à l'attaquant de prendre le contrôle de vannes, de portes – y compris de prisons lorsque des gardiens sont allés jouer sur l'Internet…

D'où la **nécessité de protéger le réseau contrôle-commande au moyen d'une détection d'intrusion toute l'année, de jour comme de nuit**. Le laboratoire a conçu une plate-forme de test à cette fin.

Le laboratoire étudie aussi la sécurité des environnements, par exemple à travers des configurations vulnérables d'équipements comme *Android*, très largement utilisé notamment dans les téléphones portables, ce qui facilite les comportements malveillants d'attaquants se livrant à la même quête de vulnérabilité.

Le laboratoire mène également une importante activité de recherche en cryptographie – notamment celle dite à clé publique – dont le niveau de sécurité doit être sans cesse relevé.

Cette activité s'étend également à la sécurité des protocoles – ou description de comportement à adopter – par exemple les protocoles cryptographiques de sécurisation des communications sur les réseaux ouverts (cartes bleues, téléphones, vote électronique, etc.)

L'INRIA s'attache à identifier le ou les procédés d'authentification adaptés à chaque usage et étudie les fragilités de chacun. C'est ainsi que les recours aux empreintes digitales ou à l'iris apparaissent peu sûrs car impossibles à changer une fois volés – ce qui n'est pas très difficile ; de plus, des doigts souples ont pu être fabriqués…

À noter qu'une fois l'authentification subtilisée, l'accès à toutes les applications est possible.

Quant au vote électronique – interdit pour les élections politiques en Allemagne, en Grande-Bretagne et en Irlande –, **il est difficile de garantir la fiabilité des machines à voter comme le secret du vote** – ce qui ouvre la voie à l'achat de celui-ci ; en outre, la **vérification par les citoyens est impossible**.

Vos rapporteurs ont retiré de la visite du centre breton de l'établissement DGA Maîtrise de l'information et du laboratoire de Haute sécurité de l'INRIA à Nancy que **l'analyse de l'expérience de cybersécurité militaire devait permettre de gagner des années dans la cybersécurité civile** et, inversement, que **les recherches de l'INRIA pourraient irriguer le secteur de la défense** – les deux étant indissociables – et qu'**une coopération accrue des acteurs militaires et civils était indispensable** pour la protection des opérateurs d'importance vitale et des infrastructures dont ils ont la charge.

Cependant, aucun effort en ce sens n'est possible sans une perception des vulnérabilités numériques à leur juste degré.

C. L'AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (ANSSI)

Créée en 2009, à la suite de la parution, en 2008, du Libre blanc sur la défense et la sécurité nationale, l'ANSSI a pour mission de :

- **conseiller** les administrations et **les opérateurs d'importance vitale** ;

- **informer les entreprises** et le grand public sur les menaces informatiques et les moyens de s'en protéger – notamment au moyen de la publication de **bulletins d'actualité** dont un exemple récent figure en annexe ;

mais également de :

- prévenir concrètement la menace en développant une **offre de produits et de services de confiance** pour les administrations et les acteurs économiques ;

et, en urgence, de :

- **réagir au plus tôt face aux attaques informatiques** contre les réseaux les plus sensibles de l'administration, **détectées grâce à un centre opérationnel renforcé de cyberdéfense agissant vingt-quatre heures sur vingt-quatre**.

Au-delà de ces missions initiales, l'ANSSI se préoccupe également de **la sécurisation des objets connectés** dont le nombre pourrait approcher les cinquante milliards avant 2050.

L'ANSSI s'intéresse aussi à la place du numérique dans l'économie. À cet égard, elle relève que **chaque année, en France, l'insécurité informatique est à l'origine de la perte de dizaines de milliers d'emplois** car les attaques numériques pénalisent la compétitivité.

D'où l'importance de **développer des outils de détection d'attaques souverains** grâce au programme d'investissements d'avenir.

« L'article 21 de la loi de programmation militaire permet, en cas d'attaque d'un système d'information critique, de pénétrer le système d'information adverse pour caractériser l'attaque et en neutraliser les effets. **N'est légale que l'action défensive.**

Comme l'a rappelé le Livre blanc sur la défense et la sécurité nationale de 2013, **la France a annoncé se doter de capacité offensive en 2008**. »

M. Christian Daviot
Chargé de la stratégie auprès du directeur général, ANSSI
26 juin 2014
Auditions. Tome II du présent rapport

De plus, **l'article 22 de la loi de programmation militaire autorise le Premier ministre à imposer des règles techniques aux opérateurs d'importance vitale**.

Cela peut d'ailleurs aussi concerner également des entreprises relevant du potentiel scientifique et technologique dont les entreprises innovantes – donc au-delà d'une liste d'entreprises à protéger prioritairement.

Pour l'avenir, une capacité offensive est envisagée.

Quant au niveau de sécurité numérique maximal, il doit être assuré par le respect des préconisations de l'ANSSI comme les quarante recommandations d'hygiène informatique définies dans son guide – et rappelées dans les recommandations du présent rapport pour bien situer les propositions de vos rapporteurs au regard des préconisations de l'agence.

D. LA GENDARMERIE NATIONALE

La Gendarmerie nationale n'a pas été la dernière à observer les risques du cyberespace et à en relever les défis. Cette démarche s'inscrit dans le cadre de la doctrine nationale de cybersécurité.

Pour la Gendarmerie, il est évident depuis longtemps que **les technologies du numérique ont pour effet de fragiliser la société**, qu'il s'agisse des transports, aérien ou ferroviaire, de celui de l'énergie, ou encore des équipements médicaux. La connectivité à l'Internet ne fait qu'accentuer cette fragilité.

C'est pourquoi **la Gendarmerie tente d'accélérer la prise de conscience collective de tous les acteurs**, publics et privés, estimant que, pour faire face aux menaces et aux risques actuels, **chacun doit devenir acteur de sa propre sécurité numérique**, qu'il s'agisse du particulier, de l'entrepreneur ou encore d'une organisation privée ou publique.

La brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI), service de la sous-direction des affaires économiques et financières de la direction de la police judiciaire de la préfecture de police de Paris, compte dans ses missions **la sensibilisation, l'information et la formation à la cybercriminalité des acteurs publics ou privés dont le grand public**. Cela permet notamment d'**apporter une réponse réactive aux victimes** pour qu'elles acquièrent une cyberattitude, un comportement cybersécurisé.

La BEFTI tente de diffuser un **apprentissage des bons usages numériques** aux enfants, aux adolescents comme à leurs parents et grands-parents. Elle se tourne également vers les administrations, les entreprises et les associations en prodiguant des **conseils préventifs ou de réaction juridique à une attaque**. La BEFTI se concentre sur les piratages d'entreprises d'ailleurs de plus en plus nombreuses à déclarer aux autorités judiciaires leurs sinistres car elles savent que, de cette déclaration, dépendent un soutien rapide et une expertise de l'attaque intervenue. Cela est important compte tenu de la durée limitée de conservation des données de connexion et alors qu'il convient d'identifier l'attaquant, plus ou moins parvenu à se rendre anonyme, et de mesurer l'ampleur des informations qu'il a pu extraire de l'entreprise attaquée.

Vos rapporteurs ont entendu la Gendarmerie nationale à deux reprises.

« Enfin, demeure l'importante question de savoir, à propos des collectivités locales, des petites et moyennes entreprises et des particuliers, vers qui ils doivent se tourner en cas d'incident. Aujourd'hui, rien n'est défini. Ils se tournent donc vers des amis, vers un service après-vente des matériels mais ils ne trouvent pas forcément de réponses quant à la sécurité.

Il serait souhaitable de développer des acteurs de proximité, des réparateurs en réponse à des incidents de sécurité ; ces personnes devant être capables de remettre en état un ordinateur, vérifier les virus qui l'ont affecté, comprendre ce qu'il s'est passé, expliquer à la victime ce qu'elle n'a pas bien fait. Or, aujourd'hui, ce genre de personne se forme sur le tas ou même n'existe pas. Ce type de service ou de formation n'existe pas.

De plus, **l'information sur ces incidents ne remonte pas**. L'ordinateur est remis en fonction mais la perte de données importantes ou confidentielles peut être à déplorer. Il faut donc développer des formations pour remédier à cela et créer cette chaîne incluant des réparateurs. »

Colonel Éric Freyssinet
Coordinateur du plateau d'investigation Cybercriminalité & Analyses Numériques (PI CyAN) - Pôle judiciaire de la gendarmerie nationale
6 mars 2014
Auditions. Tome II du présent rapport

E. LES INDUSTRIELS

Les industriels ont été les premiers à comprendre la nécessité de mettre en place une sécurité numérique à la hauteur du risque et même de la menace encourus. Mais pas tous les industriels et il s'en faut de beaucoup.

À la suite de la révélation d'une faille majeure dans la sécurité de l'Internet, en 2008, les cinq plus grandes entreprises du secteur de l'informatique et des réseaux (*Cisco systems*, *IBM*, *Intel*, *Juniper Networks*, et, *Microsoft*) ont créé une association à but non lucratif dénommée ***l'Industry Consortium for Advancement of Security on the Internet (ICASI)*** **pour démontrer les risques de sécurité liés aux cartes-mères, aux logiciels, aux processeurs, aux réseaux, aux systèmes d'exploitation**, etc.

En France, plusieurs initiatives coexistent.

III. ORGANISATION DE LA SÉCURITÉ NUMÉRIQUE

De nombreux domaines sont aujourd'hui confrontés à la gestion de situations de crise nées de la mise en danger de leur sécurité numérique. Le besoin de mesures institutionnelles est alors ressenti concernant les institutions spécialisées, leur rôle et leur accès, les normes, l'arsenal juridique, les certifications, les aides financières.

Le rôle des institutions spécialisées est d'apporter une aide au sein d'un écosystème. Pour être efficace, ces institutions ont intérêt à être multi-échelle en s'adressant aussi bien aux individus, entreprises, communautés, pays, continents et monde, dans les buts de faciliter la circulation des informations qui proviennent du contexte, d'ajuster les actions correctives et, enfin, de mesurer les variations de la cybercriminalité.

En outre, leur rôle, qui comprend la prévention comme le contrôle, mérite bien le nom de gouvernance. Ce système hiérarchique favorise la circulation des informations de contrôle en dépit des conflits d'intérêts. À noter que le mode d'accès aux institutions traduit leur capacité à rendre le service attendu d'elles ; cette caractéristique est donc essentielle.

A. LES INVESTIGATIONS DES OBSERVATOIRES PUBLICS ET PRIVÉS

Au-delà de l'évaluation de la criminalité numérique déjà évoqué, la notion d'attaque et sa mesure gagneraient à être précisées.

C'est avec ses repères sociétaux habituels que l'internaute s'engage dans l'échange. Parmi les préjudices remarquables, résultant d'actes interagissant entre les sphères sociétales et technologiques, le vol d'identité qui selon les statistiques du gouvernement québécois – l'un des rares à communiquer sur ce sujet – toucherait près de 15 % de la population d'internautes. L'obtention de telles statistiques bute sur la difficulté de s'accorder sur une définition technique et juridique d'un tel vol, d'où le fait que tous les pays n'en comptabilisent pas les mêmes formes. De plus, seule une minorité de victimes (21,8 % au Québec) déclarerait ce type de préjudice.

Enfin, le **manque de méthodologie de surveillance** est lié aux faibles taux constatés de ce délit et aux dommages limités qu'il entraîne en raison notamment de la politique de dédommagement systématique menée par les établissements financiers.

En France, en 2013, ce sont 236 millions d'euros de petits cyberlarcins qui ont été commis au moyen de malveillances dans les échanges technologiques et sociaux.

La dangerosité ne provient pas des conséquences de tels larcins (d'un montant estimé inférieur à 100 $ par victime) mais de son étendue dans le temps (réitération et récidive) et dans l'espace (absence de frontières) ainsi que de la facilité insidieuse de son mode opératoire. L'étendue se traduit en plus du nombre de victimes par la nature très variée de son utilisation allant de la fraude bancaire (obtention de crédit), à la fraude aux services, qu'il s'agisse d'immigration, de terrorisme ou de justice.

En dehors de l'utilisation frauduleuse de cartes de crédit ou de cartes Vitale, le vol d'identité consiste aussi pour le délinquant à voler ou obtenir des « renseignements d'identification personnelle » ou des « documents d'identification personnelle » comme, par exemple, un permis

de conduire, un certificat de naissance, une carte de sécurité sociale, un badge d'employé ou encore à diffuser ou vendre de l'« information d'identification personnelle », comme une facture de services publics (*EDF*), à un groupe du crime organisé.

À ces inquiétudes sapant la confiance que l'on peut éprouver envers un système technologique, vient s'ajouter l'incompréhension née de résultats statistiques contradictoires en fonction des différents observatoires privés ou publics de la sécurité consultés. Par exemple, les statistiques d'incidents publiés par le CERT évaluent le risque d'intrusion en France à 8 % environ.

L'enjeu de publier des statistiques cohérentes est extrêmement fort puisque c'est au travers d'outils d'informations pertinentes et utiles que les usagers retrouveront leur confiance dans l'Internet.

B. L'INVESTIGATION POLICIÈRE

L'étude de la dangerosité des comportements relève des sciences criminelles et se concrétise par l'infraction qui est une atteinte à la loi, « *une action ou omission de nature à troubler l'harmonie sociale* ». À l'infraction correspond une sanction selon une échelle de valeur partagée entre la société et la victime. Cette mesure est approximative car elle se fonde sur l'infraction à des règles sociétales préétablies.

Pour qu'un crime ou un délit soit avéré et une sanction appliquée, la preuve doit en être apportée. De cette notion de preuve, fondamentale en droit français, dépend l'existence juridique d'un crime au travers de la présence conjointe de l'**intention de nuire** de l'auteur, d'un **préjudice** et d'une **plainte**. Afin de déjouer les formes d'attaques des plus dangereuses et d'identifier les auteurs des crimes et délits, les sociétés modernes se sont dotées d'une discipline scientifique. C'est le rôle des sciences forensiques, plus couramment appelées criminalistiques, d'étudier les modes opératoires en se fondant sur des outils et des méthodes.

Le fondement de la criminalistique repose sur le principe de Locard qui concerne **l'utilisation de traces comme preuves.** En effet, en application du « principe de transfert de traces » qui ne peut manquer d'être constaté lors d'un crime, l'identification de traces d'un individu sur une scène de crime ou/et la trace d'une scène de crime sur un individu sont recherchées ; le « principe d'individualité » permet ensuite, par comparaison, de confondre un criminel ; l'ensemble étant permis grâce à l'isolation de la scène de crime.

Mais il semble que **le principe de Locard rencontre des impossibilités techniques pour s'appliquer dans le domaine de la cybercriminalité**.

« Le gros problème en matière de cybercriminalité, c'est l'absence de lien entre le lieu de l'infraction et son auteur. En effet, le principe d'échange de Locard ne s'applique pas à la cybercriminalité. C'est un gros changement pour les forces de l'ordre en général. L'attaquant n'est pas forcément en Europe, il a peut-être rebondi sur un site au Venezuela ou au Vietnam. Ou ce peut être une attaque entre deux personnes situées dans la même rue. La perte de ce lien géographique appelle nécessairement une coopération entre les polices internationales. »

M. Jean-Dominique Nollet
Lieutenant-colonel de la Gendarmerie nationale, chef d'unité de laboratoire de recherche Centre européen de lutte contre la cybercriminalité (EC3) à Europol
19 juin 2014
Auditions. Tome II du présent rapport

C. L'ASSURANCE CONTRE LE RISQUE CYBER

En fonction de l'**analyse de risque de sécurité informatique** relatif à l'ensemble d'une entreprise précédemment réalisée, incluant celle des signaux faibles – indispensable mais difficile à mener, il convient d'**analyser les causes** des dommages, constatés ou non, **le transfert de responsabilité et la possibilité d'assurer les dommages**.

Comme pour tous les dommages dont risque d'être victime une entreprise, il est du devoir de ses dirigeants de tenter d'en réduire les impacts et de contracter une assurance pour se couvrir du montant du préjudice subi.

En matière de risque numérique, l'offre d'assurance est très peu développée. En effet, les assureurs ont coutume d'évaluer les risques en fonction de statistiques fiables et indépendantes mais, en l'occurrence, les risques cyber étant très divers et les incidents probablement très mal recensés, notamment au niveau de leur coût, **les risques numériques antérieurs ne permettent pas de prévoir les risques futurs**, d'où une réticence certaine des assureurs et, *a fortiori*, des réassureurs à s'emparer du marché du risque numérique.

En outre, comme il est très difficile voire impossible pour l'assureur de savoir si son client a mis en œuvre toutes les mesures de sécurité numérique possibles pour éviter la survenance d'un sinistre, **le calcul de la prime d'assurance est quasi impossible**.

Si les assureurs venaient à s'intéresser davantage à ce domaine, il est probable qu'ils manifesteraient alors des exigences de protection qui deviendraient, tôt ou tard, de nouvelles normes de sécurité.

IV. LES OPÉRATEURS D'IMPORTANCE VITALE (OIV)

Plus de **deux cents opérateurs d'importance vitale**, dont la moitié appartenant au secteur privé, sont recensés en France

Cependant il est évident que la sécurisation numérique des OIV, qui sont des entreprises de tailles diverses, ne doit pas se limiter à ceux-ci mais également s'étendre à des entreprises employant des personnels nombreux ou traitant de secrets technologiques ou industriels, sans compter que **toute entreprise peut être utilisée comme relais dans des attaques de grande ampleur**.

La sécurisation numérique des opérateurs d'importance vitale (OIV) s'insère dans une construction d'ensemble partant du Livre blanc de la défense et de la sécurité nationale et de la loi de programmation militaire qui prévoient des **référentiels de sécurité édictés par l'État pour les systèmes d'information critiques**. Elle tend à améliorer la détection des attaques informatiques grâce à des systèmes exploités sur le territoire national par des prestataires qualifiés et de **notifier toutes les attaques informatiques à l'ANSSI et aux autorités de régulation compétentes** dans leur secteur, comme l'Autorité de sécurité nucléaire (ASN), par exemple.

En outre, la loi de programmation militaire de 2013 a prévu :

– le **droit pour le Premier ministre d'imposer des règles de sécurité aux systèmes d'information critiques des opérateurs d'importance vitale**, par exemple l'installation de systèmes de détection d'attaque labélisés par l'ANSSI ;

- la **notification obligatoire au Premier ministre de certains incidents de sécurité** ;

- la **mise en place de contrôles de sécurité effectués discrétionnairement sur ordre du Premier ministre**, et aux frais des opérateurs, par l'ANSSI ou des prestataires qualifiés par elle ;

- enfin, **en cas de crise majeure, le Premier ministre peut décider des mesures que les opérateurs doivent mettre en œuvre** ;

Après une période de concertation au cours de l'année 2014, **des mesures devaient être mises en place au 1er janvier 2015 selon des agendas adaptés à chaque secteur d'activité d'importance vitale**.

De plus, **les systèmes d'information critiques des OIV doivent faire l'objet de contrôles**.

Enfin, **en cas d'attaque majeure, ces opérateurs devront mettre en œuvre toute mesure de défense informatique décidée par le Premier ministre**.

Ces attaques informatiques majeures sont considérées avec autant d'attention qu'un état de guerre, de terrorisme ou des actes d'espionnage.

À noter que l'application de ces règles peut rencontrer des difficultés dans la mesure où la liste des OIV étant classifiée « confidentiel défense », **certains dirigeants et, *a fortiori* leurs personnels, ne sont pas toujours au courant du statut d'OIV de leur entreprise et ne peuvent donc avoir qu'une conscience limitée des enjeux de sécurité nationale liée à son activité**.

Comme l'entreprise doit s'organiser eu égard aux états de crise numérique envisagés, elle doit commencer par **indiquer clairement à l'ANSSI les personnes constituant des points d'entrée dans l'entreprise** afin que la gestion de l'attaque ne soit pas déficiente dès les premières minutes. En effet, **il est essentiel que les dirigeants de l'entreprise comprennent immédiatement le caractère vital de la menace exercée à leur encontre**.

Jusqu'alors, en cas de crise numérique, les entreprises n'avaient pas tendance à se tourner vers l'État car il n'existait ni partenariats ni, *a fortiori*, d'exercices de crise entre elles et l'ANSSI. Désormais, les entreprises devront davantage étudier les interdépendances existant entre elles et leurs sous-traitants et fournisseurs.

De plus, il n'est pas toujours aisé de déterminer le type d'attaques qui aura le plus d'impact sur telle ou telle entreprise.

Il est important que les OIV mettent en place des systèmes de détection qualifiés mais les systèmes de détection actuels étant majoritairement nord-américains, un problème de souveraineté se pose.

Vos rapporteurs espèrent que, de ce problème, puisse jaillir une opportunité dans la mesure où la possession de sondes de détection de confiance devrait pouvoir faire naître un marché d'outils souverains français ou européens.

L'ANSSI pourrait d'ailleurs aider les entreprises à s'entraîner pour tester leur matériel à partir de la détection d'incidents passés non répertoriés officiellement ;

Enfin, de grandes entreprises seront peut-être considérées comme des OIV en France et également, ou non, à l'étranger, ce qui peut compliquer les règles à leur appliquer selon le territoire considéré.

A. LA PROBLÉMATIQUE GÉNÉRALE

La perception de l'importance stratégique des opérateurs d'importance vitale est assez récente puisque **c'est un arrêté du 2 juin 2006 qui dresse la liste des secteurs d'activité d'importance vitale**, c'est-à-dire ceux liés à la possibilité de l'exercice de la souveraineté nationale.

Le bon fonctionnement des onze secteurs recensés repose sur le numérique. Certains concernent très directement le numérique comme, par exemple, les matériels destinés à intercepter les correspondances, à détecter à distance les conversations, la cryptologie et la cryptographie, l'évaluation de la sécurité des produits et des systèmes de l'information.

Les investissements étrangers dans ces secteurs doivent être autorisés par le ministre chargé de l'économie.

Depuis 2006, **les directives nationales de sécurité (DNS) ont précisé ce qu'il fallait entendre par opérateurs d'importance vitale et les droits et obligations attachées à ce statut**.

À noter qu'une trop grande rigidité en la matière risquerait de ne pas être adaptée à la rapidité des mutations.

Par comparaison, aux États-Unis d'Amérique, le président peut placer à tout moment un secteur d'activité, une organisation ou une entreprise sous la protection dont bénéficient les opérateurs d'importance vitale. Cette réactivité peut permettre d'empêcher à temps un investissement étranger intempestif.

Il est vrai que c'est dès 1998 que le président William Clinton a pris le décret présidentiel n° 63 pour mettre en place une « protection des infrastructures de base des États-Unis » au moyen notamment d'une coordination assurée par le *National Infrastructure Protection Center (NIPC)*.

Les attentats du 11 septembre 2001 ont conduit au renforcement de cette préoccupation à travers une série de nouveaux organismes et de programmes incluant d'ailleurs une **capacité offensive en matière de cybersécurité** et **l'organisation régulière, dès 2006, de simulations d'attaques numériques à grande échelle contre le pays** incluant des entreprises et des gouvernements étrangers comme ceux du Canada, du Royaume-Uni et de la Nouvelle-Zélande.

Comme toujours aux États-Unis d'Amérique, ces initiatives ont été accompagnées, dès 2003, par l'**édiction de normes** relatives, cette fois, à la **sécurité du parc informatique des administrations fédérales et des systèmes de communication stratégiques**.

B. L'EXEMPLE DU SECTEUR DES TÉLÉCOMMUNICATIONS

Les opérateurs de télécommunications cumulent plusieurs rôles : ils sont à la fois opérateurs d'infrastructures et de services Internet et de téléphonie. Ils fournissent, par exemple, des centres de données permettant aux opérateurs d'importance vitale d'externaliser l'hébergement de leurs données.

Face au risque numérique, **les opérateurs de télécommunications placent au premier rang la capacité de réaction** à partir d'une organisation

agile aux cycles de décision courts avec des dirigeants et des collaborateurs impliqués et pragmatiques.

Quant à **la protection**, elle **est conçue dans la profondeur.**

> « Il convient enfin d'**opter pour « *une protection dans la profondeur* », soit un système de défense organisé autour de cercles concentriques de plus en plus sécurisés**. Au niveau de chaque cercle, les problèmes doivent être détectés, analysés et corrigés. Nous devons **être dans un état de « *paranoïa raisonnable* »**, c'est-à-dire qu'il nous faut nous astreindre à **une vigilance permanente, où tout risque de relâchement – dû notamment à la croyance en une technologie miracle –, est prohibé. »**
>
> ***M. Alexandre Archambault***
> ***Responsable des affaires réglementaires, en charge des obligations légales, Free.***
> *26 juin 2014*
> *Auditions. Tome II du présent rapport*

Certaines entreprises de télécommunications, comme *Orange*, sont considérées comme des entreprises d'importance vitale et sont donc soumises à des contraintes particulières : par exemple, **ses administrateurs informatiques ne disposant que de postes de travail non reliés à la messagerie ou à l'Internet, doivent utiliser d'autres postes pour intervenir sur un système à distance.**

Des **projets dits « confidentiels défense** » nécessitent la délimitation de **zones réservées** à leur traitement à l'intérieur desquelles, par exemple, il est recouru à la précaution consistant à **laisser son téléphone portable à l'entrée** et où **aucune connexion Internet n'est possible**.

Free a décidé de **limiter voire d'exclure toute infogérance** et de **stocker ses données sensibles en interne**.

Free achète ses équipements mais maîtrise ses réseaux. Cependant, pour les routeurs et les solutions mobiles, **les équipementiers sont soumis à des obligations de sécurité spécifiques**. De la sorte, les réseaux français de troisième génération (3G) et de quatrième génération (4G) ont atteint un degré de sécurité supérieur aux normes fixées par le *Third generation partnership project (3GPP)*.

Il est à noter que, en dépit d'une vive concurrence commerciale entre opérateurs de télécommunications, la forte interdépendance entre eux les conduit à **partager rapidement toute information en cas de crises** au cours desquelles **la capacité de réaction importe plus que tout.**

La Fédération française des télécoms (FFT) relève qu'**il est impossible – et, en tout cas, très coûteux – de savoir ce qu'il y a derrière les composants à partir du moment où on ne les fabrique pas.** D'où, pour les entreprises, la **recherche permanente d'un équilibre entre le risque et les opportunités au moyen d'évaluations de risque**.

La FFT souhaite que soient mis en place un label européen de stockage de données et que les logiciels et les équipements critiques diffusés en Europe soient soumis à une certification.

C. L'EXEMPLE DU SECTEUR DE L'ÉNERGIE

À la lumière des attaques subies par *Saudi Aramco* et *RasGas* en 2012, les opérateurs du secteur de l'énergie ont constaté que **l'avantage est toujours du côté des attaquants en matière de risque numérique**.

D'où la nécessité d'une anticipation méthodique incluant l'élaboration d'une **cartographie des risques numériques** assortie d'un **plan de sécurité des systèmes d'information actualisé chaque année**.

Pour *Total*, ce plan repose sur les quatre piliers suivants : **la sécurisation du système d'information de gestion** incluant les infrastructures des services partagés (télécommunications…) pour les mille sites de *Total* dans le monde reliés à des entités du groupe ; **la sécurité de l'information industrielle ; la sécurité des applications** et, enfin, **la sensibilisation des utilisateurs** pour changer leurs comportements.

Ce plan prévoit d'**apporter un soin particulier aux systèmes de commande, les *SCADA***, au sein de l'information industrielle dans la mesure où la vulnérabilité de ces systèmes repose sur des composants informatiques traditionnels.

Plus qu'à une logique de prévention, *Total* s'oriente vers une **logique de détection et de réaction rapide grâce à un centre opérationnel de sécurité**.

Dans cette optique, **le partage d'informations** avec d'autres opérateurs du secteur de l'énergie ou avec l'ANSSI est un gage d'efficacité accrue.

Toutefois, ces fonctions sont d'autant mieux assurées que les équipements stratégiques sont conçus par des entreprises françaises et que les personnels comprennent la nécessité de changer les comportements.

À noter les **réticences de *Total*, de *GrDF* ou encore d'*AREVA* à utiliser le numérique en nuage** actuellement insuffisamment sécurisé et qui doit être assorti d'un **système d'authentification** et de **chiffrement**. *GrDF* stocke 90 % de ses données dans des centres privés ; seules celles ne présentant pas de caractéristiques particulières sont stockées dans un nuage public.

Total estime que seules les données peu confidentielles peuvent être stockées dans le nuage public, d'où la **nécessité de distinguer entre diverses catégories de données dont certaines sont interdites de stockage dans un nuage public.** En fin de compte, ***Total* préfère louer des centres de stockage de données qui lui soient propres**.

D'une manière générale, ***Total*** observe les **règles d'hygiène informatique édictées par l'ANSSI et par la CNIL** et choisit ses matériels et ses fournisseurs à partir des **référencements de l'ANSSI**.

Même si seule une petite partis des activités de *Total* (raffineries, quelques dépôts, les *pipes lines*, etc.) est considérée comme relevant d'un opérateur d'importance vitale, **le plan global de sécurité est appliqué à l'ensemble de ses activités** et l**e référentiel de sécurité est étendu également aux filiales et aux sous-traitants auxquels un plan d'assurance sécurité est imposé.**

Pour le *CEA*, opérateur d'importance vitale à plusieurs titres, certaines données ne doivent faire l'objet d'aucune attaque. Dans ce contexte, **est présumée avoir un caractère professionnel toute information traitée par les moyens informatiques du *CEA***.

Le *CEA* a créé **son propre laboratoire de sécurité des systèmes d'information**, placé auprès de la direction centrale de la sécurité.

Les téléphones et les abonnements professionnels fournis par le *CEA* à son personnel peuvent être désactivés en cas de difficulté. **Ces matériels disposent d'un code d'accès et ne permettent pas d'afficher les contenus chiffrés de la messagerie CEA**.

Quant aux **ordinateurs portables deux systèmes de chiffrement –** antivol et *data* – assurent leur sécurisation.

Face à l'informatique en nuage et à l'infogérance, le *CEA* pose que, pour conserver la maîtrise de son système d'information, il ne doit **pas utiliser le *cloud computing* et ne recourir à l'infogérance qu'à condition d'héberger les sous-traitants dans ses locaux.**

Pour *GrDF*, la préférence est donnée à **l'intégration de la sécurité numérique dès la conception** (*GrDF*). Dans le même esprit, **le degré de confidentialité des données est évalué** (*GrDF*), ce qui donne lieu ensuite à différentes conditions de fonctionnement des applications et de mise à disposition des données. **Les données personnelles sont celles qui bénéficient de la meilleure protection** au sein du système d'information

90 % des données sont stockées dans des centres privés mais celles qui ne présentent pas de caractéristique particulière sont conservées dans un nuage public.

CHAPITRE III – LA COMPLEXITÉ DU NUMÉRIQUE REND SA SÉCURITÉ POUR LES ENTREPRISES DIFFICILE À CONCEVOIR

C'est dans le contexte complexe et extrêmement mouvant décrit au chapitres précédents **les entreprises utilisant toutes le numérique sans toujours avoir eu la possibilité et la capacité d'en mesurer pleinement les potentialités ni toutes les failles**.

Pour être à même de comprendre la situation actuelle des entreprises face au risque numérique, vos rapporteurs ont estimé indispensable d'analyser la complexité du numérique, la nature d'un message et la place de l'information dans l'entreprise.

Le présent chapitre se borne à en donner un aperçu largement illustré par des schémas conçus par l'OPECST.

Pour concevoir le numérique, dont les multiples facettes (composants, ordinateurs, téléphones, objets connectés, logiciels, réseaux, Intranets, Internets, etc.) sont tellement liées à la vie quotidienne qu'elles ne sont même plus perceptibles, tout se passe comme si, pour dessiner un éléphant, chacun n'apercevait qu'une des parties de son corps : qui la tête, qui le dos, qui la trompe, qui la queue, etc.

Une des manières permettant de penser la complexité du numérique est, par exemple, de **parler non pas de l'Internet mais des Internets car s'il existe des frontières séparant le numérique du reste de la réalité, il existe aussi des frontières qui lui sont spécifiques, bien différentes de celles des États**.

L'usage du numérique se ramène à une relation entre l'usager, le propriétaire des ressources ou des données et le fournisseur. Aucun contrat n'en règle l'ensemble de l'économie.

L'Internet, et de façon plus générale le numérique, sont aujourd'hui au cœur de tous les échanges, de l'individu à l'entreprise, de l'entreprise à la société, de la société aux gouvernements. La question du rôle que celui-ci joue dans les échanges est centrale : L'Internet est-il un outil au service de ces échanges ou bien plus que cela ? En tant qu'outil est-il porteur des principes de base pour protéger les échanges ? Dans quelle mesure cet outil peut-il garantir qu'il ne modifiera pas, sous quelque forme que ce soit, les termes de l'échange entre les différents acteurs de l'entreprise, allant de l'employé, du client ou du fournisseur à l'entreprise ou aux institutions ?

Pour répondre à ces questions, il convient de mieux cerner les enjeux et les buts recherchés au travers de l'échange.

I. VERS UNE REPRÉSENTATION DU NUMÉRIQUE DE NATURE À FACILITER SA CONNAISSANCE

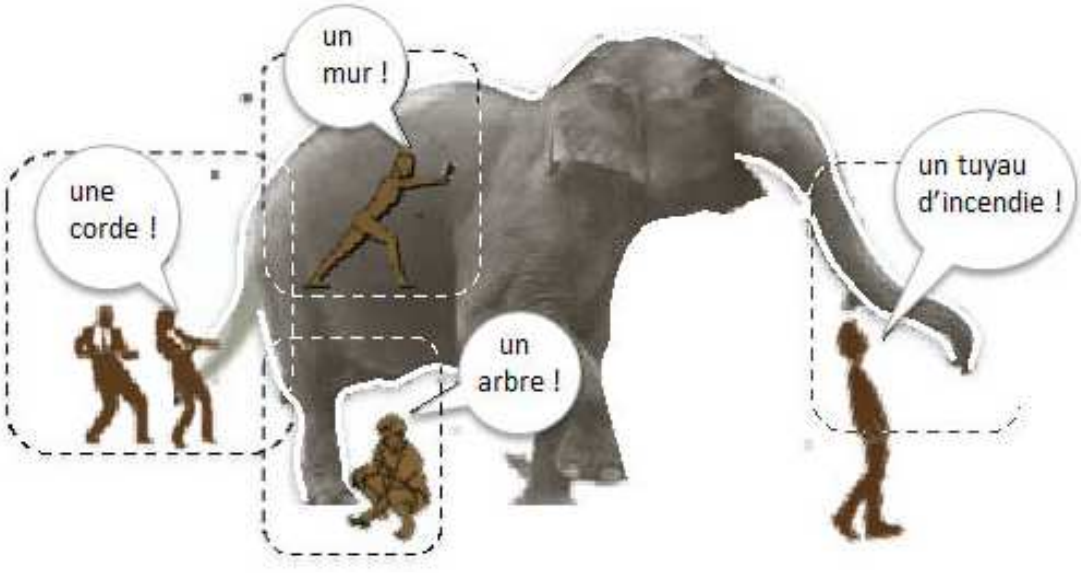
Pour tenter d'approcher la complexité du numérique, la tentation est grande de le tronquer et de le figer en pensant pouvoir ensuite considérer en lui-même chaque morceau du puzzle comme un tout mais, en réalité, séparant alors ce qui ne peut l'être. C'est ainsi que, souvent, le numérique à usage militaire est distingué du numérique à usage civil ou encore que le numérique à usage professionnel est distingué du numérique à usage personnel alors que ces deux distinctions sont des trompe-l'œil puisque **la sécurité du numérique est transversale et mêle militaire et civil, professionnel et personnel**.

« Pour autant, il a été choisi de ne pas retenir exclusivement cette approche « technophobe » et fausse – car l'informatique suppose à l'évidence l'utilisation d'un ordinateur – et nous avons recensé des activités possibles avec un ordinateur. Par exemple, le simple fait d'envoyer un courrier électronique et de se demander comment il parvient à destination ouvre un vaste champ de questions, qui conduisent à **s'interroger sur la manière dont les ordinateurs sont reliés entre eux en réseau d'un continent à l'autre, la manière dont les informations sont acheminées sur ces réseaux, etc.** »

M. Gilles Dowek
Secrétariat du groupe de travail de l'Académie des sciences
16 avril 2014
Auditions. Tome II du présent rapport

Ne pas assumer cette vision transversale de la sécurité numérique conduirait, comme l'explique le théorème de Hace, à ne pas comprendre que **la non-protection du système pourrait être à l'origine d'une grande catastrophe. Ces imbrications doivent être prises en compte pour assurer la sécurité numérique des entreprises**.

Schéma n° 5 : Illustration imagée de la complexité par le théorème de Hace



***Source** : ACE*

Or **le numérique n'a pas de forme finie, il est protéiforme** comme l'a suggéré M. Bernard Stiegler lors de son audition.

La difficulté de représenter le numérique tient au fait que ce réseau des réseaux – incluant tous les objets et outils qui y sont liés – est immense, dynamique et omniprésent impliqué dans tous les échanges, qu'ils soient humains ou technologiques. Ainsi, le numérique se présente-t-il à chacun comme **une, voire plusieurs, « boîtes noires » fascinantes**, augmentant nos capacités d'échange et de coopération tout en en atténuant l'éloignement, l'absence ou même l'ignorance.

Néanmoins, **en matière de sécurité, la représentation du système est une condition essentielle à un usage responsable**. En effet, si ses caractéristiques physiques (forme, poids, etc.) ainsi que les effets produits sont méconnus, le bon usage de l'outil échappe à l'usager. C'est l'idée qu'a développée M. Bernard Stiegler en évoquant le *pharmakon* : toute technique n'est ni bonne, ni mauvaise en elle-même, « *un marteau sert à construire sa maison mais aussi à assassiner son voisin…* ».

Ainsi, l'Internet, et le numérique de façon plus générale, ne sont-ils que des outils pour accomplir les échanges. Pourtant, on parle des abysses de l'Internet pour exprimer que l'**Internet dépasse la compréhension qu'en ont les usagers,** risquant par conséquent, en cas de mauvais usage, de compromettre leur sécurité mais également celle de leurs interlocuteurs, allant des simples usagers aux opérateurs d'infrastructures critiques.

Pour améliorer cette compréhension, vos rapporteurs ont souhaité décrire l'échange dans les communications humaines comme dans les communications numériques car **il importe d'améliorer la connaissance pour créer de la confiance**.

A. L'ÉCHANGE ET LES COMMUNICATIONS HUMAINES

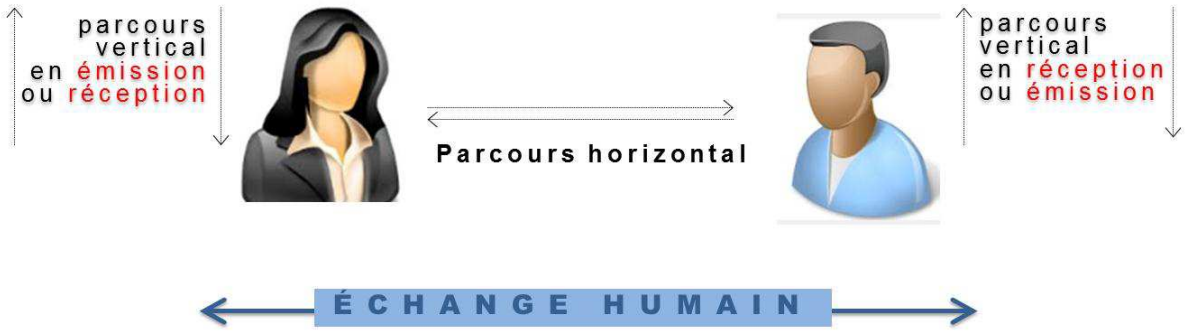
L'échange est l'activité à l'origine de l'évolution de tout être vivant. Chez l'Homme, l'échange représente le moyen par lequel chacun progresse vers une finalité qu'il partage avec un autre, une communauté ou une société.

La **finalité** représente ce que chacun attend de l'échange, un **projet** où chacun met en œuvre un **processus d'amélioration** de sa situation existante par la consommation ou la production de l'objet qui lui sera utile. L'objet peut être **matériel** (échanger un bien), **informationnel** (échanger un message) ou même de **connaissance** (échanger un savoir-faire).

Ainsi, l'échange s'accompagne-t-il avant tout d'un **objet**, matériel ou immatériel, qui détermine **l'enjeu** de l'échange, c'est ce qui appelle dans l'échange le **comportement réciproque** entre l'auteur et son interlocuteur où chacun devient tour à tour le sujet et le destinataire.

Entre **finalité** et **réciprocité**, l'échange représente un processus à deux dimensions : l'échange dit « vertical » ou interne mené par chaque interlocuteur en lui-même ; l'échange dit « horizontal » plutôt tourné vers l'interlocuteur extérieur ; pour former ensemble : un « système global » qui relie les humains.

Schéma n° 6 : Processus « vertical » ou interne puis « horizontal » ou externe de l'échange humain



Source *: OPECST*

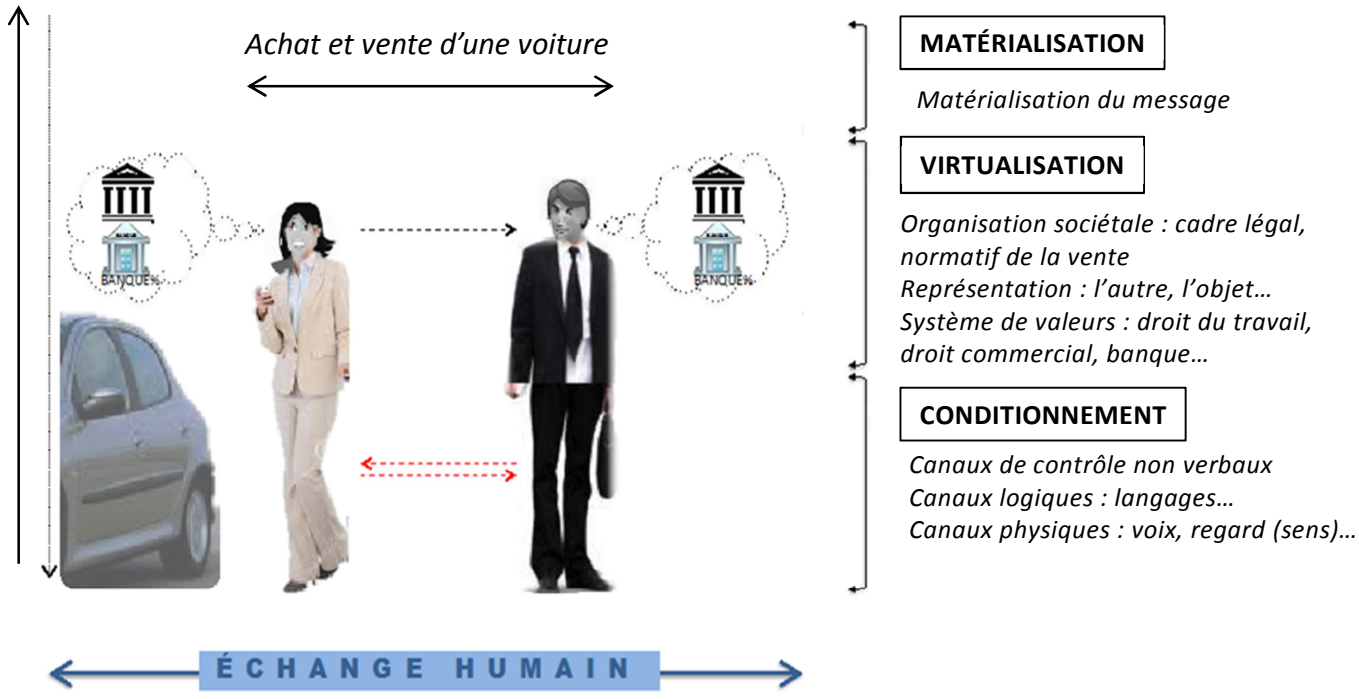
1. Le processus « vertical » ou interne de production des messages en vue de l'échange

Le processus « vertical » ou interne de l'échange regroupe l'ensemble des moyens pour passer du projet d'échanger, par exemple, acheter ou vendre une automobile, **à une série d'actions d'échanges guidées par la finalité de l'échange**.

Ce processus prépare en particulier l'objet échangé pour son transfert regroupant les conditions favorables. Lors du processus « vertical », **l'objet de l'échange subira trois transformations** : la **matérialisation** pour définir l'objet dans le monde réel – il s'agit de l'achat ou de la vente d'une automobile ; la **virtualisation** pour définir l'objet dans un système de valeur et de référence, individuel et sociétal – des règles sont à respecter, des documents à réunir présentant certaines caractéristiques lors de la vente d'une automobile ; le **conditionnement** pour définir l'objet dans le système de transport des messages liés à cette vente.

Ces trois niveaux sont illustrés ci-après à partir de l'exemple d'un échange entre deux individus dont l'objet serait la vente d'un véhicule automobile.

Schéma n° 7 : Les trois niveaux verticaux ou internes de l'échange humain : matérialisation, virtualisation, conditionnement du message



Source *: OPECST*

a) La matérialisation du message

Le processus de matérialisation définit l'existence de l'objet, ici de l'automobile, sa réalité, qui, à l'inverse d'un monde virtuel ou d'un monde imaginaire, se traduit par l'existence de **propriétés évaluées de façon tangible** au travers de nos sens et de nos connaissances. La voiture se caractérise par la matière dont elle est faite et ses propriétés réelles comme sa

forme, sa couleur, ses performances techniques, etc., tout cela va influer sur sa vente.

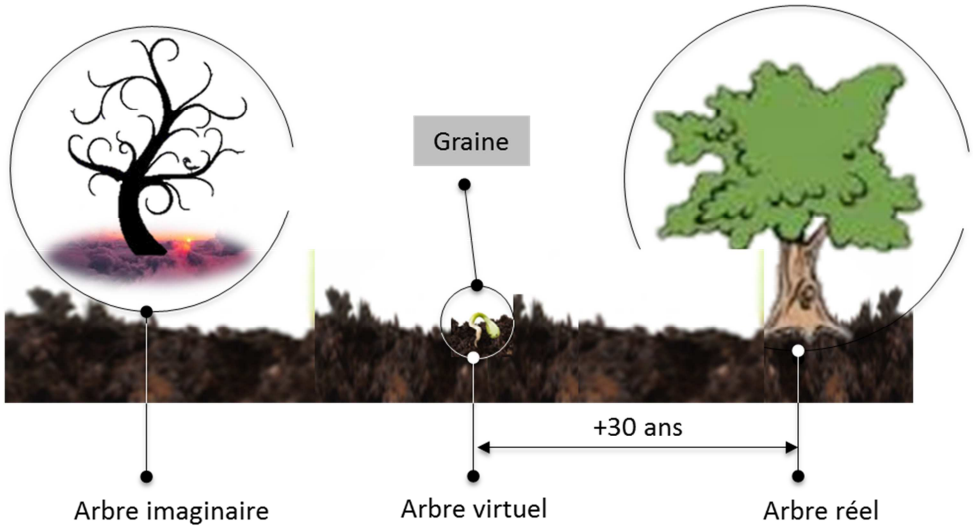
Pour bien appréhender la différence entre l'imaginaire, le virtuel et le réel, l'exemple de l'arbre, illustré ci-après, souligne que **l'imaginaire ne saurait se confondre avec le virtuel**, alors que **ces deux notions sont très souvent confondues lorsqu'il est question du numérique**.

b) La virtualisation du message

Le processus de virtualisation situe l'objet, ici l'automobile à vendre, dans un système de référence et de valeurs. Le cadre virtuel permet à chacun de représenter l'objet dans ce système à l'aide de règles et d'institutions (le droit commercial, la monnaie choisie, etc.). Ce cadre permet de **fournir les éléments de décision** qui vont guider les actes que chacun envisage. C'est en cela qu'il est nécessaire d'expliquer souvent que **le virtuel ne s'oppose pas au réel mais à l'actuel**.

Dans la poursuite de leur objectif, les interlocuteurs conviennent au préalable d'**un système de valeurs individuel ou sociétal, régulé par un tiers de confiance afin de garantir la bonne fin de l'échange**. Il peut s'agir, par exemple, du droit civil, du droit commercial en vigueur en tel pays, d'une banque, d'une institution de confiance pour garantir la valeur de la monnaie de l'échange. Ce niveau est qualifié de virtuel car les actes de l'organisation ne se manifestent que plus tard par leurs effets.

Schéma n° 8 : Illustration des concepts de « imaginaire, virtuel, réel »



Source *: OPECST*

c) Le conditionnement du message

Le processus de conditionnement définit les propriétés que l'objet de l'échange devra respecter pour son transport au travers de son système de communication qui a également pour rôle de **relier les interlocuteurs** de l'échange en un même lieu ou comme s'ils étaient en un même lieu. Le **lieu** de l'échange est le lieu des pactes et négociations.

Ce processus assure la transformation de l'objet pour son transport, en particulier lorsque le lieu de l'échange est distant.

Dans le cas d'échange de messages humains, le processus de conditionnement transforme le message à l'aide d'un **langage** puis l'adaptera sous forme d'un **signal** par le biais d'un **adaptateur** : l'**organe de la voix** qu'un interlocuteur captera à l'aide de son **organe sensoriel auditif**.

2. Le processus « horizontal » ou externe de transport du message

Pour atteindre sa finalité dans l'échange, chacun a recours à plusieurs canaux de communications, tous en charge d'un rôle particulier. Les sciences humaines qualifient de **mode « multicanal »** ce mode de communication, qu'il soit à l'échelle de l'individu ou du groupe.

On distingue les canaux logique, physique et de contrôle.

- *Le canal logique de l'échange*

Le canal logique représente le médium de **transport des messages codés à l'aide d'une langue ou d'un code** dans le but de les rendre transportables puis intelligibles à son ou ses destinataires en préservant le sens et l'organisation originels de l'information transportée. Par exemple, une phrase en chinois ne sera pas comprise par un Français ne maîtrisant pas le chinois.

- *Le canal physique de l'échange*

Le canal physique permet le **transport de l'objet**, ses caractéristiques seront directement liées aux contraintes qu'imposent conjointement l'objet transporté, le milieu de son déploiement puis la cible vers laquelle il est dirigé et la source qui l'émet. Cela suppose des capacités d'adaptation à chacun de ces niveaux : l'objet, le milieu, les sources et destinataires. Par exemple, un message oral sera transmis par la voix sous forme de signal, une automobile sera livrée par voie routière.

Schéma n° 9 : Établissement du canal « physique » de l'échange humain par la voix et divers organes sensoriels



***Source** : OPECST*

- *Le canal de contrôle de l'échange*

Le canal de contrôle dote chaque individu d'un mécanisme de **régulation** et de **contrôle** afin d'évaluer une situation en fonction des objectifs à atteindre. À l'aide de signes ou de paroles spécifiques, **ce canal assure la supervision de l'échange**, détecte des anomalies et émet des alertes en cas de déviance. Par exemple, on acquiesce en réponse à un interlocuteur soucieux d'avoir été bien compris.

3. Le niveau virtuel ou global de l'échange interindividuel et sociétal

L'échange est avant tout l'un des phénomènes à l'origine de toute vie individuelle et de groupe ; **c'est par leurs échanges que les sociétés d'hommes se sont organisées** pour leurs équilibres et contre leurs déséquilibres. L'échange sociétal fut, depuis le début du XX[e] siècle, un sujet d'étude pour l'anthropologie, comme en témoignent, par exemple, les ouvrages de Marcel Mauss[1] ou de Claude Lévi-Strauss[2] mais également, pour les sciences humaines et sociales, dès 1919, l'ouvrage fondateur de Rudolph Steiner qui a donné naissance à l'État « providence »[3].

---

[1] *Marcel Mauss, « Essai sur le don. Forme et raison de l'échange dans les sociétés archaïques », (1923-1924) dans A.A Sociologie et anthropologie, PUF, 1980, p. 145-279.*

[2] *Cité notamment par John Tolan, « L'échange : Séminaire Le Lien Social », Paris, L'Harmattan, 2009, pp. 201-214.*

[3] *Rudolph Steiner, « Kernpunkte der sozialen Frage »: « Les aspects fondamentaux de la question sociale - 1919 ».*

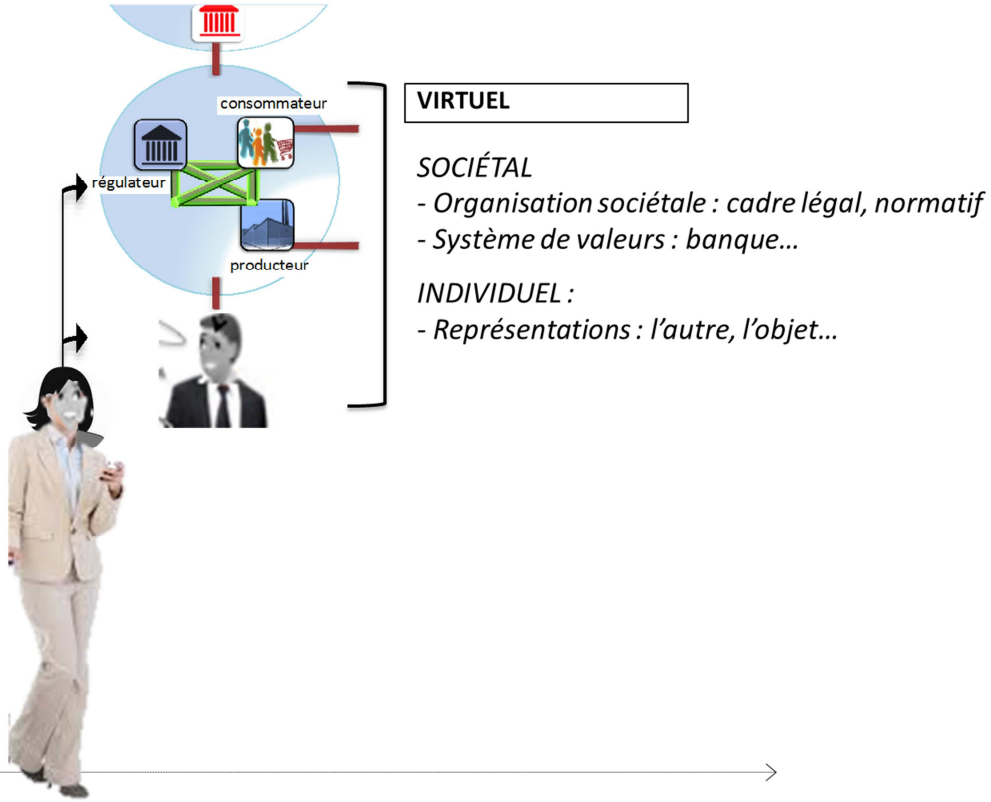
a) Structure interindividuelle de l'échange

L'échange se ramène à un ensemble d'actions et de réactions qui se succèdent entre un individu et son interlocuteur, chacun mû par l'**obligation de réciprocité**. De multiples formes d'échanges existent dont les manifestations peuvent être verbales ou/et non verbales pour que chacun puisse se situer vis-à-vis de l'autre pour décider d'échanger avec lui selon ce qu'il observe de lui et ce qu'il croit sur lui.

Chaque individu échange avec la connaissance du fonctionnement des sphères au sein de laquelle ou desquelles il échange et avec la connaissance de l'autre. D'où la nécessité, pour le numérique, de mettre ces connaissances à la portée du plus grand nombre, ce qui est loin d'être le cas actuellement.

Chaque individu prépare son échange en tant que consommateur et/ou fournisseur. Le rôle du niveau « virtuel » de chaque individu consiste à favoriser les chances d'atteindre sa finalité dans l'échange en prenant en compte les facteurs inter et intra sphères potentiellement capables d'influer sur la situation de l'échange.

Schéma n° 10 : Structure interindividuelle et sociétale de l'échange

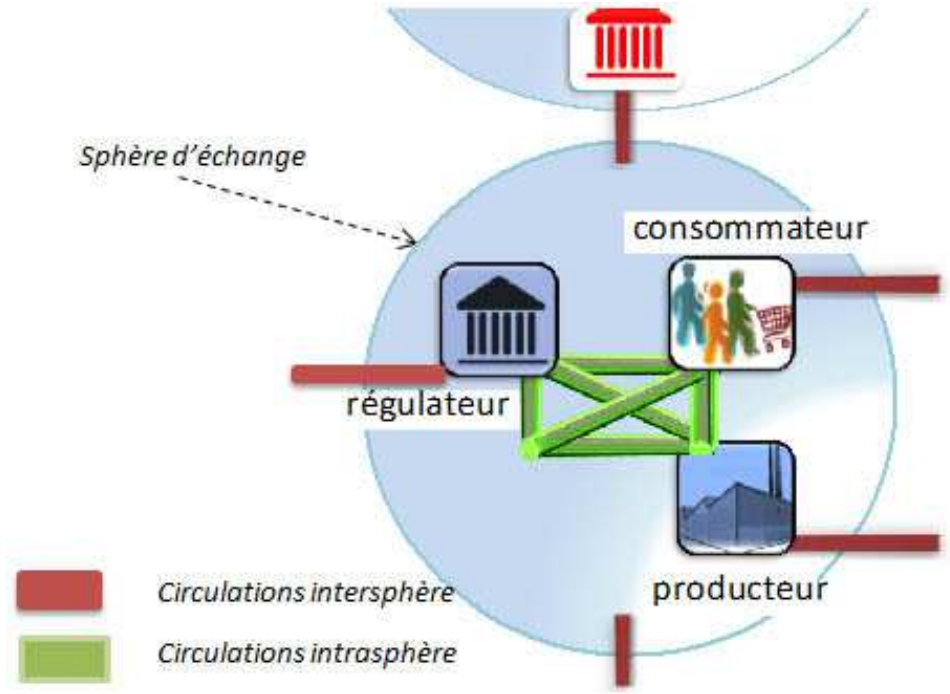


***Source** : OPECST*

b) Structure sociétale de l'échange

Il ressort des différents travaux cités ci-dessus un certain type de structure de sociétés modernes qui domine où on distingue **trois sphères d'échanges principales : l'État, le marché et l'individu**. Elles sont indépendantes, chacune offre des circulations, figurées en vert sur le schéma ci-après, mais capables d'interagir entre elles. Au sein de chacune de ces sphères, l'échange se définit comme « *le mode de circulation des biens et services impliquant une évaluation pour aboutir à un accord entre deux parties, le producteur et le consommateur*[1]». À noter également, que le mode de circulation dépend de l'objet et de la finalité de l'échange ; il caractérise chaque sphère régulée alors par une instance globale et supérieure.

Schéma n° 11 : Organisation sociétale de l'échange



Source *: OPECST*

c) Les principes de la circulation des biens et des services au sein de l'échange

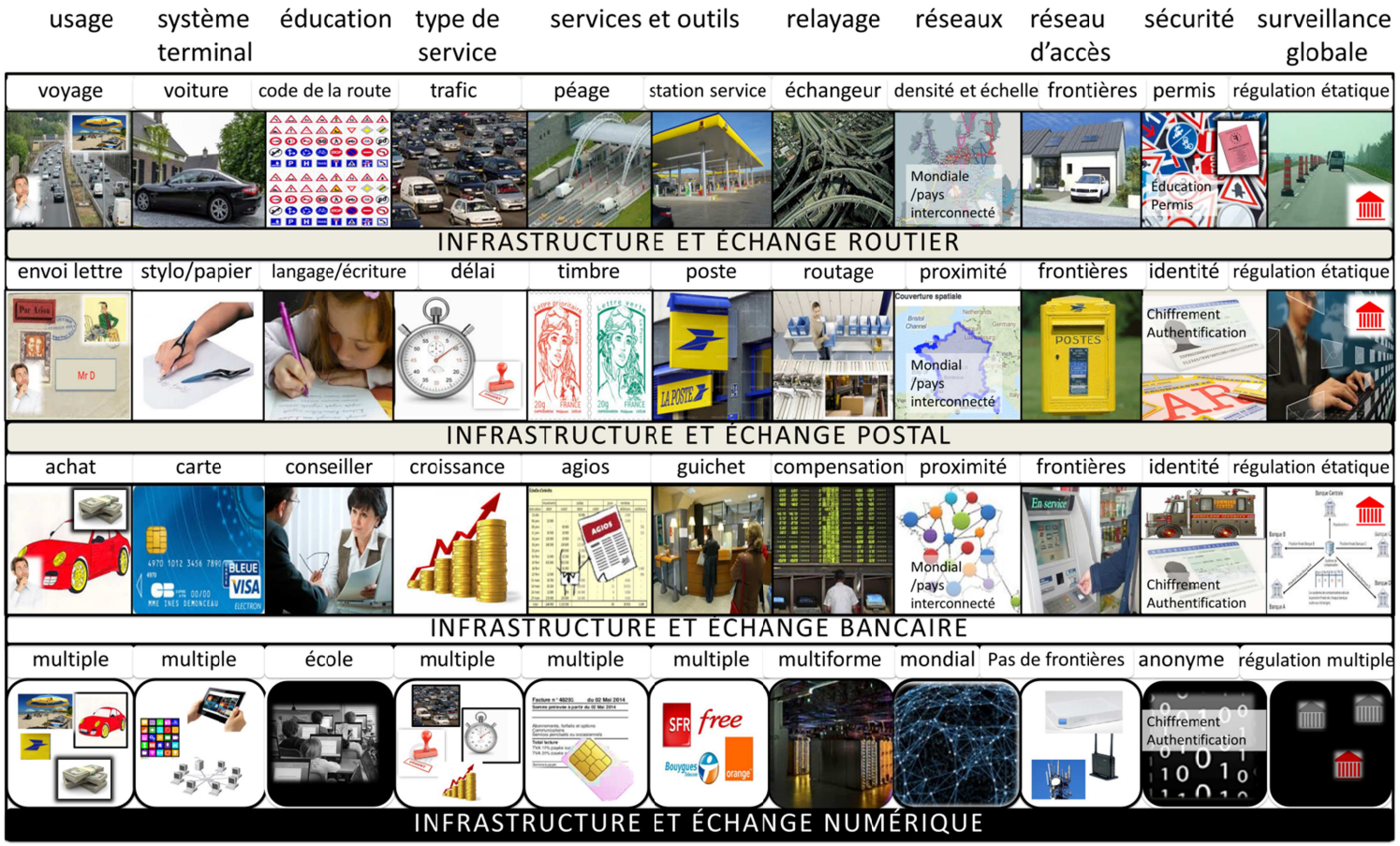
Les modes de circulation des biens et services se traitent différemment selon l'éloignement des interlocuteurs d'autant que l'objet de l'échange traversera les sphères publiques et privées.

---

[1] *Contributeurs de Wikipédia, « Échange » Wikipédia, l'encyclopédie libre, http://fr.wikipedia.org/w/index.php?title= %C3%89change&oldid=38160006 (Page consultée le 23 octobre 2009).*

Dans les différents modes de circulation pour l'échange représentés dans le schéma ci-après : routier, postal, bancaire puis numérique, **la circulation des biens et services est encadrée par des instances de régulation** car elle doit être optimisée entre tous les usagers. **L'échange ne peut être réduit à un simple canal de communication reliant un émetteur et son destinataire**. C'est ainsi que le rôle des infrastructures sera de mutualiser des services sociétaux et, d'autre part, d'en organiser le transport et la distribution.

Schéma n° 12 : Infrastructures sous-tendant divers types d'échange



***Source** : OPECST*

Dès lors que des infrastructures de l'échange relient deux interlocuteurs distants au moyen de **réseaux publics et privés**, plusieurs **propriétés** apparaissent comme essentielles :

- l'**usage** qui détermine la **finalité** que l'usager et le fournisseur de service poursuivent par le biais de la mise à disposition du réseau (un voyage, l'envoi d'une lettre, l'achat d'une automobile, **des usages multiples pour le numérique, etc.**). La forme et la performance de l'outil en seront les éléments clés ;

- les **systèmes terminaux** qui sont les **vecteurs du parcours vertical (interne)** de l'usager afin de produire l'objet de l'échange sous une forme compatible avec le médium de transport (grâce à une voiture, un stylo et du papier, une carte de crédit, **des systèmes terminaux multiples pour le numérique, etc.**) ;

- l'**éducation** qui situe l'usager dans le système communautaire en lui apprenant les concepts d'usage, droits, obligations et règles de prudence liée à la **mutualisation du réseau au niveau public** (ce qui suppose le respect du code de la route, de l'orthographe, de conseils techniques et **encore trop d'auto-apprentissage pour le numérique**, etc.) ;

- les **services** qui déterminent les **applications** dont peut tirer parti l'usager et pour lesquels il a été formé (prise en compte des réalités du trafic routier, des délais d'acheminement des données, des taux de change **et d'innombrables services et applications multiples pour le numérique**, etc.) ;

- la **performance** attendue du service qui détermine l'objectif entre l'usager et le fournisseur de service et, par là même, les **choix des outils** (voies à péage, stations-services ; timbres, bureaux de poste ; agios, agence bancaire, **outils multiples pour le numérique**, etc.) ;

- les **systèmes intermédiaires** (relayage ou routage) qui permettent de **remédier aux inconvénients dus à la distance** (échangeurs routiers ; routage postal ; chambres de compensation **; relais multiformes pour le numérique, etc.**) ;

- la **densité** et la **couverture** des réseaux qui déterminent la **proximité** du service pour l'usager et **l'équité** de sa distribution (réseaux routiers, postal, bancaire, nationaux et internationaux et **réseaux sans frontières pour le numérique**, alors que **la notion de frontière existe dans tous les échanges sauf pour l'échange numérique)** ;

- les **accès aux réseaux** qui déterminent la **souplesse** offerte à l'usager pour qu'il bénéficie du service ;

- la **sécurité des usagers, des réseaux et des objets** transportés qui déterminent les **risques** auxquels ils s'exposent et prévoient leur **éducation** ainsi que la mise à disposition d'**outils** pour qu'ils puissent **contrôler les effets de leurs actes** (permis de conduire et compteur de vitesse, accusé de

réception, balance de compte, **chiffrement et authentification pour le numérique**) ;

- la **surveillance globale** généralement sous la responsabilité de l'institution qui en assure la gouvernance et la régulation (**régulation étatique sauf pour l'échange numérique**).

Il apparaît que les infrastructures sous-tendant l'échange numérique se distinguent nettement des infrastructures sous-tendant des échanges traditionnels. Leurs caractéristiques sont celles du numérique : **anonymat, mondialisation et absence de frontières, multiplicité des usages et des régulations**.

B. L'ÉCHANGE ET LES COMMUNICATIONS NUMÉRIQUES

Comme explicité ci-dessus, **l'échange humain établit une communication multicanal** avec son interlocuteur au moyen des canaux logique, physique et de contrôle.

Lors d'un échange numérique, cette complexité est encore accrue par le réseau constitué d'une multitude de systèmes intermédiaires reliés entre eux et formant une multitude d'infrastructures : c'est un système de systèmes.

Ce sont ces entrelacs qui amènent souvent certains spécialistes à évoquer les Internets pour évoquer différents sous-ensembles :

- l'**Internet en tant que système de communication composé de canaux physiques et logiques** ;

- l'**Internet en tant que service entre clients et serveurs numériques** afin d'offrir des services numériques mutualisés comme, par exemple, la circulation des données des usagers ou leur stockage ;

- l'**Internet en tant qu'application** afin d'offrir de l'intelligence (communautés d'expérience : *Facebook*, *Doctissimo*, etc.) pour des usages humains et sociétaux.

Le numérique est à la fois un échange individuel et sociétal qui repose sur une infrastructure complexe. Dès leurs origines, les machines ont permis d'automatiser les activités complexes de la communication humaine. Mais le numérique, aujourd'hui, semble avoir élevé cette relation entre les individus au niveau d'un échange d'une complexité encore inégalée.

Schéma n° 13 : Échange à l'aide d'un réseau numérique

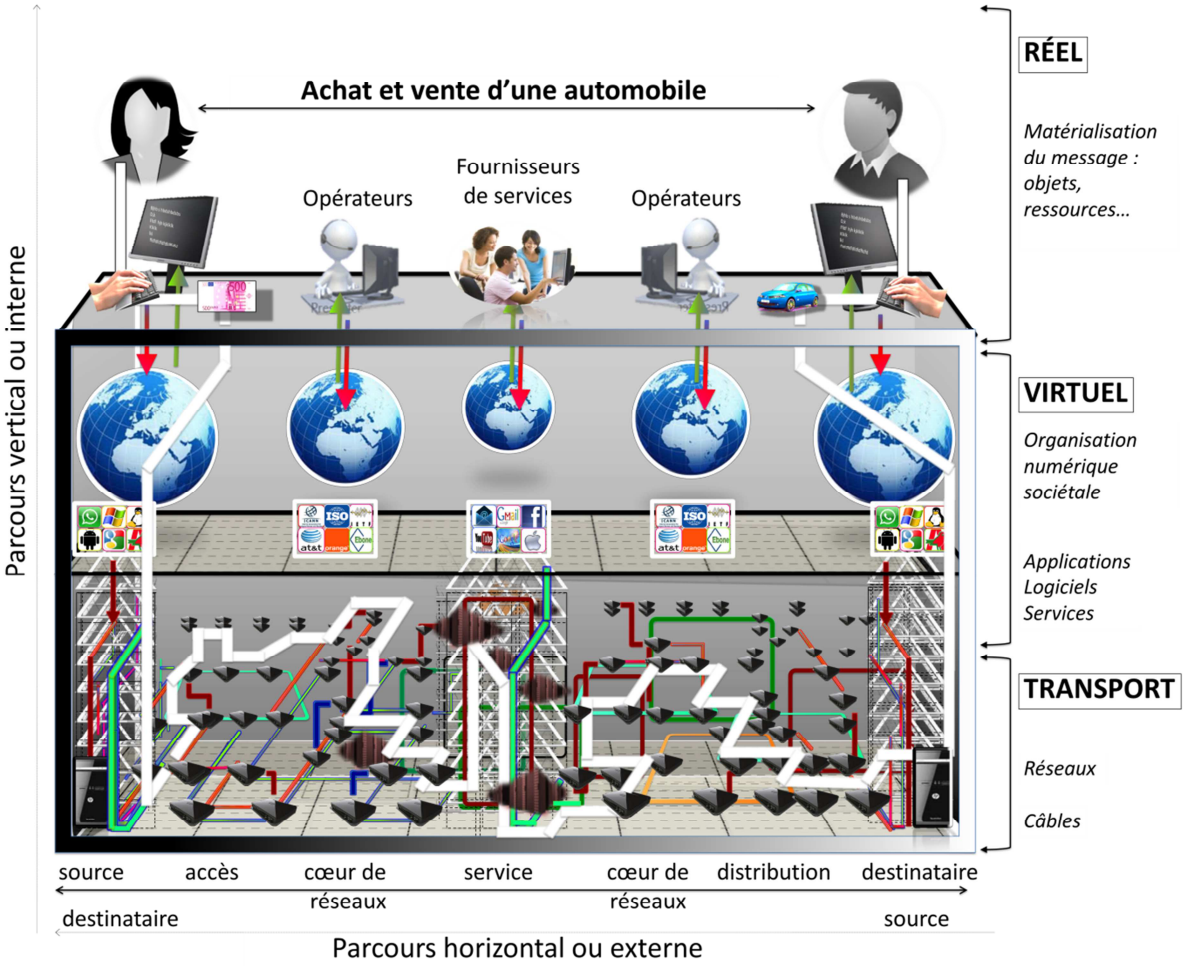


***Source** : OPECST*

Pour appréhender la complexité du numérique et éclairer les personnes pour lesquelles le numérique constitue une « boîte noire » située au-delà de l'interface familière (ordinateur, téléphone portable, etc.) à l'aide de laquelle chacun accède à l'Internet.

Afin de mieux comprendre cette « boîte noire » qu'est le numérique, il faut l'ouvrir, en proposer une représentation simplifiée. Le schéma ci-après représente les différents environnements d'un message électronique.

Schéma n° 14 : Ouvrir la « boîte noire » du numérique : représentation simplifiée des niveaux de l'échange numérique : réel, virtuel, transport



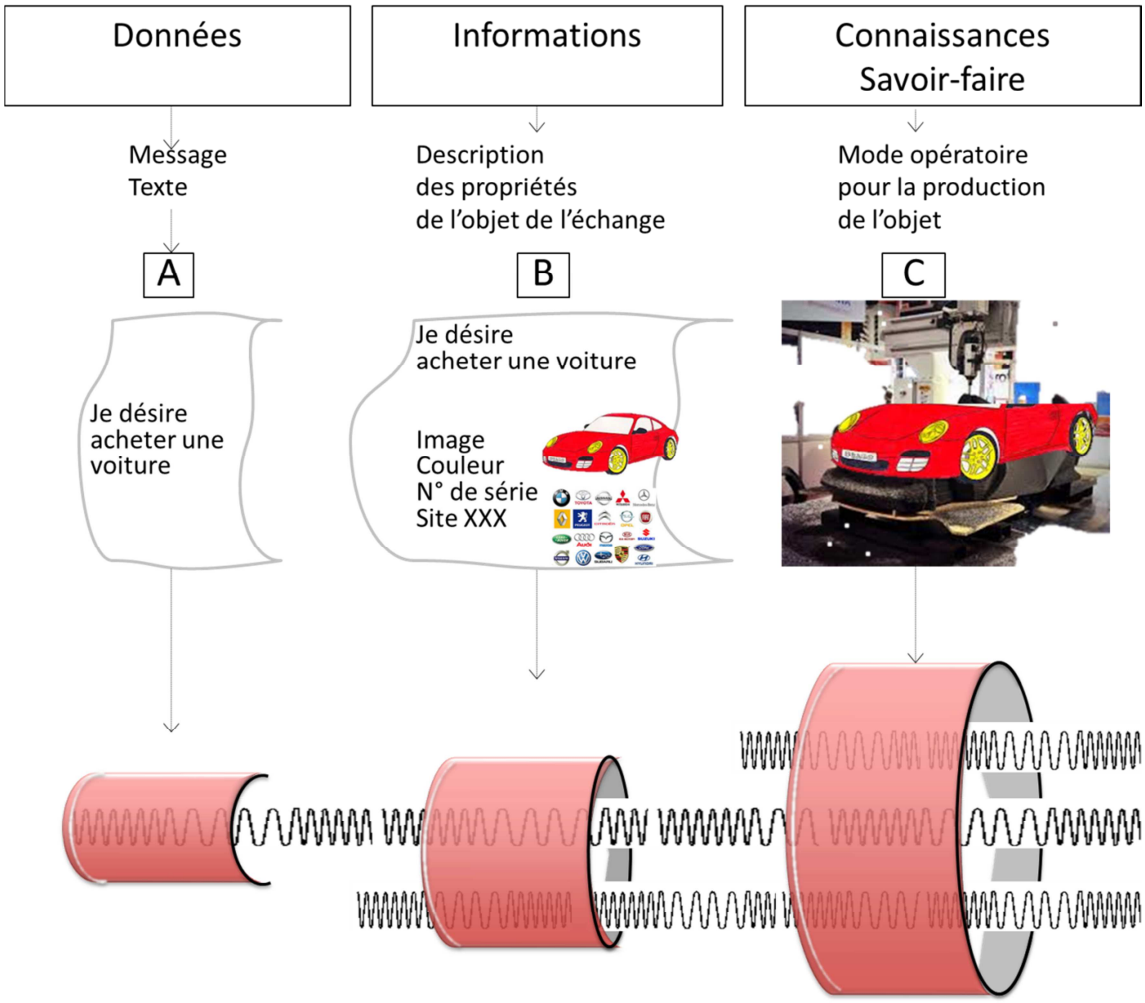
Source *: OPECST*

1. Le message comme objet de l'échange numérique

Lors d'un échange électronique, l'objet de l'échange est un message d'information émis par une source vers un destinataire.

Ces dernières décennies ont montré une évolution fulgurante de ce qui est échangé dans le monde du numérique : au cours des années **1980,** les messages étaient simples symbolisés par des **signaux** (représentés par A dans le schéma ci-après) ; depuis les années **1990,** les messages se sont enrichis d'**informations** pour décrire l'objet vendu, pouvant également y associer une image (B). Mais ces dernières années, avec l'apparition d'imprimantes 3D, ce sont des **connaissances** comme les **expériences** et maintenant, des **savoir-faire** (C) qui s'échangent *via* le réseau, des modes opératoires pour la fabrication d'objet.

Schéma n° 15 : Évolution du message électronique des années 1980 à 2015 : du signal au savoir-faire



Source *: OPECST*

« **L'information est devenue une matière première** à partir de laquelle on peut réaliser ce que l'on veut. Comme toute matière première, elle peut être protégée, vendue, raffinée, etc. De plus, **les acteurs économiques qui utilisent cette matière première le font de manière totalement dérégulée**. Ce qui n'est pas le cas de toutes les matières premières. »

Mme Claude Revel
Déléguée interministérielle à l'intelligence économique
27 mars 2014
Auditions Tome II du présent rapport

Les mêmes principes que pour l'échange humain, décrits précédemment, sont présents dans l'échange numérique : un processus « vertical » ou interne et « horizontal » ou externe.

2. Le processus « vertical » ou interne de production de message numérique

Comme déjà vu pour l'échange humain, le processus « vertical » ou interne produit un objet sous une forme adaptée au mode de transport, il s'agit, pour l'échange numérique, de **transformer le message en un signal numérique**. Lors de la réception de ce message, le parcours « vertical » inverse à celui effectué par l'émetteur sera suivi par le destinataire, qui pourra **retrouver le message d'origine à partir du signal numérique** en lui appliquant précisément les mêmes opérations.

Ces opérations particulières sont généralement désignées par le terme de protocole. **Un protocole assure l'interopérabilité entre les différents traitements nécessaires à l'échange**.

a) La matérialisation du message

Cette étape définit l'**existence du message en donnant le sens du message**, **ce dernier donne au message sa réalité et exprime la finalité de l'échange** : « vendre une automobile » qui correspond avant tout, pour chaque interlocuteur, à la mise en évidence d'un **besoin d'échanger**. Ce processus de matérialisation suppose également une **définition partagée** de **l'objectif** et des **modes d'échange**. Lors d'un échange numérique, plusieurs questions vont se poser quant au **choix du processus de virtualisation** qui devra, en outre, être connu au préalable des interlocuteurs.

b) La virtualisation du message

La virtualisation repose sur un ou plusieurs systèmes de référence en lien avec la finalité à atteindre. Ce processus part du message matérialisé pour l'adapter au **système de référence**. C'est le rôle des **applications** (courriel, service *web*, etc.) ou des **services numériques** ou même d'un **support physique** (*Wi-Fi* ou 3G).

La virtualisation définit également les **protocoles** à l'aide de **langages se devant d'être compréhensibles par tous**. Par exemple, un logiciel de traitement de texte est une application pour écrire un texte, compréhensible par d'autres logiciels de traitements de texte et les destinataires. De même, pour « vendre une automobile », l'application ou logiciel « vente » permet de virtualiser et traduire chaque action contribuant à la vente. La virtualisation doit également être **compatible** avec les contraintes du médium physique pour que le message puisse suivre le processus de conditionnement.

c) Le conditionnement du message

Le processus de conditionnement définit les propriétés que le message devra respecter pour son transport du fait des contraintes du

système de communication. Cette étape permet de produire un message transmissible par le canal physique.

Le passage du langage naturel au langage numérique s'accomplit par le **processus de codification**.

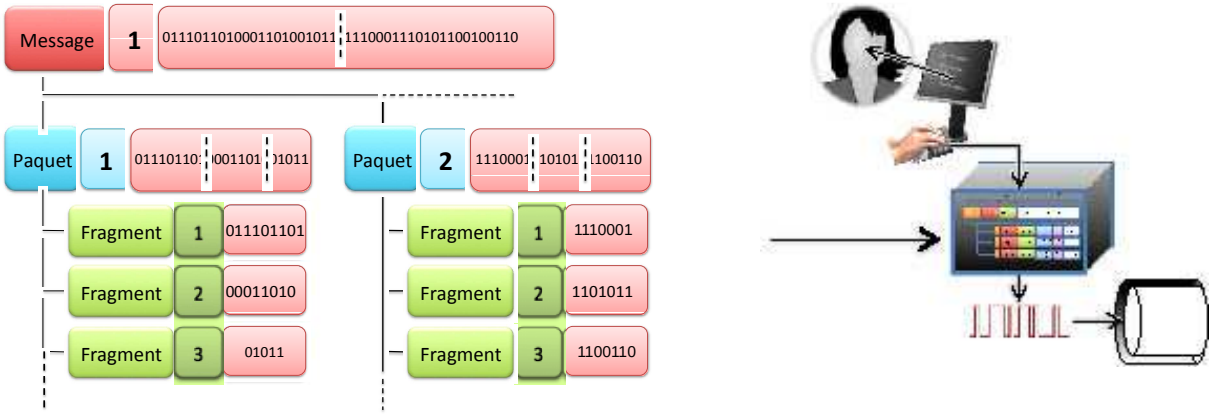
Tout d'abord, **le message initialement décrit en langage naturel est transformé en langage binaire, à savoir un code numérique (0,1) également appelé signal (0=pas de signal, 1=signal), le seul format compréhensible par les ordinateurs et les équipements de télécommunications**.

Pour être transporté, le message ne peut conserver son intégrité initiale, il doit être découpé en paquets et sous-découpé en fragments. Afin d'optimiser son passage dans les réseaux numériques, chaque fragment évoluera au travers d'un maillage de nœuds d'aiguillages. À l'image du courrier postal, afin que les paquets ne soient pas perdus et puissent être regroupés par le destinataire, **chaque paquet est mis sous enveloppe avec les adresses de l'émetteur et du destinataire ainsi qu'un numéro d'identification**.

> Dès 1971, avec le projet expérimental Cyclades, créé par M. Louis Pouzin, visant à mettre en place un réseau global de télécommunication celui-ci estimait : « ***J'avais idée d'envoyer des paquets de données sous forme de carte postale*** *: mettre une adresse, la déposer à la Poste, puis elle se débrouille pour arriver.* ***Que les cartes postales prennent le même chemin ou non, ça n'a pas d'importance. Qu'elles arrivent en séquence ou non, ça n'a pas d'importance.*** *Parce qu'il existe des protocoles, des règles de fonctionnement, qui permettent au récepteur de vérifier que tout est bien arrivé et de remettre les choses dans le bon ordre si nécessaire. C'était donc simple à faire ! Cette façon nous apportait aussi des garanties de bon fonctionnement :* ***s'il y avait des embouteillages dans le réseau, la carte passait par un autre chemin*** ».
>
> ***M. Louis Pouzin***
> ***Ingénieur en informatique***
> « Louis Pouzin : pionnier de l'Internet, sa vision de l'avenir »
> *Revue de la gendarmerie nationale, 4e trimestre 2013, p. 127*

Ensuite, les mécanismes de fragmentation du message doivent : ne pas endommager le message ; permettre sa recomposition ; permettre de véhiculer indépendamment chaque paquet ou fragment de paquet vers le destinataire adéquat tout en regroupant d'autres paquets appartenant à d'autres sources et/ou destinataires.

Schéma n° 16 : Découpage d'un message numérique en paquets et fragments en vue d'un échange numérique



***Source** : OPECST*

Depuis son origine, Internet propose une multitude de protocoles pour s'adapter aux différentes caractéristiques des médias et/ou des applications. **L'histoire d'Internet explique sa complexité du fait d'une succession de convergences technologiques** allant de la convergence des systèmes d'exploitation virtuels (*Java*) ou des protocoles réseaux (*IP* et *DNS*) à la convergence de la voix et des données, des câblages cuivre et fibre optique, etc.

3. Le processus « horizontal » ou externe de transport de message numérique

À l'image du mode d'échange multicanal de l'échange humain, le processus « horizontal » d'Internet distingue :

- **le canal logique** : des réseaux d'accès, de transport et de distribution pour acheminer les informations ;

- le **canal physique** : des câbles pour véhiculer le signal afin d'annihiler l'effet de la distance ;

- le **canal de contrôle** : **qui permet à chaque interlocuteur de contrôler son échange n'a été, à ce jour, que très faiblement structuré au sein du numérique**. Il en résulte que **la sécurisation des messages pendant leur transport repose sur les choix de l'émetteur et du destinataire**, qui, dans le meilleur des cas, établissent des conventions ou des usages avec **de faibles moyens pour les contrôler**.

a) Le canal logique de l'échange numérique

(1) Techniques de base pour la communication électronique

L'infrastructure Internet n'est pas un réseau « point à point » car, si une connexion devait s'établir jusqu'au domicile de chacun avec chacun, le

maillage en résultant serait trop complexe et trop coûteux au regard des presque trois milliards d'internautes actuels. Néanmoins, deux interlocuteurs peuvent souhaiter, ne serait-ce que pour préserver leur vie privée, établir un canal point à point réservé à leur espace de communication électronique.

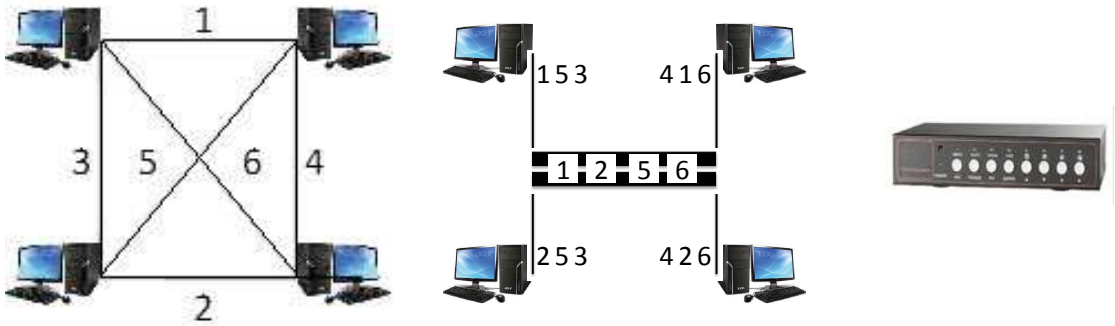
(2) Techniques de multiplexage pour la mutualisation des médias

À partir du concept utilisé posant qu'**il est possible de créer sur un même lien physique plusieurs voies logiques**, il est alors mis en application le **principe du multiplexage au niveau du signal**, par exemple, par la réservation de fréquences temporelles ou spatiales.

L'emploi de techniques de multiplexage permet cette optimisation. De chaque côté du média, se trouve un multiplexeur/démultiplexeur. Un tel équipement accueille en entrée du multiplexeur une grande quantité de systèmes terminaux. La capacité globale de transmission est ainsi divisée en sous-canaux dont la capacité dépend de la technique utilisée. Ces dernières sont de différents ordres.

Schéma n° 17 : Le multiplexage

Réseau maillé **Réseau multiplexé** **Multiplexeur**



***Source** : OPECST*

La mutualisation par le biais des multiplexeurs pose la question de la façon dont les paquets sont véhiculés au sein d'un réseau de grande dimension.

(a) Chaîne de liaison pour un canal logique « de bout en bout »

La liaison entre un utilisateur et un serveur *via* un réseau Internet forme une chaîne où les systèmes terminaux (*DTE*) sont reliés par des nœuds de communication (*DCE*). La nature des tronçons qui la compose peut être hétérogène selon l'opérateur qui fournit le service.

Pour rendre transparente, c'est-à-dire non perceptible, la distance entre la source et la destination, les messages sont relayés par le biais de différents équipements appelés des relais. De cette façon, **source et destinataire ont l'impression que les messages qu'ils échangent n'ont subi aucune transformation**. On représente cet échange à l'aide de schémas séquentiels.

(b) Fonction de commutation

Un commutateur assure la fonction de commutation qui permet de choisir, de nœud en nœud, un chemin. Un réseau commuté est composé de voies logiques pour assurer le transit des données et de commutateurs. Son rôle est d'envoyer les informations, qui arrivent sur une voie d'entrée, vers la voie de sortie.

Les types de commutation, les plus connues sont :

- La commutation de circuits : les terminaux établissent un circuit virtuel point à point, ils sont en mode connecté, par lequel **tous les échanges suivent le même chemin ; le réseau téléphonique** en est un exemple. Pendant la transmission entre les deux terminaux, le circuit virtuel est bloqué.

- La commutation de messages : **un message est associé à l'adresse du destinataire** et transmis au commutateur de proximité qui attend la réception de la totalité du message avant de le relayer. En cas d'erreur et de délai, la transmission est bloquée.

- La commutation de paquets : **un message est découpé en unités**, chacune associée à une adresse afin d'en permettre l'acheminement au travers du réseau étendu et d'un numéro afin d'en permettre sa reconstitution. **Les unités sont transmises par des chemins indépendants** *via* les commutateurs. Les paquets peuvent se perdre. **Le protocole *IP* suit ce principe**.

- La commutation de trames : la commutation de trames reprend la **commutation de paquets** sur circuits virtuels **mais n'assure pas le contrôle des erreurs**. *Frame Relay* utilise ce mode en offrant un service de liaisons virtuelles rapides (similaires au circuit virtuel), permanentes ou commutées.

- La commutation de cellules : une cellule est une petite unité de taille fixe (53 octets) qui a l'avantage de **supprimer tout contrôle sur les données** et de **n'exploiter que l'en-tête des cellules**. Les fonctions des commutateurs du réseau se réduisent à l'établissement des connexions et le routage. *ATM* (*Asynchronous Transfer Mode*) est un mode de transfert asynchrone pour la commutation de cellules. **Leur performance exceptionnelle a permis la mise en œuvre d'applications multimédias**.

- La commutation de label : née du routage *IP* et de la commutation de paquets pour **améliorer la vitesse de commutation** tout en incorporant des **services réseaux supplémentaires** comme la priorisation de flux. Le principe est d'insérer un **label placé en en-tête du message** afin que, très rapidement, le routeur puisse le lire et appliquer des règles de routage. Ces atouts en font actuellement **l'architecture de cœur de réseau la plus déployée par la majorité des opérateurs de télécommunications**.

Pour couvrir tous les points de la planète, les États se sont mobilisés en déployant sur leur territoire des réseaux câblés. Les zones non couvertes, ou zones blanches, l'ont été en moins de dix ans, offrant à chaque citoyen un accès au réseau.

Mais, en faisant cela, **les États ont confié leurs infrastructures à des opérateurs spécialisés, parfois étrangers**, et ont construit ce réseau par segment pour étaler les budgets parfois considérables.

(3) Techniques avancées pour l'échange de messages

Au travers d'un monde géographiquement étendu, le canal logique regroupe plusieurs fonctions :

- d'**adressage** pour la **distribution des paquets** ;

- d'**infrastructure globale** pour assurer une **distribution de « bout en bout »** ;

- de **routage** pour choisir des routes en fonction d'adresses.

(4) Système d'adressage

Chaque paquet est associé à une adresse *IP* source pour identifier la source à l'origine de l'émission du paquet **et à une adresse de destination** pour permettre aux systèmes intermédiaires de véhiculer les paquets au travers du réseau jusqu'à leurs destinataires. **Cela suppose qu'il existe un moyen unique d'identifier chaque entité susceptible d'émettre ou de recevoir un paquet.**

À l'image du courrier postal, le système à échelle mondial le plus efficace pour attribuer une adresse tout en assurant l'unicité se devait d'être **hiérarchique**. Par ailleurs, ce système d'adressage se devait d'être **codifié** afin de permettre sa transformation en binaire sur le média Internet.

Ce système hiérarchique s'est donc déployé de la manière suivante avec :

- un domaine d'adressage parent pour identifier un numéro de réseau comme un nom de ville dans un pays ;

- un domaine d'adressage enfant pour désigner un nœud dans le numéro du réseau comme une rue dans la ville.

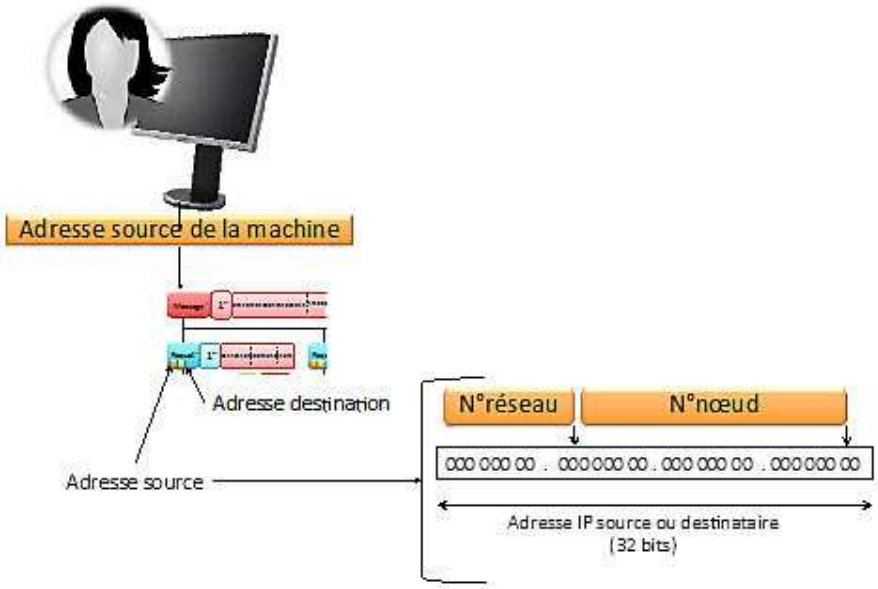
Le principe ci-dessous indique que **le nombre de numéros de réseau disponible dans le monde peut devenir saturé**. En calculant le nombre maximum de réseaux possibles sur 24 bits (0 ou 1), on atteint 16 777 216 réseaux. En rapprochant ce chiffre des trois milliards d'internautes, apparaît évidente **la nécessité du nouvel adressage *IPv6*** qui permet des adresses sur 256 bits et sur un niveau hiérarchique supplémentaire.

Néanmoins, **deux autres techniques** permettent d'étendre le nombre des adresses de réseau :

- la technique du *CIDR* (*Classless Inter Domain Routing*) considéré comme **un préfixe qui préciserait le « pays » de l'adresse *IP*** ;

- et la technique du masque de sous-réseau considéré comme **un suffixe qui préciserait « l'immeuble » dans la rue**.

Schéma n° 18 : Principe de l'adresse *IPv4* d'une machine (ordinateur, mobile, etc.) sur un réseau *IP* Internet



***Source** : OPECST*

Afin de simplifier la notation, on représente communément une adresse *IP* par quatre chiffres séparés par un point : 1.2.3.4.

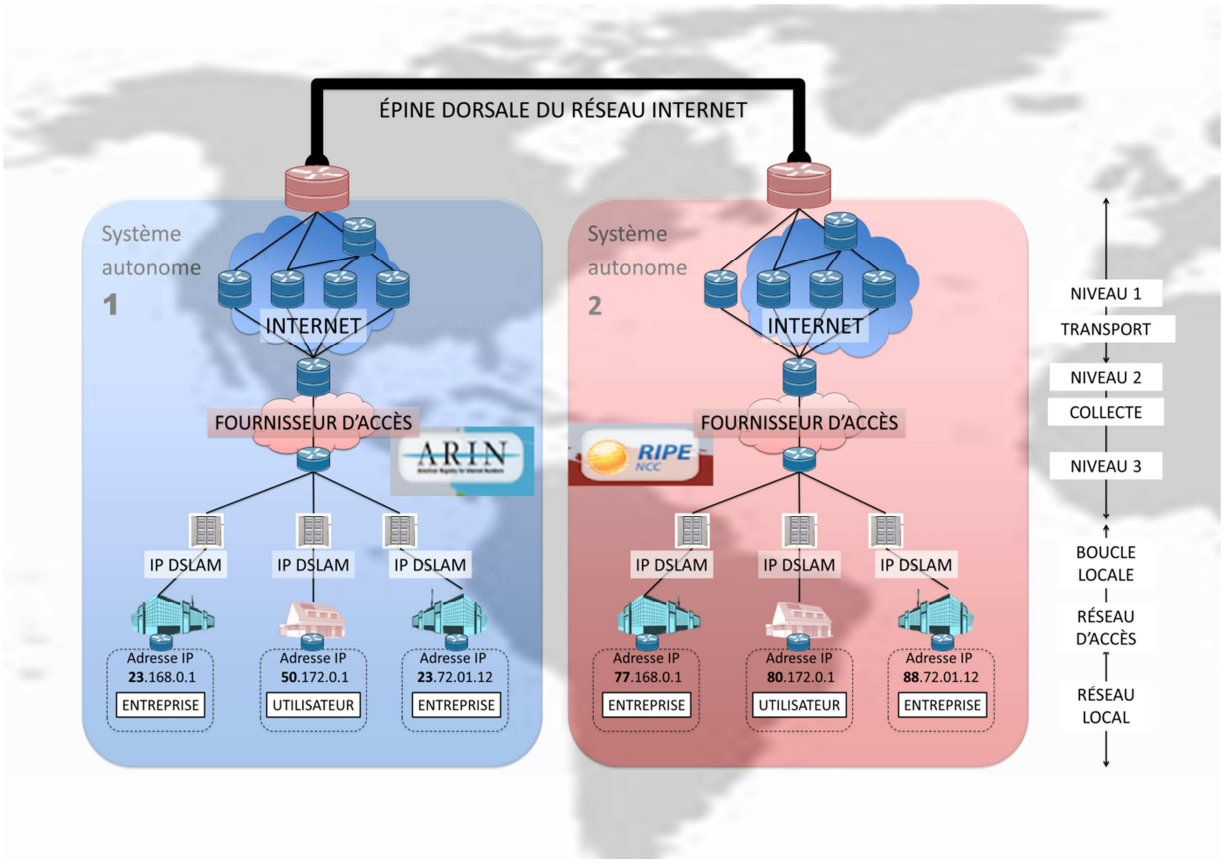
(5) Infrastructure globale

Le conditionnement permet de préparer le message pour son transport en le découpant et en l'étiquetant avec une adresse *IP*, ces deux éléments jouant un rôle majeur lors du parcours horizontal ou externe.

L'Internet repose sur **une infrastructure globale faite d'échangeurs** (à l'image d'un réseau routier) reliés entre eux par des routes (liens). Comme le représente le schéma ci-après, chaque maison, quartier, ville, pays, continent, est associé à une adresse *IP*.

Afin d'assurer l'unicité de l'adresse de chaque site, un découpage hiérarchique est proposé au niveau mondial. Par exemple, les zones bleue et rose du schéma ci-après contiennent des milliards de réseaux ; trois réseaux sont représentés par zone, ici, dans la zone bleue trois adresses sont mentionnées : « entreprise 1 – 23.168.0.0 » « utilisateur – 50.172.0.0 » « entreprise 2 – 23.172.1.0 ».

Schéma n° 19 : Vue partielle de deux réseaux Internet

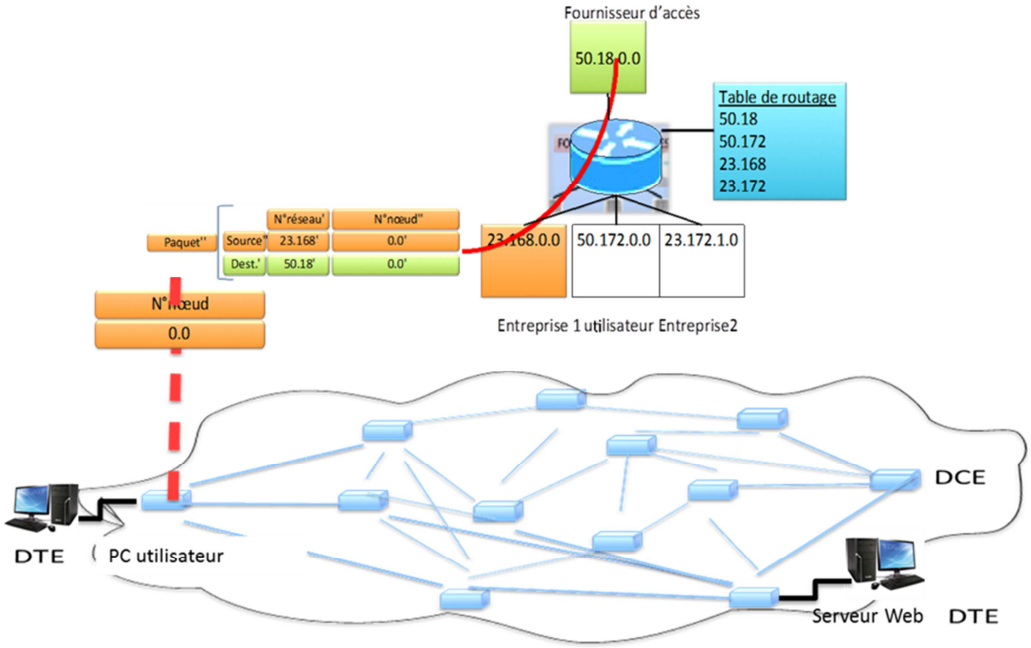


***Source** : OPECST*

(6) Routage

C'est à partir de l'adresse de destination que les relais ou systèmes intermédiaires vont décider de la route que le paquet empruntera.

Schéma n° 20 : Principe du routage au niveau d'un routeur



***Source** : OPECST*

Chaque échangeur dispose d'un mécanisme automatique capable de lire, pour chaque paquet, les adresses de destination puis de mettre celui-ci sur la bonne route en fonction de cette adresse ; c'est pour cette raison que ces équipements sont appelés des routeurs.

Dans le schéma ci-dessus, l'adresse de destination (verte) avec l'adresse source (orange) est émise au moment du conditionnement du paquet dans l'entreprise 1. Le routeur (en bleu) possède des tables de routage qui lui indiquent les destinations possibles.

Puis, le paquet est transmis de routeur en routeur jusqu'à atteindre son destinataire, l'entreprise 2.

Chaque routeur décide de transférer le message au routeur suivant à l'aide de l'**adresse de destination** et de la **connaissance de la topologie du réseau** dont il fait partie. **Il existe plusieurs dizaines de milliers de routeurs sur l'Internet**, un message adressé, par exemple, à *Google* (*www.google.fr*) sera en moyenne relayé par une vingtaine de routeurs. **À chaque seconde, un routeur relaie plusieurs centaines de paquets**.

b) Le canal physique de l'échange numérique

Dès la fin du processus de codification du message par le canal logique en un signal électrique, celui-ci est transporté sous cette forme sur le canal physique.

L'objectif des réseaux d'interconnexion à l'échelle planétaire comme l'Internet ou la téléphonie mobile est d'en permettre l'accès et la distribution à chaque citoyen. Dans la majorité des pays, la distribution s'accomplit selon un principe d'équité.

Comme déjà indiqué, l'infrastructure Internet n'étant pas un réseau « point à point », le principe pour relier l'ensemble de la planète a donc été de fournir deux types de réseau correspondant à deux modes de distribution :

- l'un, plutôt robuste, pour couvrir de grandes distances : le cœur de réseau :

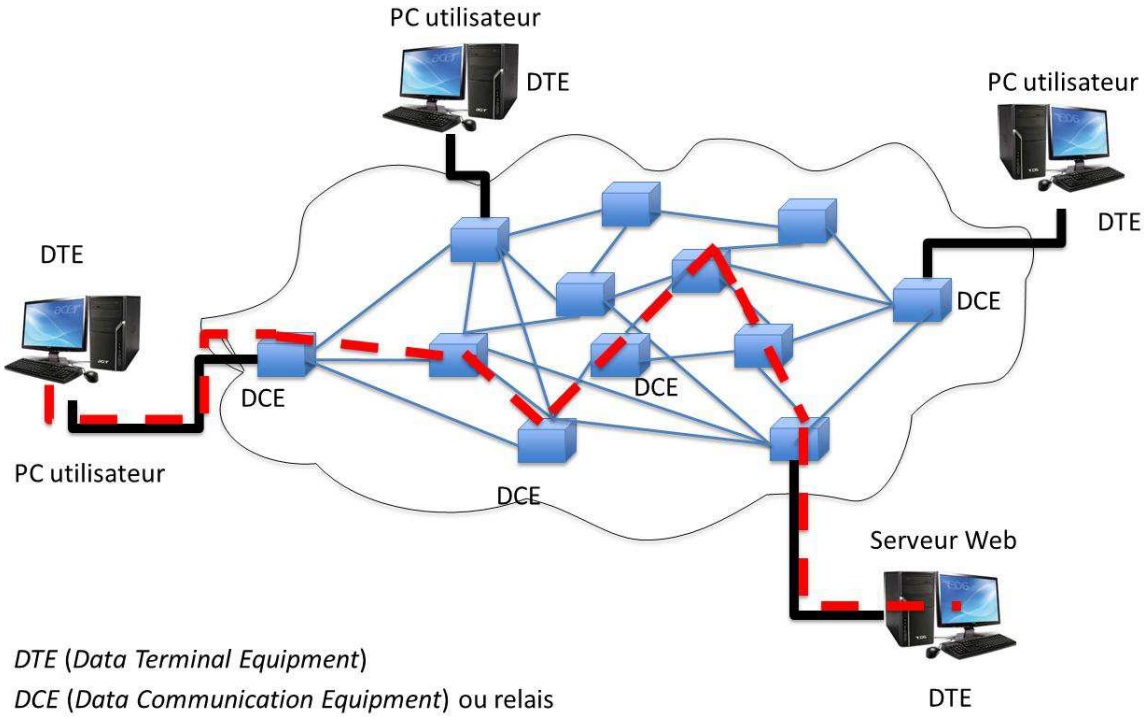
- et l'autre, plus ramifié, pour assurer la connexion réseau jusqu'au domicile de tout abonné.

(1) Principe de base d'une chaîne de liaison

L'étendue d'un réseau se mesure au moyen de la nature du média et de la distance entre les points les plus éloignés qu'il relie. On distingue les réseaux reliant deux nœuds distants selon leur échelle planétaire (*Wide Area Network*), leur échelle régionale (*Metropolitan Area Network*), ou encore au niveau de l'entreprise (*Local Area Network*), ou d'un individu (*Personal Area Network*).

La liaison entre un utilisateur et un serveur *via* un réseau Internet forme une chaîne où les systèmes terminaux *Data Terminal Equipment* (*DTE*) sont reliés par des nœuds de communication *Data Communication Equipment* (*DCE*). La nature des tronçons qui composent ces réseaux peut être hétérogène selon l'opérateur qui fournit le service. Le lien figuré en pointillé dans le schéma ci-après est généralement appelé un circuit.

Schéma n° 21 : Représentation d'une chaîne de liaison ou circuit (en pointillé)



***Source** : OPECST*

(2) Le cœur de réseau

Le cœur de réseau repose sur une **structure réticulaire** composée de nœuds et de liens. La première contrainte de cette structure est la **couverture physique des territoires** et la seconde contrainte est la capacité de **mutualiser un très grand nombre de communications sur un même lien**.

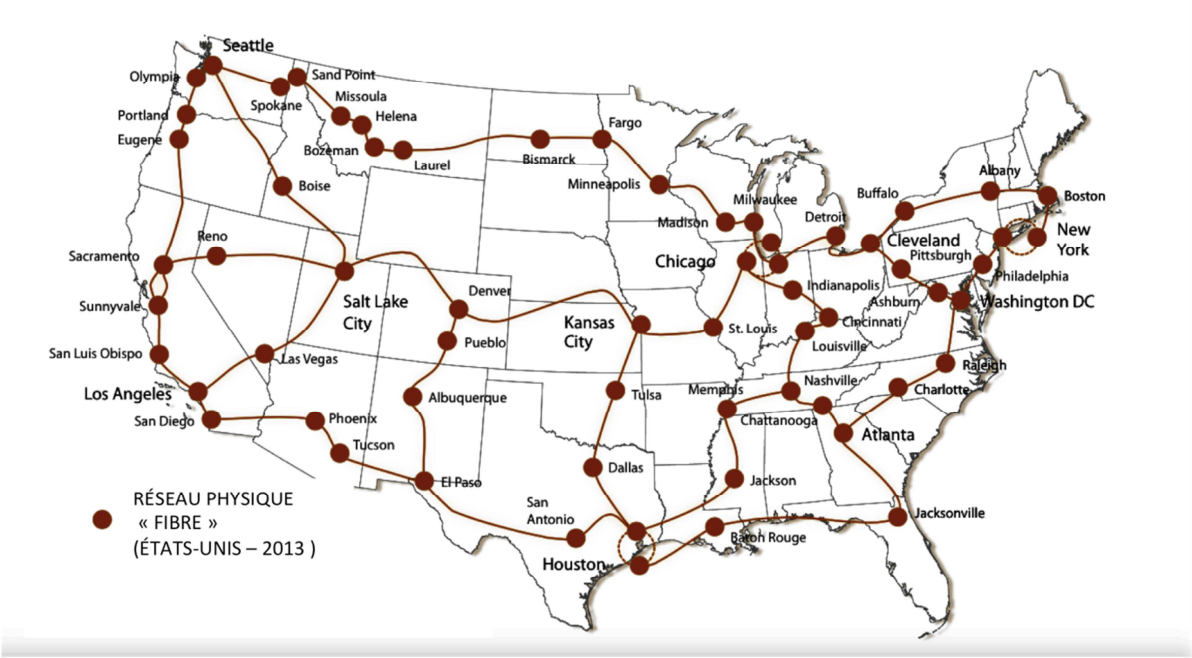
(3) L'étendue physique des réseaux

Les réseaux physiques sont de nature filaire ou aérienne. Leur déploiement assure la transmission d'éléments binaires entre deux équipements en mode point à point ou entre plusieurs équipements en mode multipoint où les terminaux sont connectés sur un même lien physique.

La structure des réseaux physiques impose une limitation des débits qui se mesure en bit/s (signal/s), on évoque alors le terme de **bande passante.** Les débits des réseaux sont au cœur des problématiques puisque, pendant longtemps, les limites physiques liées aux médias ont bridé le développement d'applications nécessitant de grandes quantités de bande passante comme la vidéo ou l'image en général.

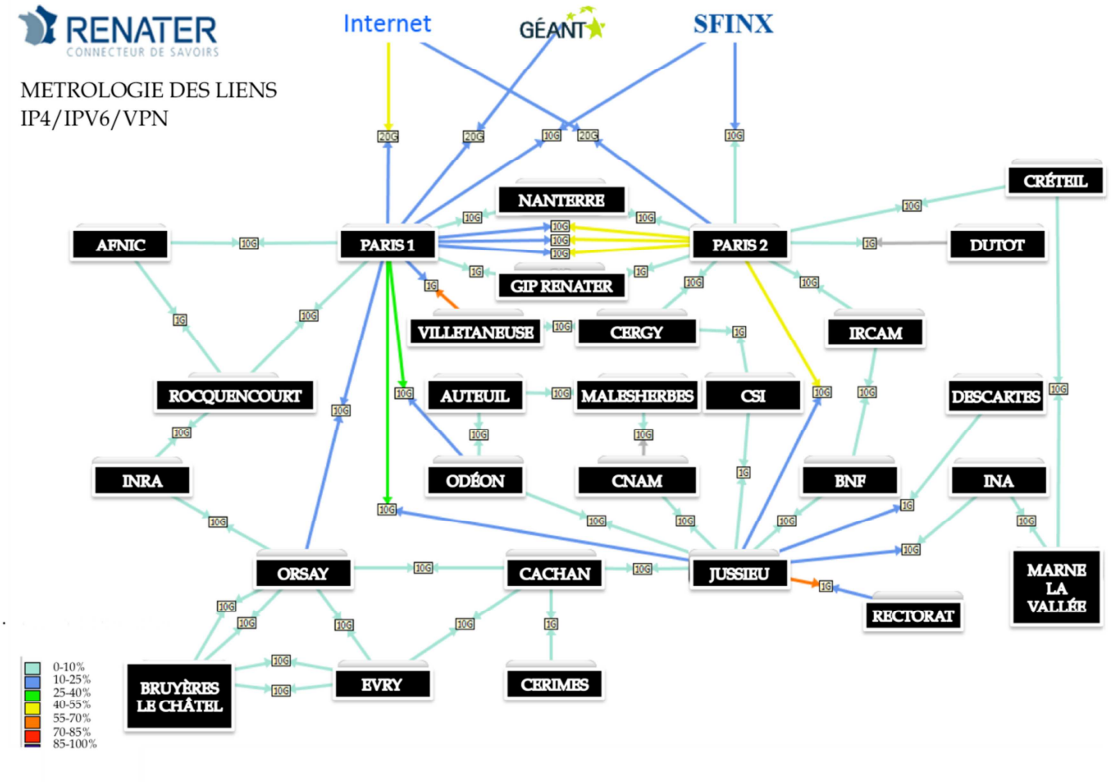
Le médium physique peut être un câble physiquement défini, comme le cuivre, le coaxial ou encore la fibre optique mais peut également être **l'air** comme le réseau hertzien, la radio ou le satellite.

Schéma n° 22 : Épine dorsale de l'Internet aux États-Unis d'Amérique



Source *: http://www.internet2.edu/media/medialibrary/2013/05/20/IS-advanced-layer-1-service.pdf*

Schéma n° 23 : Déploiement du cœur de réseau de l'Internet en Ile-de-France



***Source** : RENATER*

À l'heure actuelle, **la fibre optique constitue la technique la plus utilisée du fait de sa performance, tant pour les cœurs de réseaux que pour les réseaux d'accès**. Les réseaux de transport optique des cœurs de réseaux des opérateurs déploient des répéteurs ayant une capacité de l'ordre de 20 térabit/s par fibre.

(a) Réseaux mobiles

Les technologies des réseaux sans fil ou mobiles sont le fruit d'une histoire au cours de laquelle des choix d'architectures ont été effectués selon les pays, les services attendus ou encore les technologies disponibles.

- **2G** : le *Global System For Mobile (GSM)* proposait un débit d'environ 10kb/s ;

- **2.5G** : *General Packet Radio Service (GPRS)* a un débit de 128 kb/s ;

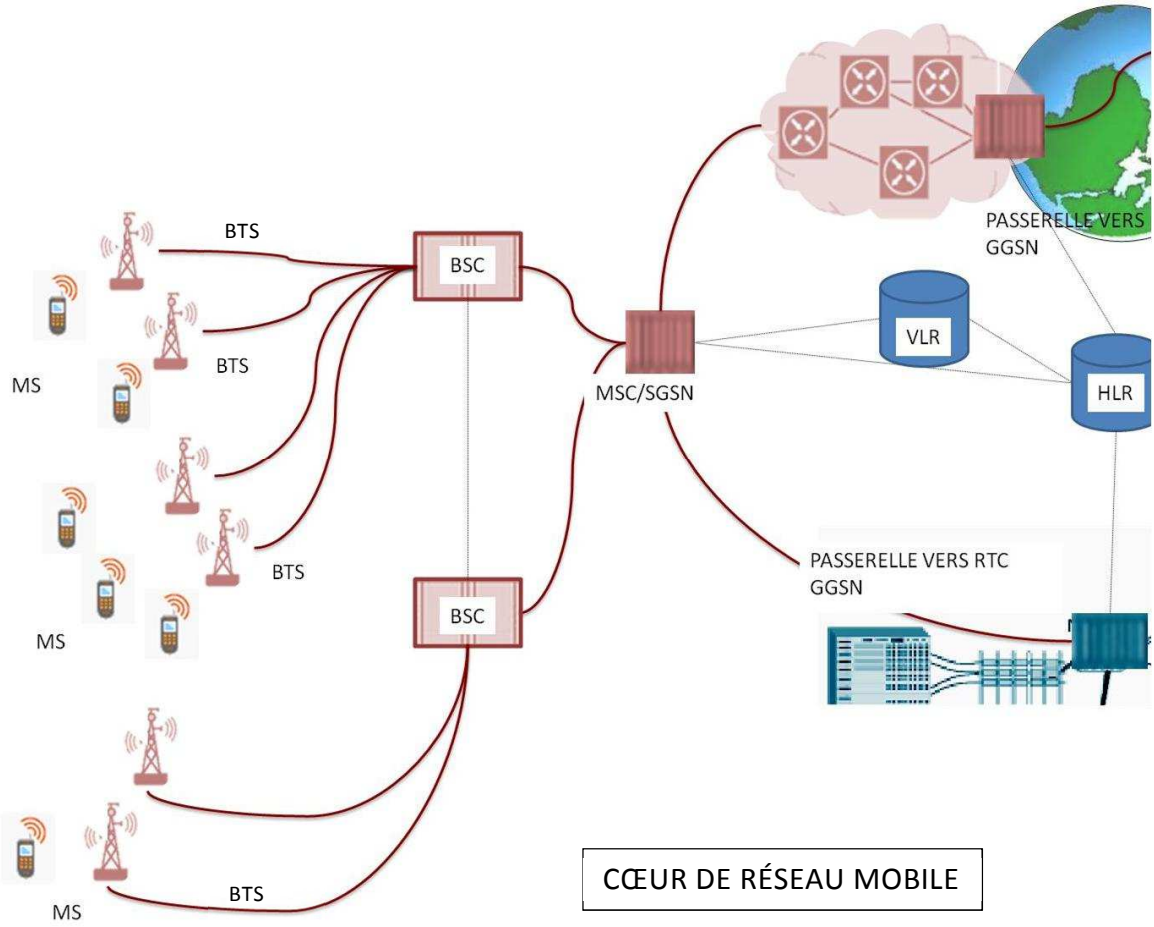
- **3G** : *Universal Mobile Telecom System (UMTS)* a un débit de 384 kb/s à 2mb/s.

À l'heure actuelle, **la convergence de ces différentes architectures est en pleine accélération** afin de faciliter les accès aux ressources (*VoIP, ToIP*, Internet, etc.) mais également leur gestion.

Les réseaux 3G et, plus récemment, 4G offrent des services qui rendent les terminaux mobiles aussi bien reliés que les ordinateurs portables ou de bureau. Les efforts pour parvenir à ce résultat ont porté sur le cœur de réseau.

Un réseau mobile est un réseau en architecture 2/3 composé d'un réseau d'accès et d'un cœur de réseau. Afin de fournir aux usagers des moyens de communications fluides et agiles, leur réseau d'extrémité est constitué d'une multitude de réseaux sans fil comme le montre le schéma ci-après.

Schéma n° 24 : L'exemple d'un réseau 3G



Source *: OPECST*

Le réseau d'accès propose en son point d'extrémité une base d'accès appelée *BTS*, pour émettre ou recevoir le signal radio entre le terminal et elle. Les *BTS* d'une même zone géographique dépendent d'un contrôleur (*BSC*) autorisant l'accès à la passerelle *MSC/SGSN*. Son rôle sera de permettre l'interconnexion avec les bases de données des utilisateurs afin de gérer leurs autorisations et leur authentification *via* leur identité (leur carte *SIM*).

On distingue deux types de bases : celui qui détient les identifiants des usagers sur leur réseau d'origine (*Home LR*), celui qui détient les identifiants des usagers sur leurs réseaux de visite (*Visited LR*).

Le cœur de réseau permet de relayer les messages mais également de fournir des passerelles d'interconnexion avec le réseau téléphonique public (*RTC*) afin de contacter des postes de téléphonie analogique **et avec le réseau Internet** afin de contacter d'autres terminaux *GPRS* ou *ToIP/VoIP*.

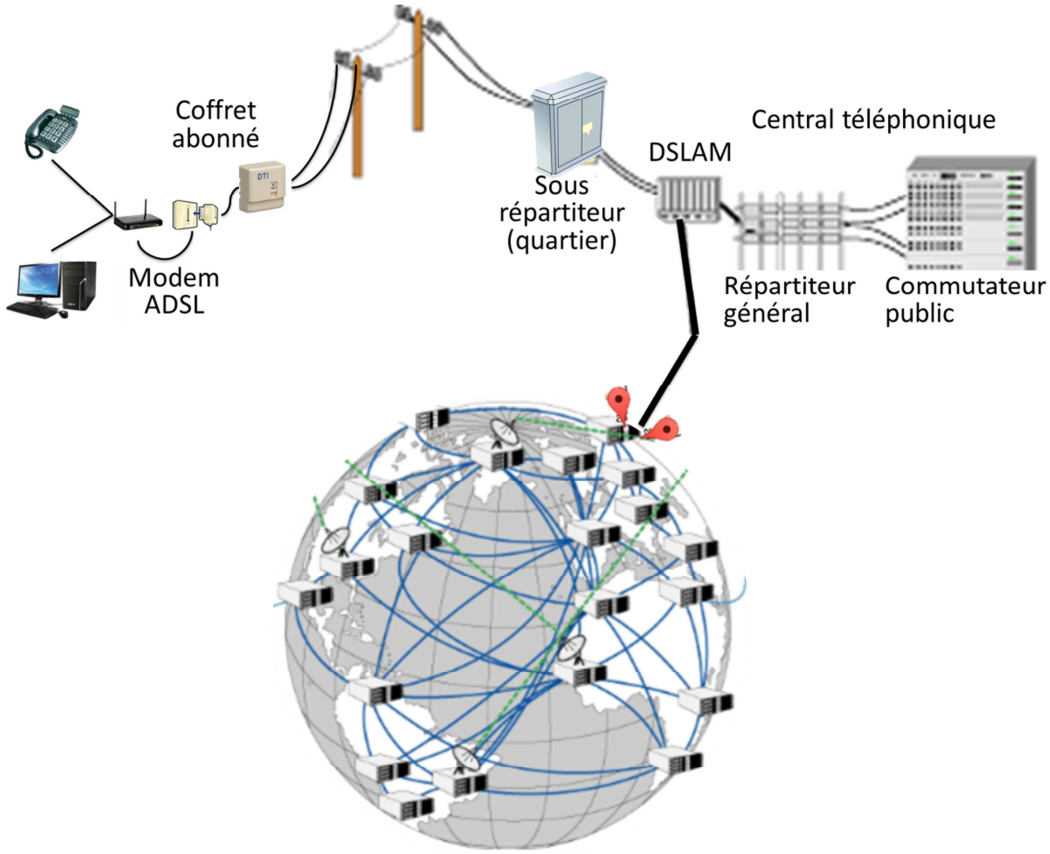
(b) Les réseaux d'accès

Le réseau d'accès, également appelé boucle locale, désigne l'ensemble des liaisons et équipements qui permettent de **relier les installations d'abonnés au réseau de transport**.

Comme le présente le schéma ci-après, le réseau d'accès permet la collecte et la distribution des trafics d'abonnés. La paire de cuivre peut servir de support au trafic vocal et au trafic de données grâce à l'emploi des techniques numériques. D'autres supports peuvent être employés ou combinés ensemble (fibre optique, voie radioélectrique, coaxial, etc.) pour desservir les entreprises ou les domiciles résidentiels en débits numériques à des conditions économiques variables.

Avec le schéma directeur territorial d'aménagement numérique, il est prévu que le déploiement de la fibre à l'abonné permette de déployer la fibre à la maison (*FTTH*) pour tous les territoires, au cours des dix prochaines années, en traitant en priorité les principales zones dites grises, c'est-à-dire en améliorant les débits des accès inférieurs à 2 Mbits.

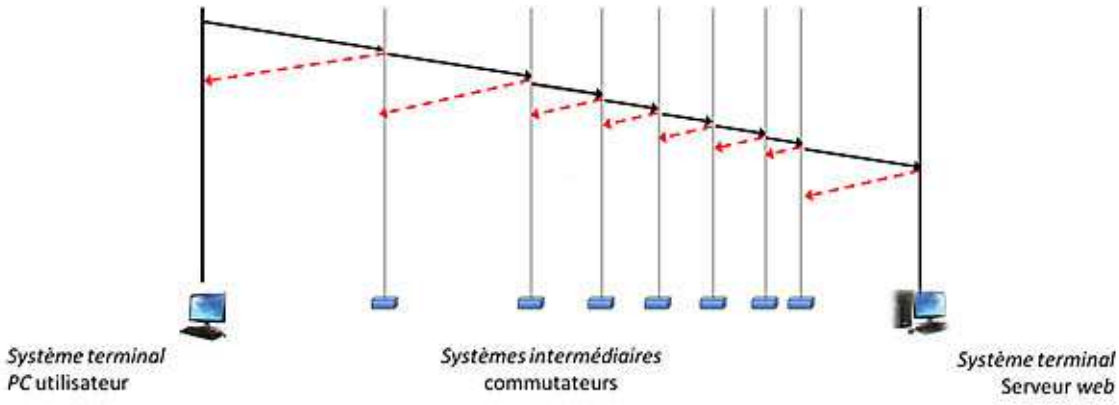
Schéma n° 25 : Réseau d'accès et réseau de transport



Source *: OPECST*

c) Le canal de contrôle de l'échange

Schéma n° 26 : Contrôle de l'échange d'un message entre la source et son destinataire au moyen d'un contrôle sur le message



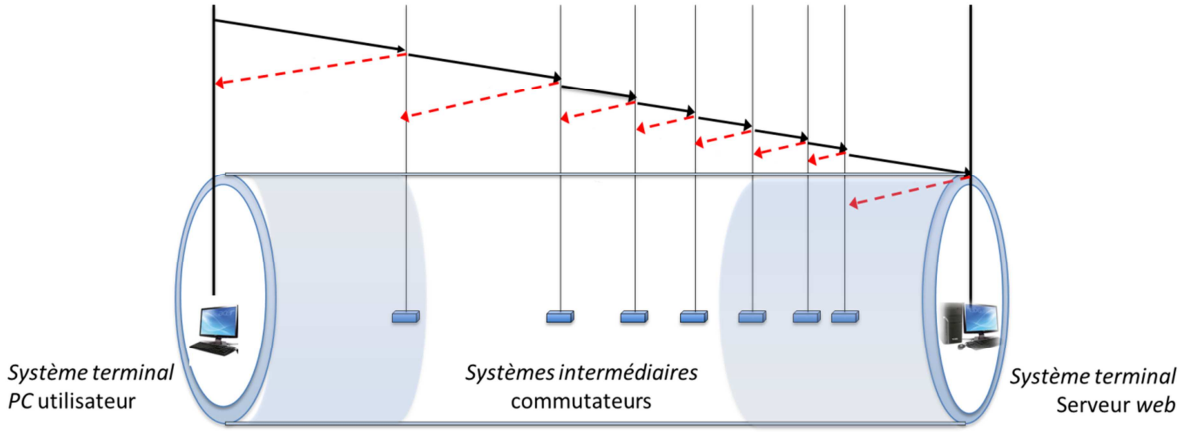
Source *: OPECST*

Lors d'une communication électronique, les protocoles vont permettre à chaque système d'engager, maintenir et terminer sa relation avec son interlocuteur. Il s'établit entre eux **une boucle de contrôle** semblable à la boucle de rétroaction des systèmes.

Lorsqu'une source émet une information, même binaire, elle contrôle l'action d'émission qu'elle a formulée. Il existe deux mécanismes de contrôle : soit sur le message lui-même soit sur le canal.

Dans ce second cas, le protocole met en place des messages affectés au contrôle des autres messages (en pointillés sur le schéma ci-après).

Schéma n° 27 : Contrôle de l'échange d'un message entre la source et son destinataire au moyen d'un contrôle sur le canal



***Source** : OPECST*

d) Maintien d'une connexion TCP/IP

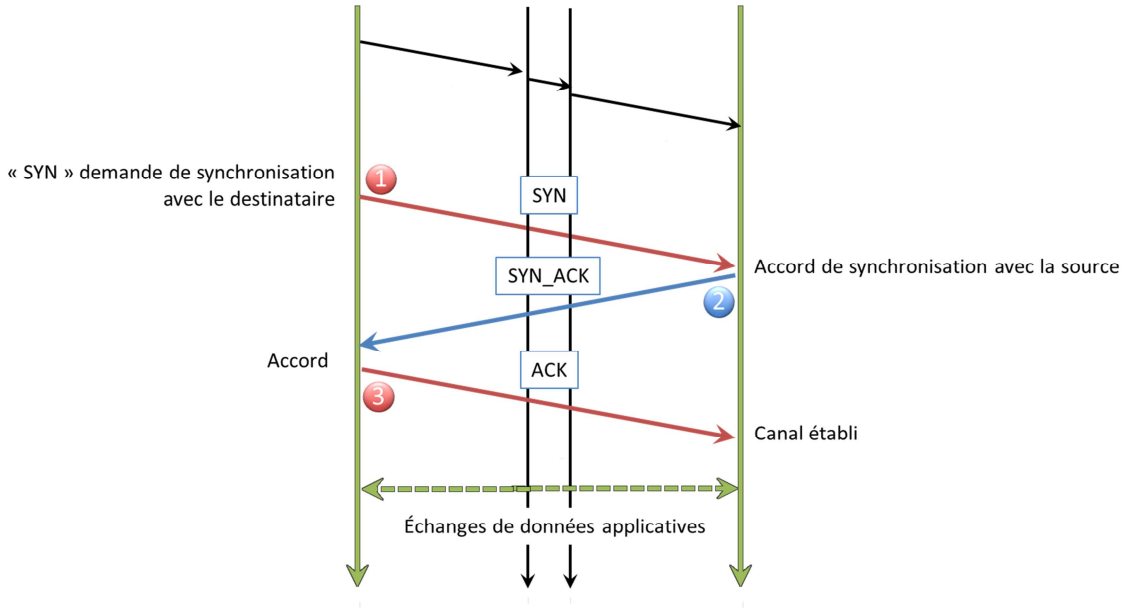
Le maintien de la connexion *TCP/IP* constitue un principe fondamental des réseaux étendus. C'est une application du principe précédent où deux interlocuteurs (un client et un serveur numérique) établissent un canal logique.

La connexion est initialisée, maintenue puis rompue en temps quasi réel au cours de la communication entre une source et son destinataire.

Le schéma ci-après montre la phase d'initialisation qui se déroule en **trois échanges, à l'image d'une poignée de main** (« *Bonjour* », « *Bonjour* », suivis du geste familier)**. Les routes ont été déterminées au préalable en fonction des adresses *IP*. Ensuite la connexion *TCP* s'établit.**

Cette connexion constitue un socle solide pour que des applications puissent fonctionner sur un canal homogène en toute transparence de la granularité du réseau physique, du cœur de réseau ou d'accès.

Schéma n° 28 : « Poignée de main » numérique, scellant un accord pour l'initialisation d'une session *TCP/IP*



***Source** : OPECST*

II. LES INFRASTRUCTURES DU NUMÉRIQUE

À l'image du niveau virtuel des échanges humains, l'échange numérique présente une structure globale.

A. INFRASTRUCTURES DE SERVICES MUTUALISÉS POUR LES ÉCHANGES NUMÉRIQUES

1. Infrastructure de noms de domaine (*DNS*)

C'est l'évolution croissante de systèmes à configurer puis à tenir à jour qui a suscité la mise à disposition d'un service centralisé, le *DNS*. L'infrastructure *DNS* est quasi publique, fédérée à destination des usagers de l'Internet par des institutions ou des gouvernements.

L'infrastructure globale repose sur une architecture client/serveur numérique au sein de laquelle les serveurs sont organisés de façon hiérarchique.

Le nommage consiste à juxtaposer le nom de la ressource représentant chaque niveau de la hiérarchie, le plus bas dans la hiérarchie.

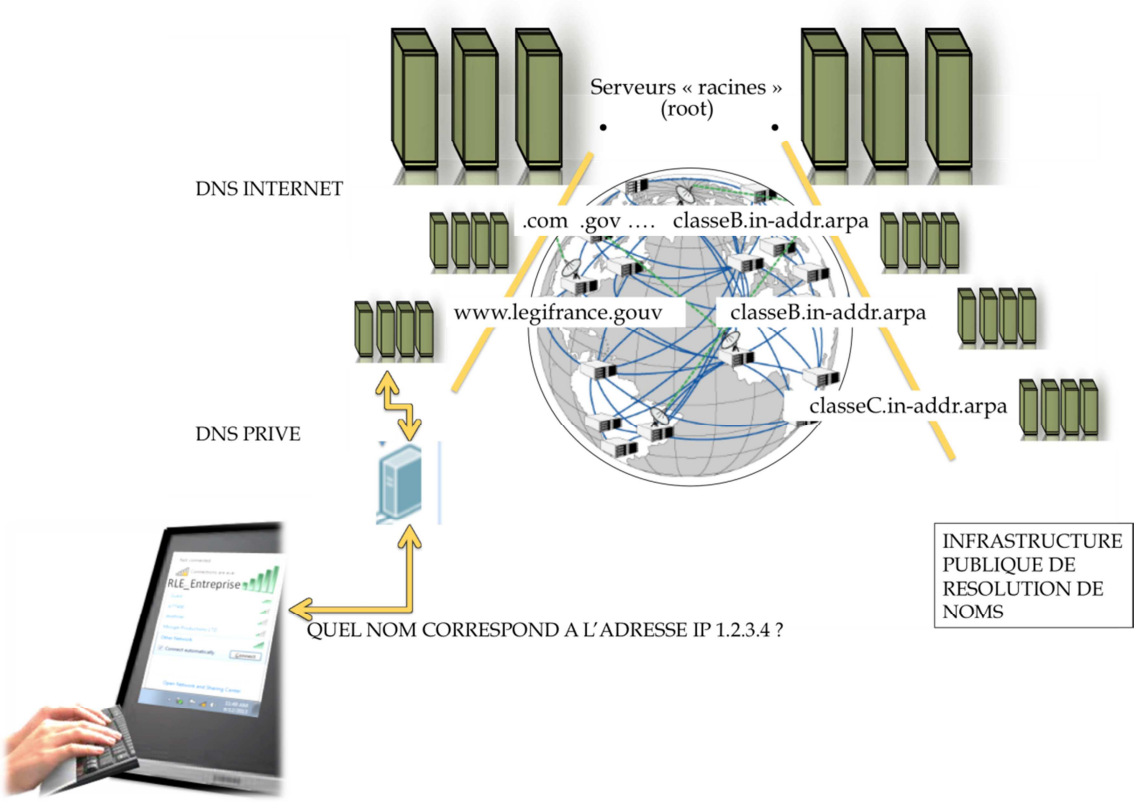
Le principe général est que le client émet une requête vers un serveur de proximité afin d'obtenir le nom de domaine résultant de la résolution, des serveurs enfants aux serveurs racines ou *root*. Ces derniers

constituent en quelque sorte la charpente du *DNS* mondial, ils sont au nombre de treize environ, hébergés aux États-Unis d'Amérique et sous le contrôle de l'*Internet Assigned Numbers Authority* (*IANA*).

Sur le plan opérationnel, le *DNS* permet à la fois une fonction technique pour communiquer entre domaines et serveurs interconnectés *via* des requêtes et une fonction indirectement commerciale grâce aux fonctions de recherche et priorisation d'un site sur le nom de domaine.

L'infrastructure de noms de domaine ou *Domain Name System* (*DNS*) permet la conversion d'une adresse *IP* en nom ou domaine et inversement. Étant donné qu'il est plus aisé de saisir des adresses de noms comme « www.france.gouv » que des adresses de nombres comme une adresse *IP* « 1.2.3.4 », une première étape a consisté à **configurer sur chaque poste de travail une association *IP*/nom de domaine**.

Schéma n° 29 : Infrastructure de noms de domaine (*DNS*)



***Source** : OPECST*

Le DNS s'est transformé en un modèle d'affaire pour certains acteurs qui, dans le but d'une revente spéculative, se sont mis à acquérir des noms de domaine d'entreprises de réputation élevée.

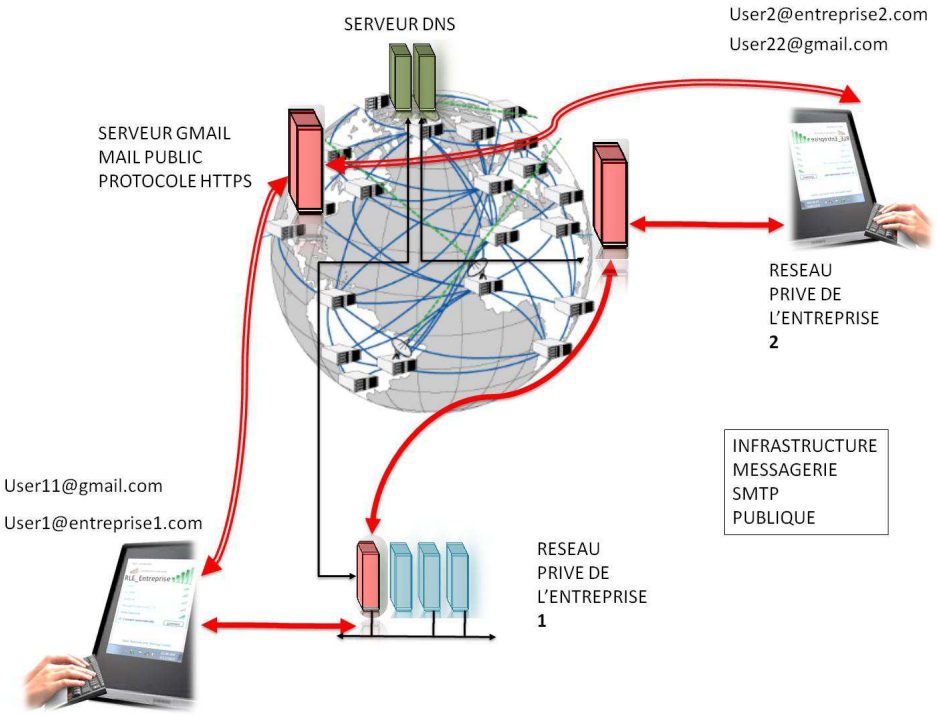
> « Le fait que les noms de domaines soient attribués par une association américaine ne pose pas de problème particulier à *Total*. Les domaines intéressants ont été réservés : le Total.com, le total. »
>
> ***M. Patrick Hereng***
> ***Directeur des systèmes d'information et télécommunications, Total***
> *6 mars 2014*
> *Auditions. Tome II du présent rapport*

2. Infrastructure de routage et de messagerie

La messagerie électronique permet de véhiculer des courriers à partir de services mutualisés ou/et privés en apportant un certain nombre de fonctions tirées de celles proposées par le courrier postal : accusé de réception, etc. Les avantages sont l'accélération dans les modes de communications et, par là-même, dans les cycles de décision.

L'infrastructure de messagerie est une architecture client/serveur numérique composée, d'une part, d'un réseau d'accès et, d'autre part, d'une infrastructure affectée au routage des messages.

Schéma n° 30 : Infrastructure de messagerie



Source *: OPECST*

3. Infrastructure de navigation : les moteurs de recherche

Le principe d'information est le principe fondamental de l'Internet où l'outil incontournable pour l'usager est la recherche et la classification de l'information.

L'infrastructure du *web* repose sur trois éléments :

- **le robot** également appelé *crowler* ou *spider* qui collecte toutes les pages ;

- **l'index** qui renferme tous les mots de toutes les pages collectées par le robot, puis, qui le relie aux *URLs* des pages dont ils proviennent, repérées à l'aide des noms de domaines *DNS* ;

- **l'interface** pour émettre la requête et en recevoir les résultats.

L'infrastructure du *web* repose sur une architecture client/serveur où le navigateur *web* est client et **les serveurs *web* sont de deux types** : **le serveur de contenu** qui détient l'information et la rend disponible et **le serveur de recherche** qui détient l'index général avec l'algorithme de classement des réponses.

- Le serveur de recherche

Le processus d'une recherche numérique se déroule en sept étapes :

1) l'usager lance une requête ;

2) le moteur de recherche interroge l'index à l'aide des mots de la requête ;

3) l'index pointe les pages qui contiennent les mots-clés ;

4) l'index classe les pages dans un ordre déterminé par un algorithme spécifique : *Search Engine Result Pages* (*SERP*) ;

5) l'index prépare la liste de réponses : titre, extrait, *URL*, et la transmet à l'usager grâce aux protocoles *HTTP* et *HTTPS* ;

6) l'usager clique sur le « titre » de la page et se connecte sur le site concerné ;

7) **l'index apprend le lien entre la requête initiale et la réponse choisie à l'étape 6, ci-dessus, pour améliorer la pertinence de la prochaine recherche**.

- La description de la connaissance

Pour décrire une connaissance, le langage *HyperText Markup Language* (*HTML*) :

- décompose la connaissance diffusée **en pages de contenu** : la page *HTML* est l'entité élémentaire localisée et identifiée de façon unique par son *URL* ;

- relie les pages *HTML* entre elles : un peu comme le principe du « fil d'Ariane », **la connaissance est structurée en réseau**.

Une fois l'information trouvée sur une page principale, l'index et les liens suivis vont conduire l'usager vers une information de plus en plus précise.

Les protocoles *HyperText Transfer Protocol* (*HTTP*) et *HyperText Transfer Protocol Secure* (*HTTPS*) sont les protocoles pour transporter les liens et pages au sein de l'architecture *web*.

Cette capacité repose sur l'organisation documentaire des serveurs *web* et en particulier du *webmaster*. Chaque site *web* possède une tête de liste, souvent appelée « index » qui oriente le visiteur de pages en pages. L'intérêt de ce modèle est la taille très petite d'une page *html* qui permet ainsi d'envisager des accès de masse.

- Le témoin de connexion ou *cookie*

Lors d'une visite sur un site *web* (lors de la phase 6 de la recherche), les serveurs incorporent dans leur protocole plusieurs capacités :

- lire les informations transportées dans le protocole *HTTP* qui rendent unique la source de la requête : tel usager. Il est également possible de noter son adresse *IP*, son nom de domaine de connexion, etc.

- relier ces informations à celles demandées à l'utilisateur : son nom de *login*, son mot de passe, et les autres informations données lors d'une inscription sur son site *web* ;

- le serveur peut également inclure dans le protocole la demande d'un fichier de connexion appelé *cookie* dans lequel les serveurs incorporent des informations comme les identifiants de session (temporaire), les heures de connexion et autres informations.

Ce petit fichier anodin le resterait s'il n'était pas utilisé à de nombreuses reprises :

- par les responsables de sites pour élaborer des profils dits de « *user experience* » ;

⚠ **- par des attaquants pour obtenir des numéros de session et s'insinuer dans le flux légitime ;**

- pour toute autre utilisation.

B. INFRASTRUCTURES GLOBALES POUR LES SERVICES : LE NUAGE NUMÉRIQUE

1. Les quelques étapes clés

La recherche de la mutualisation de services trop coûteux au niveau individuel mais envisageable à l'échelle communautaire a été, depuis la révolution industrielle du début du XIXe siècle, la préoccupation sociétale majeure, c'est elle qui a conduit au déploiement de la voie ferrée, d'un réseau RTC, etc.

Dans le numérique, cette démarche a conduit successivement à la création de :

- dans les **années 1950 - 1980 :** applications « grands systèmes *IBM* » centralisés et mutualisés entre entreprises ;

- dans les a**nnées 1980 - 1990** : services experts en téléphonie loués (*IBM*, etc.) comme le fax, les liens télécoms pour les petites entreprises ;

- dans les a**nnées 1990 :** mutualisation d'applications par le biais de fournisseurs d'accès aux applications (*ASP*, ancêtre du *SaaS*).

L'informatique en nuage (ou *cloud computing*) se présente désormais comme l'évolution naturelle de la distribution mutualisée de services informatiques tout en un, alliant en particulier la **productivité**, la **compétitivité**, l'**agilité** et l'**organisation de la sécurité de l'entreprise**.

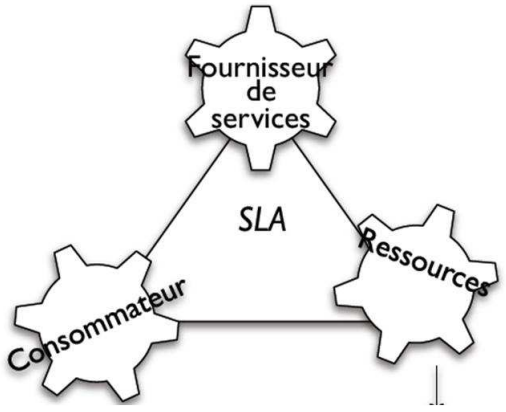
Les échecs de la sécurisation des systèmes d'information, la complexité et le nombre de normes et lois devant être respectées, les coûts considérables que ces obligations engendrent amènent l'entreprise à se poser la question de l'externalisation de la fonction de sécurité ainsi que de nombreuses autres, comme celle des liens télécoms aux applications coûteuses en développement logiciel.

2. L'informatique en nuage comme changement de paradigme

L'informatique dans les nuages numériques constitue une nouvelle manière de fournir des ressources et des services puisque l'objectif est d'assembler des technologies (protocoles, standards, etc.) et composants informatiques (serveurs, équipements réseau, etc.) existants et bien éprouvés.

Il s'agit d'un paradigme fondé sur le principe d'**un service « à la demande » totalement adapté aux besoins ponctuels ou permanents du client**. Mais ce qui paraît le plus original est que **les ressources sont des serveurs, des programmes, des liens télécoms regroupés en une seule offre de service**.

Schéma n° 31 : Relation entre le fournisseur de service et le client dans le contrat de service



***Source** : OPECST*

Après deux ans de travaux, le *National Institute of Standards and Technology* ***(NIST)*** a résumé l'informatique en nuage en cinq points essentiels :

- **libre-service à la demande** : les services et ressources sont offerts et délivrés à partir d'une architecture de type portail selon les besoins du client ;

- **accessibilité du service offert** depuis n'importe quel endroit du réseau et *via* diverses plates-formes (ordinateurs portables, téléphones mobiles, etc.) ;

- **mutualisation des ressources** : physiques ou surtout virtuelles, celles-ci sont paramétrables et réunies afin d'être dupliquées, allouées dynamiquement de façon à servir plusieurs clients au travers d'un modèle multilocataire ;

- **élasticité par rapport au besoin** : l'informatique fournie s'adapte rapidement à une variation du besoin ;

- **service mesurable** : les résultats attendus sont évalués par le biais de mécanismes capables d'instrumenter et mesurer les paramètres de consommation, etc.

Contrairement à une idée reçue, **l'externalisation ne fait pas partie de la définition de l'informatique en nuage**.

3. Les modèles de services offerts par le nuage numérique

Ces modèles concernent trois types de services :

- *IaaS* (*Infrastructure as a Service*) : les infrastructures sont fournies sous forme de service **en mode clients/fournisseurs** de façon quasi instantanée sans investissement ni installation de matériel, tout en gardant la possibilité de changer leur capacité en fonction de leurs besoins ;

- *PaaS* (*Platform as a Service*) : les plates-formes s'adressent aux **développeurs de logiciels** souhaitant adapter leurs logiciels, les mettre en production sans délais sur des plates-formes puissantes en fonction de la demande de leurs clients ;

- *SaaS* (*Software as a Service*) : une nouvelle **forme de distribution, d'achat et d'usage des logiciels**, configurés et activés sur les serveurs du fournisseur de *SaaS*, ce qui diffère d'un logiciel installé sur des serveurs ou postes de travail du client.

4. Les modèles de déploiements

Le modèle de déploiement permet de spécifier **le lieu** et **l'organisme responsable** de la gestion de l'infrastructure d'informatique en nuage. On distingue quatre modèles selon le cercle de diffusion, leur gérant et leur responsable :

- **Nuage numérique public** : accessible au grand public, aux groupes privés mais détenu et géré par un fournisseur de nuage ;

- **Nuage numérique privé** : accessible à l'organisme externe qui le gère ou le confie à un tiers, les ressources seront hébergées dans les locaux de l'organisme ou du tiers ;

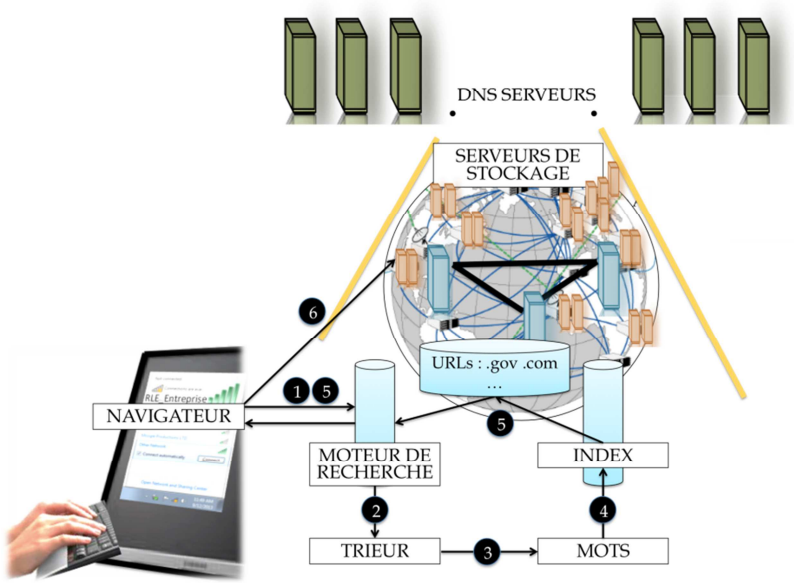
- **Nuage numérique communautaire** : accessible à différents organismes nouant des intérêts communs : politiques, règles de sécurité, activités, besoins spécifiques, etc., géré par l'un ou plusieurs de ces organismes ou par un tiers et pouvant se trouver dans les locaux de l'un de ces organismes ou du tiers.

Le **nuage hybride** combine plusieurs de ces modèles.

« **Nos données sont, à 90 %, stockées dans des centres privés** (*data centers*), mais celles qui ne présentent pas de caractéristique particulière sont conservées dans un nuage, *cloud*, public.»

Mme Pascale Bernal
Directeur du système d'information, GrDF
26 juin 2014
Auditions. Tome II du présent rapport

Schéma n° 32 : Infrastructure de nuage numérique



Source *: OPECST*

Les perspectives du nuage numérique sont maintenant bien établies, mais leur déploiement soulève encore des réserves.

5. Enjeux de sécurité du nuage numérique

L'un des principes clé est d'offrir des services à large échelle à la demande, ce qui implique une infrastructure multilocataire (*multitenant*), complexe et ouverte pouvant présenter de nouvelles vulnérabilités.

⚠ En particulier, **un modèle en nuage public repose sur le réseau Internet (non fiable)** et implique des applications, parfois des applications métier, ce qui ouvre celles-ci à des **risques de cyberattaques**.

La performance entre également en jeu selon la qualité du réseau pour accéder à ces applications. Néanmoins, ces infrastructures ont des configurations modélisées et éprouvées de la couche physique à la couche applicative, ce qui apporte des modèles, les simplifie, permet de les tester et de les vérifier afin d'en assurer une surveillance plus étroite.

> « Par ailleurs, les données ont une valeur que de nombreuses entreprises ne mesurent pas comme il se doit. **Une entreprise comme *Facebook* investit 1,2 milliard de dollars dans un *data center* sans faire payer le client ; les ressources proviennent donc de l'exploitation des données des clients et de la publicité**. **Rien n'est gratuit sur Internet**. Nous ne nous inscrivons pas dans cette logique et nous n'avons pas ce volet d'optimisation financière : les clients qui viennent chez nous paient le service que nous proposons. Cela dit, **nous respectons la loi française et n'exploitons pas les données de nos clients** ».
>
> ***M. Thierry Floriani***
> ***Responsable de la sécurité des systèmes d'information, Numergy***
> *26 juin 2014*
> *Auditions. Tome II du présent rapport*

Les préoccupations des clients seront de plusieurs ordres :

- **disponibilité du réseau** : la performance étant la clé de la compétitivité de l'entreprise ; perdre la disponibilité remet en question le choix d'une informatique gérée et mutualisée ;

- **perte de contrôle physique des données** qui ne sont plus que partiellement à leurs propriétaires ; or la perte de leur contrôle menace le principe de confidentialité ;

- **viabilité du fournisseur** : le fournisseur multilocataire dépend de plusieurs tiers ; le manque de maturité de ces fournisseurs peut amener un client à s'interroger sur leur fiabilité.

« **En ce qui concerne le *cloud computing*, nous lui accordons une confiance limitée dans la mesure où la géolocalisation des données et le degré d'application des mesures d'hygiène informatique ne sont pas garantis**. Il est difficile de s'assurer que le prestataire, soumis à des objectifs de rentabilité financière, soit en capacité d'appliquer les mesures de sécurité requises. En outre, il existe un **problème de réversibilité** : une fois les données mises dans le nuage, existe-il des moyens suffisamment robustes pour les récupérer ? J'insiste sur le fait que l'accompagnement de l'ANSSI est capital, étant donné la dissymétrie des moyens et la complexité des enjeux. La Commission nationale de l'informatique et des libertés (CNIL) joue également un rôle, davantage axé sur la protection des données personnelles ».

M. Ahmed Bennour
Directeur des systèmes d'information, Areva
26 juin 2014
Auditions. Tome II du présent rapport

« Le CEA a une position claire sur le *cloud computing* et l'infogérance. **Nous n'utilisons pas le *cloud computing* car nous souhaitons conserver la maîtrise de notre système d'information**. Nous recourons à l'infogérance, mais nous hébergeons les sous-traitants dans nos locaux ».

M. Lionel Darasse
Chef du service de protection des activités classées et des informations (SPACI), direction centrale de la sécurité, CEA
26 juin 2014
Auditions. Tome II du présent rapport

« **Il faut une volonté nationale de promouvoir les outils français : des hébergeurs français, des nuages numériques français, dans un cadre français, avec des réseaux français**. Une sensibilisation est essentielle pour cela. Cela peut partir des grands groupes dans lesquels il y a des représentants de l'État.

Sinon, il est impossible d'avoir quelque confiance que ce soit dans le nuage numérique, y compris dans les nuages français et d'autant moins lorsqu'ils sont gouvernés par des lois non françaises ».

Mme Claude Revel
Déléguée interministérielle à l'intelligence économique
27 mars 2014
Auditions. Tome II du présent rapport

CHAPITRE IV – FORCES ET FAIBLESSES DU SYSTÈME D'INFORMATION DE L'ENTREPRISE

L'entreprise est au cœur des activités économiques des sociétés modernes, elle y possède un statut particulier en ce sens qu'elle en est un consommateur de biens et de services au sein de la sphère marchande mais également un producteur. En outre, ce statut particulier lui permet d'interagir avec les autres sphères étatiques et privées.

I. LES TROIS NIVEAUX DE L'ENTREPRISE

Les échanges sociétaux de l'entreprise peuvent être représentés de plusieurs façons qui marquent la différence avec un échange individuel :

- un centre de décision agissant avec les autres, de façon responsable et éclairée ;

- un réseau maillé ou chacun, tour à tour, produit et consomme les biens produits par d'autres ;

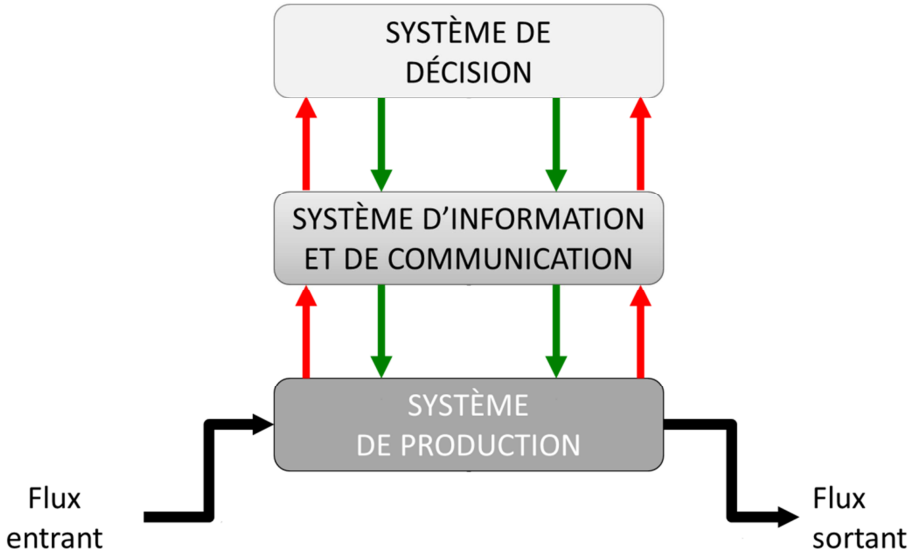
- un centre de production pour manufacturer un bien ou proposer un service.

L'entreprise achète une matière, sous une forme plus ou moins brute, pour la transformer en un produit, plus ou moins fini, dans l'objectif de vendre avec profit.

La théorie systémique distingue trois systèmes principaux qui vont conditionner la réussite du processus de production : le système de décision, le système d'information et de communication et le système de production.

Tous ces systèmes ont été transformés par le numérique. Ils y ont gagné en efficacité mais l'analyse des failles numériques éventuelles desdits systèmes est impérative.

Schéma n° 33 : Les trois niveaux de l'entreprise (décision, information et communication, production)



***Source** : OPECST*

A. LE RÔLE DU SYSTÈME DE DÉCISION

Le système de décision a pour finalité de produire une action éclairée en s'appuyant sur des connaissances issues des informations qui proviennent du contexte et de savoir-faire, raisonnements et méthodes capitalisés au fur et à mesure de son expérience. En particulier, le système de décision incorpore, dans la définition de ses stratégies, des modes d'organisation en fonction de normes, règles ou lois. **Les entreprises actuelles orientent leur management vers un mode dit agile afin d'anticiper les menaces qui pèsent sur leur activité** et de développer plusieurs modèles d'affaires.

Les outils du système de décision reposent sur trois pivots :

- la connaissance de l'écosystème ;

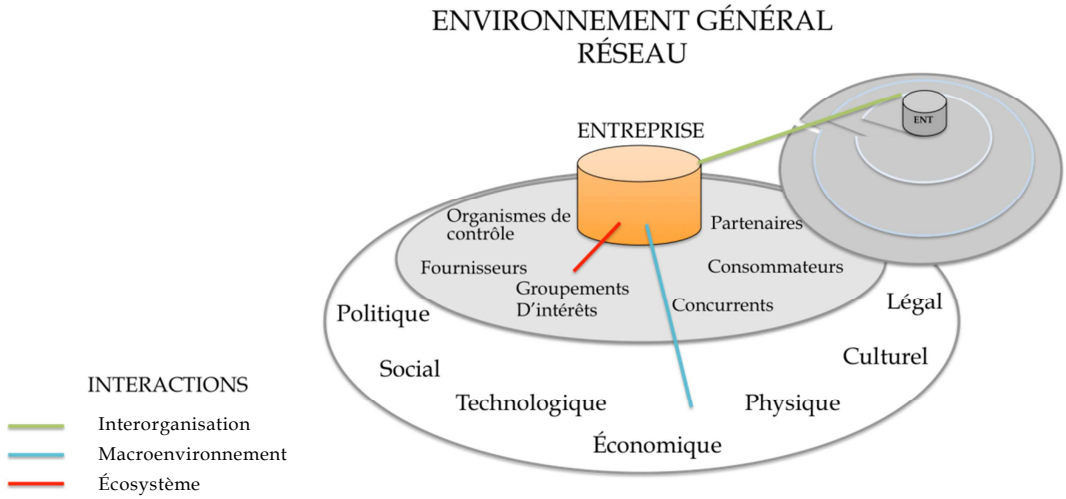
- la définition d'une stratégie clairement énoncée et diffusée ;

- les indicateurs.

a) La connaissance de l'écosystème

Les connaissances concernent les métiers de l'entreprise, inséparables aujourd'hui d'une maîtrise du numérique, le marché, les règles, normes et lois. L'absence de telles connaissances représente une menace directe pour la vie de l'entreprise.

Schéma n° 34 : Les interactions avec l'écosystème



***Source** : OPECST*

b) La stratégie de l'entreprise

On distingue généralement le pilotage stratégique de l'entreprise qui s'appuie sur une gouvernance la reliant à son écosystème et le pilotage opérationnel focalisé sur la production. Plusieurs processus conjoints sont nécessaires pour garantir le fonctionnement de l'entreprise au sein de son écosystème : l'identité, la régulation vis-à-vis de l'extérieur et la connaissance du marché, la gestion des connaissances de l'entreprise, la régulation interne à l'aide de règles d'usage et de chartes.

(1) Identité de l'entreprise

La première étape d'une stratégie consiste **à définir l'identité de l'entreprise**, celle qui va fédérer les collaborations.

Pendant longtemps, les organisations ont élaboré leurs divisions logiques ou services à partir de leurs implantations physiques : le bâtiment de la division « direction », le pavillon de la division « étude ». Dans un tel modèle, la frontière de l'entreprise se calque sur celle de son patrimoine immobilier. En théorie des organisations, cette façon de se structurer s'appelle « l'identité groupale » où une organisation construit son identité et sa reconnaissance à l'intérieur de la frontière physique du territoire qu'elle occupe : ce n'est donc pas étonnant que **les concepts d'« identité » et de « frontière » s'accommodent mal du numérique**.

Cette stratégie, qui présente l'avantage de fermer le système qu'est l'organisation aux perturbations externes et à des changements d'états, facilite par là-même son système de défense.

Mais aujourd'hui, la frontière de l'entreprise est devenue floue et mouvante.

(2) Régulation et marché

Ensuite, le décideur doit inscrire dans le collectif, les buts, objectifs ou finalités qu'il souhaite atteindre. Il fédère des mécanismes d'administration, tous fondés sur la régulation.

L'étape tournée vers le marché est l'utilité du bien ou du service produit. Ce point est devenu l'un des concepts fondateur de la micro-économie où l'on évalue par la fonction d'utilité la satisfaction du besoin fondamental exprimé par un consommateur. Un bien ou un service s'évalue par cette même fonction, un service procure également une satisfaction à son usager.

(3) Gestion des savoirs et savoir-faire

Parmi les processus stratégiques, celui de la gestion de la connaissance experte est fondamental, ainsi que la collecte et le stockage d'informations variées en lien avec l'activité de l'entreprise : l'intelligence économique. Le défaut de ces connaissances risque d'entraîner l'entreprise dans un mode sans mémoire qui, à l'extrême, produirait un système reproduisant toujours la même erreur.

(4) Règles d'usage et chartes

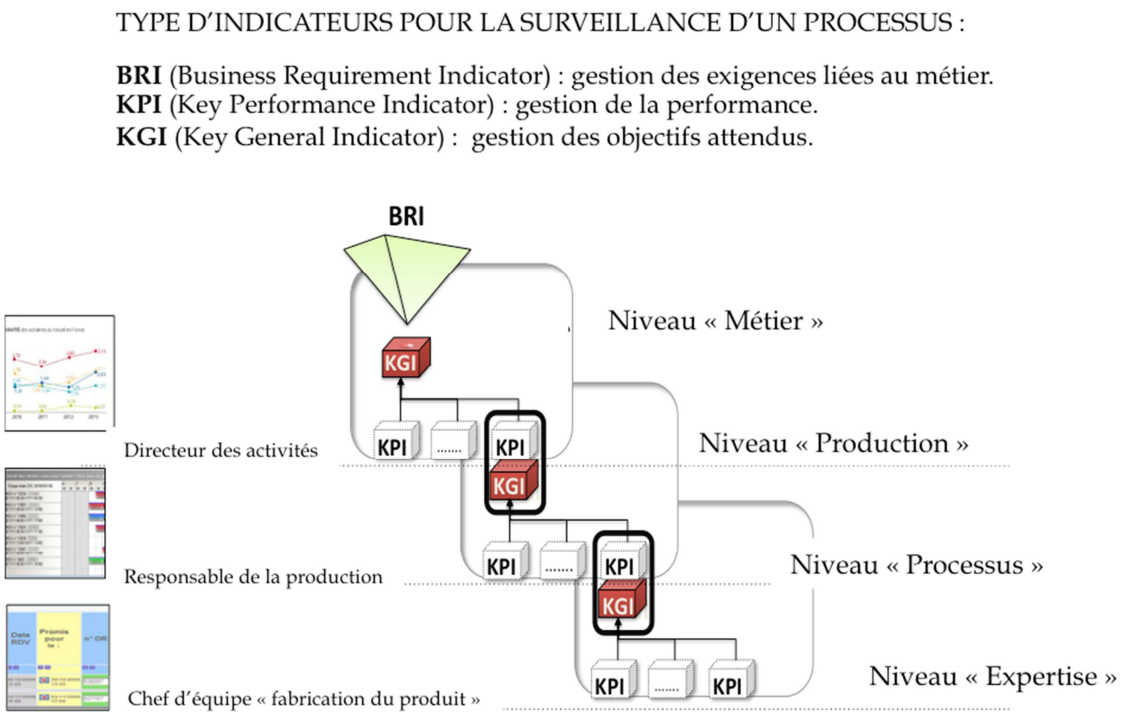
Le décideur doit également énoncer les préférences de l'entreprise et les règles face à certaines situations à l'aide de chartes d'usage ou de **politiques de sécurité notamment en matière numérique** ; ces préférences sont généralement fondées sur des fonctions d'utilité ou de survie de l'entreprise. Enfin, le décideur met en place un **système de valeurs** incluant également l'**évaluation** des processus de gestion.

c) Les tableaux de bords

Ce sont des outils de pilotage indispensables pour permettre aux décideurs de garder une vision globale sur les activités de l'entreprise de façon synthétique et analytique, dans le temps et dans l'espace.

Les méthodes pour déployer de tels indicateurs au sein des entreprises sont très complexes et requièrent plusieurs compétences : expertise métiers et managériale pour définir le besoin. Des systèmes méthodologiques (ITIL ou ISO/IEC 20 000) sont élaborés par des spécialistes. Mais cette question demeure délicate puisque **les indicateurs clés de performance (*KPI*) qui mesurent différents fournisseurs de service d'un même processus se heurtent parfois à des objectifs incompatibles**. Par exemple, **le montant d'un investissement lié à la sécurité numérique pourra être jugé excessif par rapport à d'autres investissements à la rentabilité évidente à court terme**.

Schéma n° 35 : Continuum du flux informationnel pour la surveillance



Source *: INSA, Département Télécoms*

L'efficience du système de décision repose sur la qualité des informations qui proviennent de l'environnement, ce qui donne toute sa dimension au rôle du système d'information et de communication.

B. LE SYSTÈME D'INFORMATION ET DE COMMUNICATION

1. Le système d'information

L'enjeu d'un système d'information est de fournir une valeur pertinente pour des décisions. Cette propriété, généralement difficile à évaluer, est à la base d'une décision de qualité.

Le système d'information assure la qualité de l'information dans les deux sens :

- descendant : l'information transmise au système de production permet d'accomplir les activités au mieux ;

- ascendant : l'information transmise au système décisionnel note les déviances et permet de corriger et d'optimiser le fonctionnement de l'entreprise. Ce sont des informations de contrôle à l'aide desquelles le décideur agit.

Le système d'information incorpore des capacités de **mémorisation des informations indispensables pour que l'entreprise puisse tenir des**

journaux de ses expériences et capitaliser ses savoir-faire. Le système d'information incorpore également un système de communication.

2. Le système de communication

L'enjeu du système de communication sera la cohésion de toutes les parties internes et externes de l'entreprise. Afin de préserver son équilibre, l'entreprise peut opter pour **deux formes de relations** :

- **asymétriques** fondées sur **le pouvoir**, l'expertise, le statut psychologique de l'un par rapport à l'autre ;

- **symétriques** ou égalitaires fondées sur **la confiance**.

Le rôle du système de communication sera d'assurer les circulations propres à rendre efficaces ces interactions. En effet, ces deux formes de relations peuvent toutes deux exposer l'entreprise si les circulations entre les uns et les autres sont mal gérées. Trop d'autorité ou trop de confiance dans un système quasi isolé peut conduire à des blocages. Le rôle du système de communication jouera pour cette raison un rôle de régulation à l'aide de circulations tant internes qu'externes.

a) Circulations internes

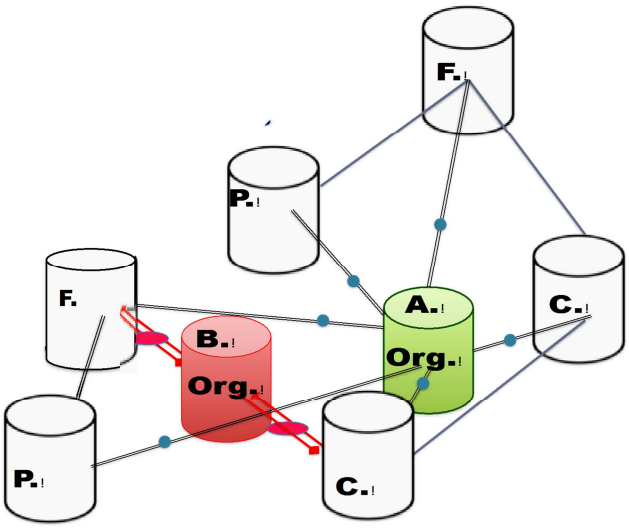
Tous les niveaux de l'entreprise sont irrigués par des flux ascendants, descendants ou transverses, pour communiquer les consignes sous forme d'informations ainsi que les effets qu'elles ont produits. Les organigrammes de l'entreprise reflètent généralement ces formes de relations.

L'exclusion d'un membre de l'entreprise par manque de circulation d'informations peut produire des relations désorganisantes qui pourraient devenir dangereuses. C'est pourquoi, **à l'heure actuelle, les entreprises s'orientent vers des structures légères plus agiles au regard de structures hiérarchiques à plusieurs niveaux**.

b) Circulations externes

Une entreprise forme un écosystème à partir duquel elle interagit avec d'autres entreprises, soit dans l'adversité, soit dans la cohésion. Par exemple, lors d'une attaque numérique ou de la résilience face à celle-ci. Les circulations externes sont les seules voies d'échange avec d'autres écosystèmes.

Schéma n° 36 : Complexité du réseau des interactions de l'entreprise



C. : Client
F. : Fournisseur
Org. : Entreprise
P. : Partenaire

Source *: INSA, Département Télécoms*

Les communications, notamment dans leurs composantes numériques, peuvent néanmoins fragiliser l'entreprise, c'est pourquoi un des devoirs de l'entreprise est également de se protéger.

C. LE SYSTÈME DE PRODUCTION DE L'ENTREPRISE

L'enjeu du système de production est d'accomplir sans erreur les consignes. L'entreprise met en œuvre des activités opérationnelles de base en exécutant et contrôlant des actions issues de consignes émises par le niveau stratégique.

1. Le concept d'industrie 4.0

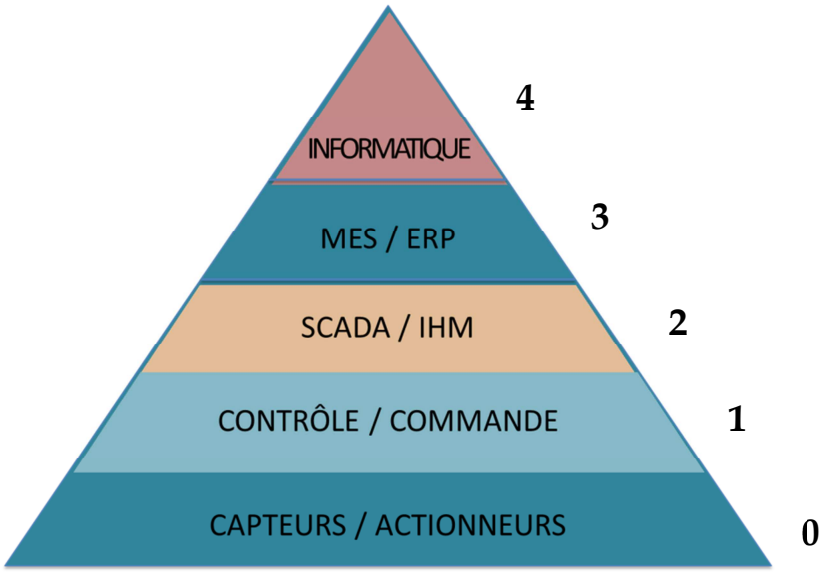
Au début des années 1990, le modèle de référence du système d'information d'une entreprise industrielle reposait sur le modèle *CIM* (*Computer Integrated Manufacturing*). L'objectif visait alors une automatisation des processus industriels et de la gestion de leurs données allant des données produites par les capteurs aux données de gestion du système d'information. L'intérêt d'une structure en niveaux étant de nature à faciliter l'évolution progressive des processus à automatiser.

Dans le schéma ci-après, les différents niveaux de la structure de l'entreprise d'après le modèle *CIM* sont représentés.

En bas, les niveaux 1 et 2 concernent le mode « contrôle-commande » lié aux capteurs et les niveaux 3 et 4 concernent la supervision et la planification de la fabrication. Par exemple, un logiciel de gestion de production assistée par ordinateur (GPAO) se situe au niveau 4.

Aujourd'hui, cette gestion est directement reliée avec les *ERP (Enterprise Resource Planning*) de l'entreprise.

Schéma n° 37 : Le modèle de référence *CIM* des processus industriels en vue de leur automatisation



***Source** : OPECST*

2. *Le Manufacturing Execution System (MES)*

Le *MES* constitue le **système de contrôle et de suivi des travaux en cours dans l'atelier**. Son rôle est la collecte (trait rouge dans le schéma n° 46 ci-après) de toutes les traces des activités de fabrication en temps réel provenant des capteurs et actionneurs contrôlés par des automates (niveaux 0 et 1 du schéma ci-dessus) ; il est au plus près de la fabrication devant répondre à des impératifs temporels de l'ordre de la minute. Ainsi, le *MES* se situe-t-il entre les niveaux 1 et 2 du *CIM*, occupés par la supervision des capteurs actionneurs ainsi que leurs contrôleurs, et le niveau 4 de la planification, occupé par la GPAO.

3. *Le Supervisory Control And Data Acquisition* (*SCADA*)

« Les systèmes de commande, appelés *SCADA* dans la terminologie des informaticiens, sont de plus en plus, à la base, construits avec des composants informatiques traditionnels. Ainsi, les *Transmission Control Internet Protocol (TCP/IP)* des logiciels de *Microsoft* ou de *Linux* sont utilisés dans les *SCADA*. Ces systèmes sont donc de plus en plus vulnérables. La

sécurisation des systèmes d'information industrielle a donc été décidée sur tous les sites de *Total*, que ce soient les plates-formes, les raffineries, les dépôts, pour compléter efficacement le dispositif actuel ».

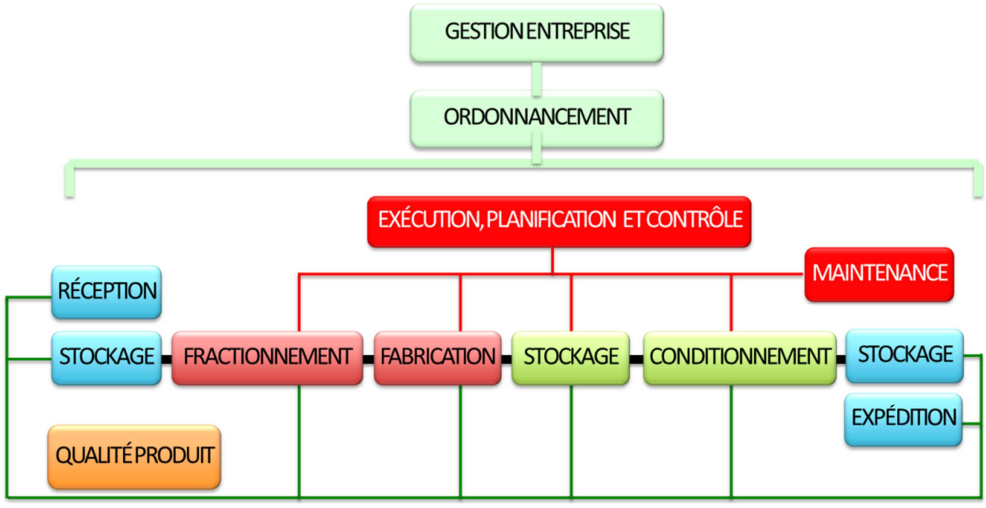
M. Patrick Hereng
Directeur des services d'information et des télécommunications*, *Total
6 mars 2014
Auditions. Tome II du présent rapport

4. Les capteurs et actionneurs

« Aujourd'hui, chez *Total*, il y a des dispositifs de surveillance installés dans des turbines sur les plates-formes pétrolières ; **ces capteurs mesurent en continu de nombreux paramètres** – la température, la vitesse de rotation – et **ces informations sont analysées à partir de technologies de *big data* pour déterminer des débuts de pannes** ; cela évite d'être victime d'une rupture de turbines obligeant à arrêter la production d'une plate-forme ».

M. Patrick Hereng
Directeur des services d'information et des télécommunications*, *Total
6 mars 2014
Auditions. Tome II du présent rapport

Schéma n° 38 : Représentation simplifiée d'un processus de fabrication de l'entreprise



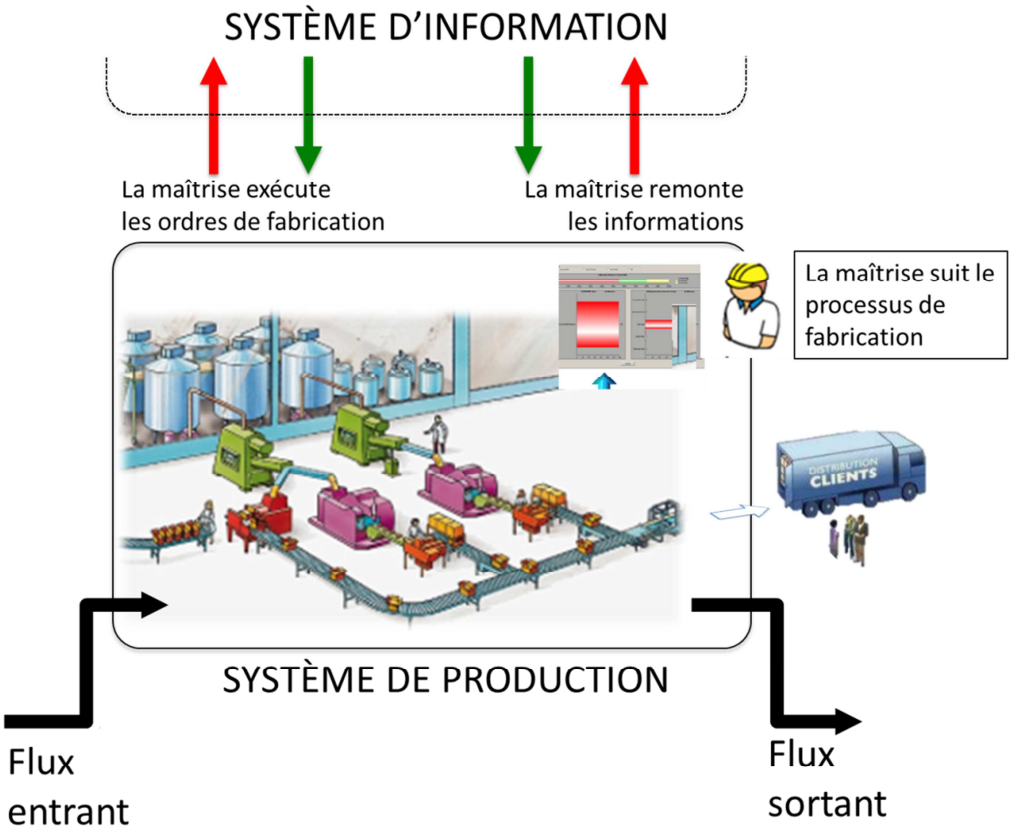
***Source** : OPECST*

Les décisions prises au niveau du *MES* sont de nature opérationnelle, plutôt de l'ordre du réflexe pour s'adapter aux aléas de

l'environnement de nature temporelle et/ou spatiale. **Le système de production reçoit les instructions par le biais du système d'information et remonte les aléas par ce même biais**.

L'ensemble de ce processus repose sur le bon fonctionnement du numérique de l'entreprise dans toutes ses composantes.

Schéma n° 39 : Représentation simplifiée d'un processus de fabrication de l'entreprise



Source : OPECST

La protection de la capacité de production de l'entreprise est fondamentale car elle conditionne sa survie. Généralement, les entreprises font en sorte que les actions soient gérées par anticipation et mettent en œuvre dans cette optique une gestion des risques industriels.

La gestion des risques est une méthode qui vise la maîtrise des processus de production. Sa complexité a très tôt nécessité la mise au point d'une méthode ; la plus connue est la méthode d'Analyse des Modes de Défaillance et de leurs Effets et Criticité (AMDEC) fondée sur les arbres des causes et des effets.

II. ANALYSE CRITIQUE DU SYSTÈME D'INFORMATION DE L'ENTREPRISE

Le système d'information est au cœur des processus de l'entreprise. Il est conçu pour exercer plusieurs fonctions généralement regroupées autour de la collecte d'informations en rapport avec l'activité de l'organisme, de leur traitement, de leur stockage puis de leur diffusion. C'est pourquoi **la forme électronique du système d'information constitue un atout considérable, jamais encore connu, pour faciliter le gain et l'obtention de l'information**.

Les activités des métiers du système d'information d'une entreprise sont modélisées pour déterminer les fonctions à automatiser à partir de l'expression des besoins. La modélisation se réalise à partir de modèles de référence qui expriment l'ensemble des connaissances et des données métiers de l'entreprise, ainsi que leurs relations.

De plus en plus, un système d'information est perçu comme un édifice construit pour et par la coopération des hommes ou d'autres systèmes d'information jusqu'à constituer un véritable réseau de connaissances. **Il semble que les fonctions du système d'information évoluent aujourd'hui afin de favoriser la circulation de la connaissance en plus de celle de l'information**.

Pour ce faire, **un système d'information recouvre plusieurs fonctions de** :

- système de communication : il réalise un **couplage entre modules opérationnels et de pilotage** afin de garantir l'atteinte d'un objectif de service vis-à-vis de l'information : sa rapidité de transmission, sa fiabilité, son adéquation face à son destinataire et sa complétude ;

- services réseaux et applicatifs : une relation de service s'établit entre le système d'information et l'usager où le système **met en forme l'information** afin de faciliter l'accès ;

- gestion de fichiers : elle permet de constituer la **mémoire de l'entreprise** à travers le stockage : serveurs, ordinateurs, données et connaissances ;

- sécurité : elle doit garantir la **disponibilité**, l'**intégrité** et la **confidentialité** (DIC) des éléments contribuant à leur transport et leur stockage. Ces dimensions ont été rappelées lors des auditions.

« [...] la cybersécurité dans ses trois dimensions : sa **couche physique,** c'est-à-dire les télécoms, les tuyaux, les ordinateurs, sa **couche virtuelle**, **logiciels**, protocoles, serveurs etc., et, dans **sa couche informationnelle**, informations, propriété de l'information, traitement de l'information ».

M. Hervé Guillou
Président, Conseil des industries de confiance et de sécurité (CICS)
26 février 2014
Auditions. Tome II du présent rapport

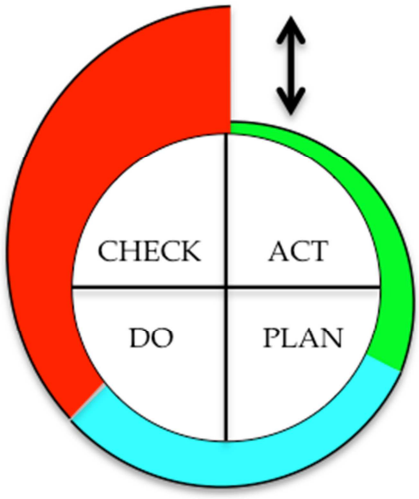
Vos rapporteurs ont estimé indispensable de passer au crible les diverses fonctions du système d'information pour en détecter les éventuelles fragilités numériques.

A. MODÉLISATION D'UN SYSTÈME D'INFORMATION EN VUE DE SON ÉLABORATION

La modélisation est une activité complexe qui requiert une méthode. Pendant longtemps, les méthodes de modélisation reposaient sur une approche dite entité-relation, puis vint la proposition d'une modélisation dite objet et enfin, **aujourd'hui, la modélisation des processus se réalise à l'aide des méthodes « agiles** ».

La roue de Deming (*plan, do, check, act*) définit les **quatre fonctions majeures qui servent de base à l'organisation des systèmes d'information**.

Schéma n° 40 : Amélioration de l'état de sécurité



Source *: INSA – Département Télécoms*

B. LE SYSTÈME DE COMMUNICATION

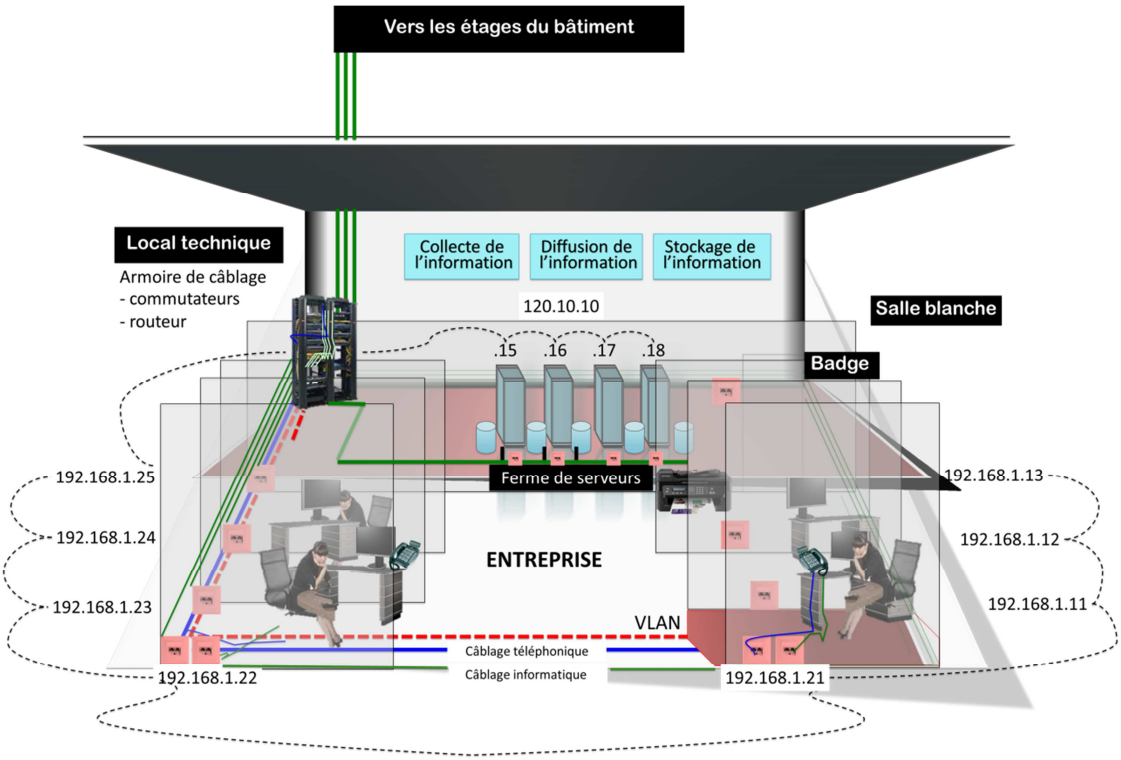
Depuis les années 1990, les entreprises se sont connectées de différentes manières pour faciliter leurs communications avec des partenaires extérieurs. Afin d'optimiser les coûts des éléments de base du système d'information, ceux-ci sont mutualisés à l'aide d'un réseau pour en gérer le partage entre utilisateurs.

⚠ Cette organisation, de plus en plus efficace pour inventer de nouveaux modèles d'affaires propices au développement des profits des entreprises, ouvre, néanmoins, par ce même chemin numérique des **opportunités de connexion à des intrus et des usages non souhaités**.

1. Le Réseau Local d'Entreprise (RLE)

La majorité des entreprises se sont dotées de réseaux locaux (RLE) afin de **partager différents types de ressources comme les imprimantes, les serveurs, le stockage, les scanners, les applications réseaux et bureautiques**. Ces réseaux peuvent être filaires ou non filaires. La technologie utilisée dans ces deux cas est de fournir un médium de connexion partagé par plusieurs utilisateurs, généralement les employés.

Schéma n° 41 : Représentation simplifiée du système d'information de gestion de l'entreprise



***Source** : OPECST*

(1) Le câblage

La première étape de la constitution d'un réseau local d'entreprise est celle de la mise en place de son support physique.

Au sein de chaque entreprise se trouve un local technique (LT) qui héberge les équipements réseaux, à savoir un ou plusieurs **commutateurs** selon la taille de l'entreprise et du commutateur. Sur chaque commutateur, entre vingt-quatre et quarante-huit postes de travail sont connectés ; au-delà, d'autres commutateurs sont empilés. Un commutateur a pour rôle de concentrer l'ensemble des flux du réseau ; cela signifie que **l'ensemble des usagers partage ce même équipement**. Généralement, **le local technique est prévu pour filtrer l'accès et le réserver aux administrateurs du réseau de l'entreprise**.

Schéma n° 42 : Apparence d'un commutateur 24 ports



***Source** : Internet*

À partir de là, **le commutateur** distribue le flux jusqu'aux postes de travail, les serveurs ou encore les ressources partagées comme les sauvegardes, les imprimantes, les scanners, etc.

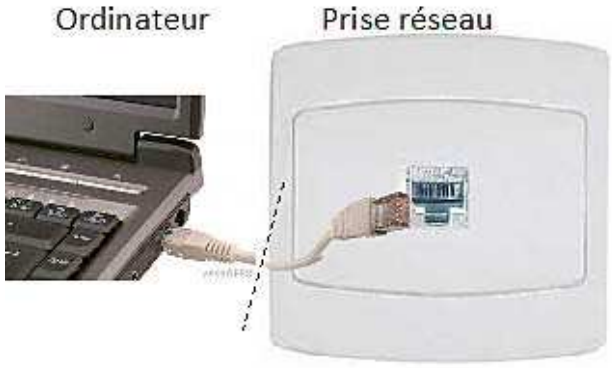
Le câblage court le long des plinthes depuis les commutateurs et rejoint une ou plusieurs prises réseau déployées dans chaque bureau. Chaque équipement connecté comme un poste de travail possède son câble jusqu'au commutateur lorsque la norme déployée est IEEE 10baseT.

Certaines zones de l'entreprise doivent bénéficier de conditions particulières : davantage de confidentialité ou de performance. Il existe une technologie appelée **réseau local virtuel (*VLAN : Virtual Local Area Network*)** qui réalise cette fonction. Un paramétrage particulier au niveau du commutateur affecte à un poste de travail un canal logique dont l'accès lui est réservé (trait rouge en pointillé sur la représentation simplifiée du système d'information de gestion de l'entreprise ci-dessus). Lorsque le câblage et le paramétrage des équipements de distribution sont terminés, l'interface réseau de chaque ordinateur est connectée sur la prise réseau de chaque bureau.

Souvent, le câblage de la téléphonie est couplé avec celui des postes de travail afin d'en optimiser les coûts de déploiement. À l'heure actuelle, la téléphonie se réalise à partir du réseau *IP* à l'aide de la technologie dite de « *voix sur IP* » et celle-ci se trouve alors connectée directement à

l'infrastructure réseau. Afin d'éviter les perturbations entre des flux voix et les données, le principe des réseaux locaux virtuels ou *VLAN* sera mis en œuvre.

Schéma n° 43 : Liaison physique ordinateur / commutateur



***Source** : OPECST*

(2) Le réseau *IP*

À ce stade, les équipements communiquent mais ne peuvent échanger des services Internet tant qu'ils ne sont pas identifiés par leur adresse *IP (Internet Protocol)*.

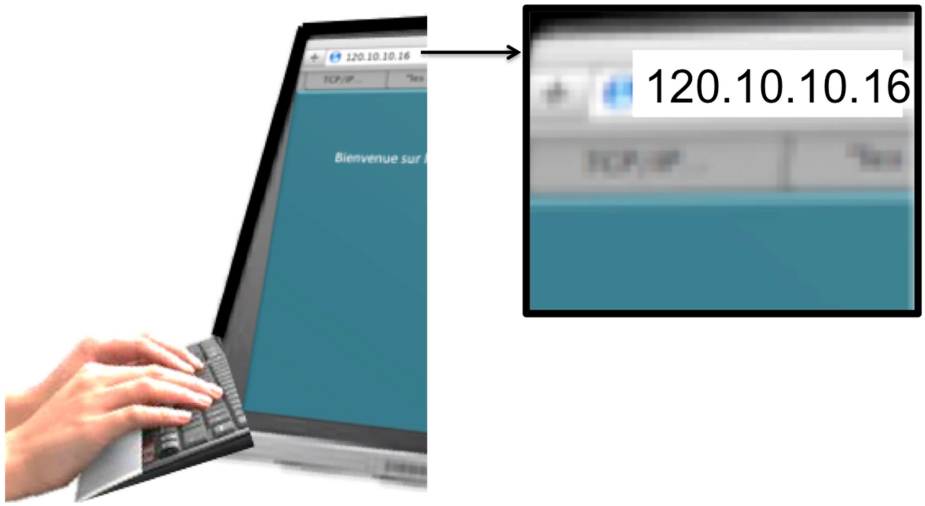
Chaque entreprise met en place un plan d'adressage *IP* afin d'associer chaque équipement à une adresse *IP* unique. Les administrateurs configurent l'adresse *IP* sur chaque équipement et serveur : poste de travail, serveur de fichier, imprimante, etc.

Le local technique héberge également **le routeur dont le rôle est de gérer les routes de l'Internet**.

La représentation simplifiée du système d'information de gestion de l'entreprise figurant plus haut présente en pointillés noirs le flux réseau *IP*. L'exemple présente deux réseaux *IP*, l'un serait celui des usagers avec des plages d'adresses *IP* en 192.168.1.x, l'autre serait celui de la ferme de serveurs 120.10.10.x où x représente l'adresse de chaque équipement, poste de travail ou serveur.

Pour utiliser des services à partir du protocole *IP*, la connaissance de l'adresse de chacun d'entre eux est indispensable. Par exemple, si l'utilisateur ayant l'adresse *IP* : 192.168.1.21 souhaite accéder au service *web* du serveur 120.10.10.16, il utilisera l'adresse *IP* du serveur comme *URL* de son navigateur *web*.

Schéma n° 44 : En réponse à l'*URL* « 120.10.10.16 » le service réseau-*web* devient disponible



***Source** : OPECST*

2. Le réseau local « radio » de l'entreprise ou *Wi-Fi*

Les évolutions des périmètres physiques des entreprises ont parfois conduit certaines d'entre elles à intégrer des solutions moins coûteuses, plus rapides et/ou plus esthétiques pour distribuer le réseau au plus près de ses usagers. Pour ces différentes raisons, les réseaux sans fil (*Wi-Fi : Wireless Fidelity*) ont connu un grand succès auprès de la majorité des entreprises. Au regard de solutions de câblage pouvant atteindre jusqu'à plusieurs centaines de milliers d'euros, **les solutions sans fil constituaient une alternative moins dispendieuse**, d'autant qu'**une simple antenne *Wi-Fi* représente un temps de déploiement de l'ordre de la journée alors qu'une solution de câblage est de l'ordre de l'année.**

a) Principe de base

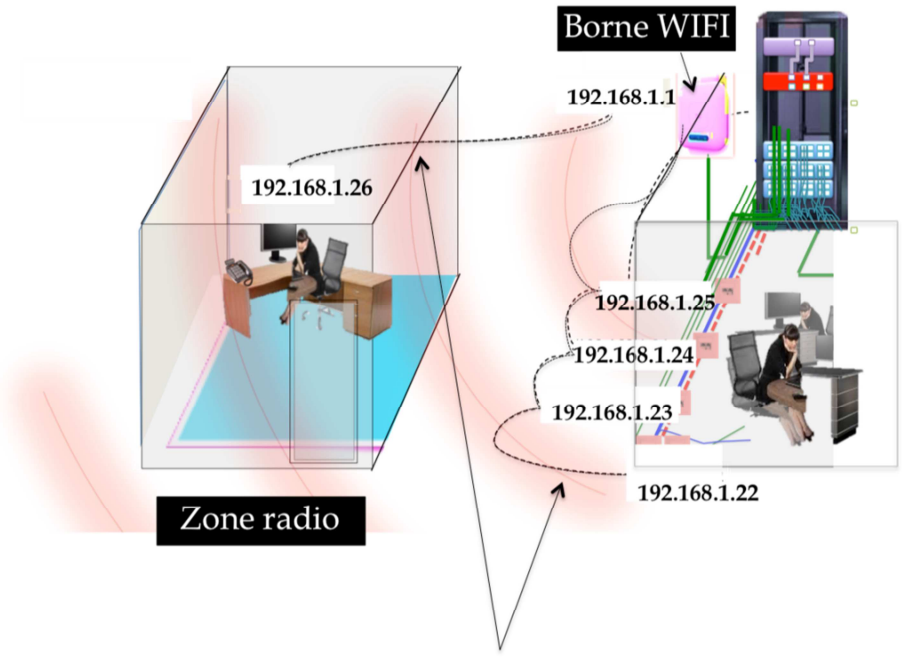
Le principe consiste à mettre en place une borne d'émission et de réception radio (« *access point* », *AP*) qui diffuse sur un canal donné un identifiant réseau appelé *SSID* (*Service Set Identifier*). Chaque poste équipé d'une carte réseau sans fil et présent dans la zone de couverture radio de la borne peut entrer en relation avec le réseau *SSID* sur ce même canal. La communication est établie ; l'opération est simple.

Afin de bénéficier des services Internet, la plupart des bornes incorporent un serveur *Dynamic Host Configuration Protocol* (*DHCP)* qui distribue automatiquement une adresse *IP* à l'utilisateur.

Dans l'illustration ci-après, ce mécanisme est mis en œuvre. Ici, l'usager est hébergé dans un petit local extérieur à l'entreprise qui a préféré mettre à disposition de ce local un service réseau *via* une passerelle sans fil,

le coût étant très faible et offrant aux utilisateurs un accès direct au système d'information de l'entreprise. La borne sans fil est reliée sur le commutateur de distribution.

Schéma n° 45 : Extension sans-fil du système d'information de l'entreprise



Transport du réseau IP sur les réseaux WIFI et filaires

Source *: OPECST*

b) Mode de connexion

La configuration *Wi-Fi* est, à l'heure actuelle, largement déployée, notamment dans les entreprises.

La connexion *Wi-Fi* est assez aisée puisque l'usager peut consulter la liste des réseaux disponibles.

⚠ **Cette liste apporte également d'autres informations sur le réseau concerné comme les mécanismes de sécurité mis en œuvre, le canal, la bande passante disponible**.

⚠ La configuration *Wi-Fi* pourrait néanmoins, du fait du **manque de maîtrise des couvertures radios**, offrir des **opportunités d'accès** et entraîner des **usages non souhaités**.

3. L'interconnexion du système d'information de l'entreprise avec son système d'information industriel

L'efficience des entreprises dépend de leur capacité de réaction face à l'évolution du marché. Lorsque l'on manufacture des produits à partir de chaînes de production lourdes, l'agilité n'est pas évidente du fait des délais de conceptions, de la prise en compte des normes et réglementations en vigueur sur ce marché, des opérations de communications sur les produits finis. Le *MES* (*Manufacturig Execution System*) déjà décrit plus haut constitue pour ces entreprises une aide à la décision précieuse.

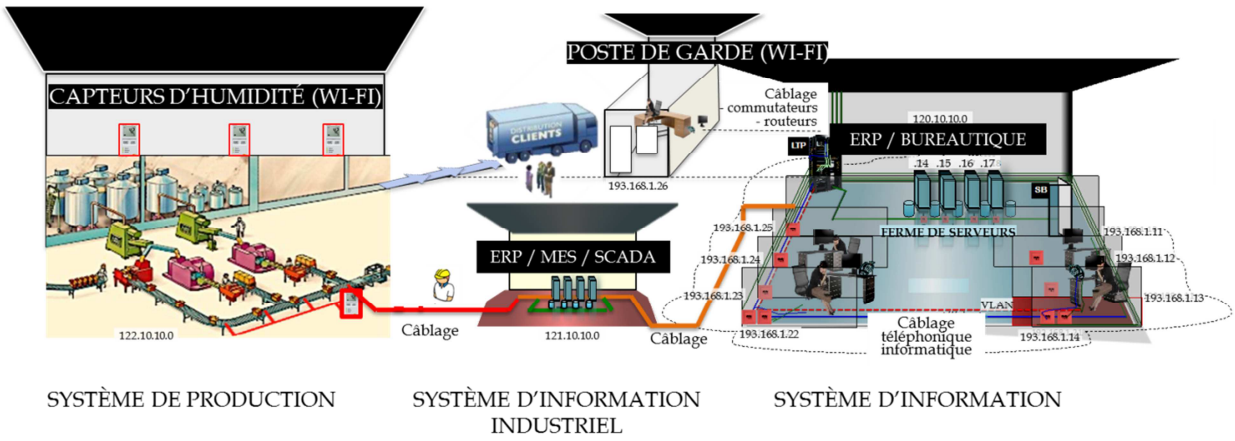
À son origine, le *MES* a été conçu, comme le préconise le modèle *CIM* (*Computed Integrated Manufacturing*), de façon autonome. Néanmoins, il devient de plus en plus intégré à la planification des ressources d'entreprise afin d'améliorer la productivité et réduire les coûts.

Demain, l'entreprise 4.0 constituera un enjeu de taille pour les industries : permettre la proactivité en assurant une livraison de produits à la demande tout en préservant la qualité et en optimisant les coûts.

« Les grandes entreprises sont également au cœur du problème avec des sous-traitants qui gravitent autour d'elles. Leurs systèmes de sécurité sont connectés avec celui de l'entreprise principale avec laquelle ils ont des échanges permanents, donc des interconnexions. Si **ces sous-traitants** n'ont pas mis en place des systèmes de sécurité sérieux, ils **vont constituer des lieux de passage pour les *hackers* cherchant à entrer dans le système principal.** Ce problème existe aussi pour toutes les petites PME et PMI qui travaillent dans l'orbite des grandes entreprises.».

M. Alain Juillet
Président, Club des directeurs de sécurité des entreprises (CDSE)
19 mars 2014
Auditions. Tome II du présent rapport

Schéma n° 46 : Le système d'information gestion interconnecté avec le système d'information industriel



***Source** : OPECST*

4. Objets connectés dans l'entreprise

> « **Actuellement débute l'ère des capteurs, des puces électroniques.** De plus en plus, des **capteurs placés sur le corps** rapporteront des témoignages, actifs ou passifs, des comportements de chacun. Les **capteurs situés dans l'environnement des individus** vont témoigner en continu. **Il y aura de plus en plus une quantification des personnes** (niveau de vie, pouvoir d'achat, compétence professionnelle, accointances entre les individus, connaissance permanente de l'étudiant en ligne, etc.), ce qui amène la **connaissance continue des comportements** ».
>
> ***M. Éric Sadin***
> ***Écrivain et philosophe***
> *5 février 2014*
> *Auditions. Tome II du présent rapport*

De nombreux objets numériques mobiles accèdent désormais aux réseaux de l'entreprise. Il peut s'agir des mobiles des collaborateurs ou encore de personnes en visite dans l'entreprise.

⚠ Il peut également s'agir d'un passant empruntant une rue adjacente, **la couverture de la passerelle sans fil n'étant pas facilement vérifiée, toute personne pourrait de cette façon utiliser des ressources de l'entreprise**. La mise en œuvre de passerelles sans fil entraîne des **opportunités pour des usages non souhaités**.

Schéma n° 47 : Visualisation aisée des réseaux sans fil disponibles aux alentours



Source *: OPECST*

Au quotidien, le problème est que la sécurité physique et la sécurité de l'information sont très imbriquées : par exemple, lorsqu'un ordinateur commande une climatisation, ou un générateur électrique qui commande lui-même une ouverture de porte ou autre chose.

C. LES SERVICES

1. La relation client / serveur numérique

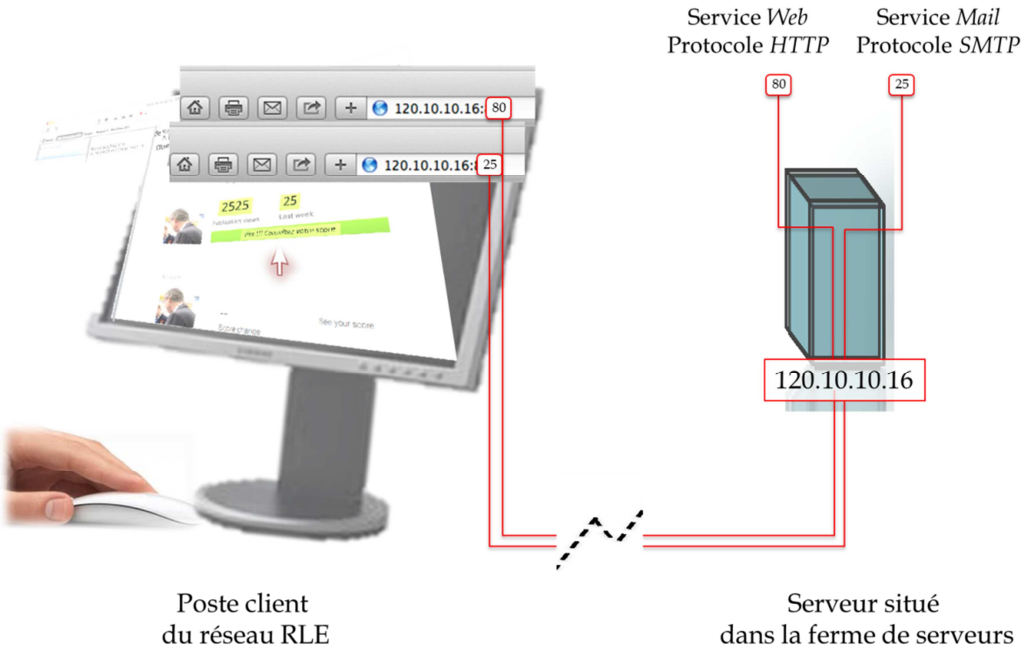
Un service dans le domaine des réseaux constitue une application hébergée généralement sur un ordinateur appelé « serveur » pour cette raison. **Un serveur a pour rôle de traiter des requêtes ou demandes provenant de postes de travail, appelés « clients »**. Pour accomplir ces traitements au service de plusieurs clients, les capacités de traitement et de stockage des serveurs sont très importantes.

Dans l'environnement *IP*, un service est accessible directement depuis le réseau au moyen d'**un identifiant appelé « numéro de port » complétant l'adresse *IP* d'un serveur**. Ainsi, un serveur peut-il héberger plusieurs services : messagerie, *web* sur un même serveur physique.

⚠ À noter qu'un serveur qui répond positivement à une requête : 120.10.10.10 : 80 donne une information sur l'origine de la requête.

Une information sur la présence du service, par exemple, de messagerie sur ce serveur, pourrait entraîner de **mauvais usages**.

Schéma n° 48 : Principe de l'adressage d'un service réseau Internet



Source *: OPECST*

2. Les services réseaux

Le réseau permet de partager des services au sein de l'entreprise. L'ensemble de ces services y est généralement hébergé dans la ferme de serveurs. Il s'agit d'un ou plusieurs réseaux *IP* isolés et localisés dans une salle spéciale appelée « salle blanche » (SB) dont **l'accès est contrôlé et restreint au personnel de l'informatique**. Ces services ont pour but d'**optimiser l'infrastructure sur le plan de la sécurité ou de la performance**, ou encore d'**améliorer l'outil de travail** des collaborateurs.

Ces services d'« infrastructure réseau » facilitent généralement les tâches d'administration ainsi que celles des usagers.

a) Le service d'attribution automatique d'adresses IP

Le premier service, *Dynamic Host Configuration Protocol (DHCP)*, est couramment mis en place dans les réseaux locaux d'entreprise afin d'automatiser la configuration des adresses *IP* sur le poste de travail des utilisateurs.

Le poste de travail du client est configuré généralement par les administrateurs au moment de sa mise en service.

Ce service présente plusieurs avantages : accueil de nombre d'adresses *IP*, diminution des temps de configuration, du nombre d'erreurs,

facilitation des changements de matériel. Le service *DHCP* généralement hébergé au sein de la ferme de serveurs attribue automatiquement une adresse *IP* à un poste de travail lors de sa connexion. Les serveurs sont configurés à l'aide d'adresses *IP* fixes afin qu'ils puissent être contactés par les usagers et les administrateurs. L'image serait celle d'un service de mairie dont l'adresse changerait en permanence.

⚠ **Le service *DHCP* requiert néanmoins un suivi afin de vérifier l'usage des adresses *IP***.

b) Le service de résolution de noms et d'adresses IP

Le second service, *Domain Name System* (*DNS*), offre aux usagers un **service de résolution de noms qui évite la saisie fastidieuse des adresses *IP* dans l'*URL* de leur navigateur**. Chaque ressource est associée à un nom d'hôte et à un domaine *DNS* ; par exemple : www.intranet.entreprise pour le serveur *web* qui devient l'*Uniform Resource Locator* (*URL*) du serveur. Il suffit ensuite à l'usager de saisir l'adresse pour accéder à ce serveur, son poste de travail s'adressera, lors de chaque requête, au serveur *DNS* de l'infrastructure.

c) Le service de gestion du réseau

Le service *Simple Network Management Protocol* (*SNMP*) est un autre service d'infrastructure souvent utilisé pour faciliter la gestion du réseau. Le *SNMP* est un protocole pour **automatiser la collecte des alertes de management afin d'alerter l'administrateur de défauts appelant son intervention**.

Il existe d'autres services d'infrastructure comme les services de réseaux virtuels ou des services de redondance réseau.

⚠ Les services d'infrastructures sont très utiles pour assister l'administrateur dans ses tâches quotidiennes mais ils ouvrent souvent des **opportunités pour des usages non souhaités**.

Certains de ces services seront également indispensables pour l'authentification des usagers et des administrateurs. Ces aspects seront développés plus loin.

3. Les services applicatifs collaboratifs

Les services dits « applicatifs » apportent des facilités aux usagers du système d'information. Il s'agit, de façon très générale, d'**applications bureautiques** ou **d'applications liées au métier de l'utilisateur**. L'usage de ces services se traduit au travers d'applications dites « clientes ». À l'heure actuelle, la tendance est d'utiliser un client « universel », le navigateur *web*, pour utiliser ces applications. De cette façon, les usagers utilisent des

Uniform Resource Identifier (URI) qui englobent les *URL* pour localiser et accéder à leurs ressources.

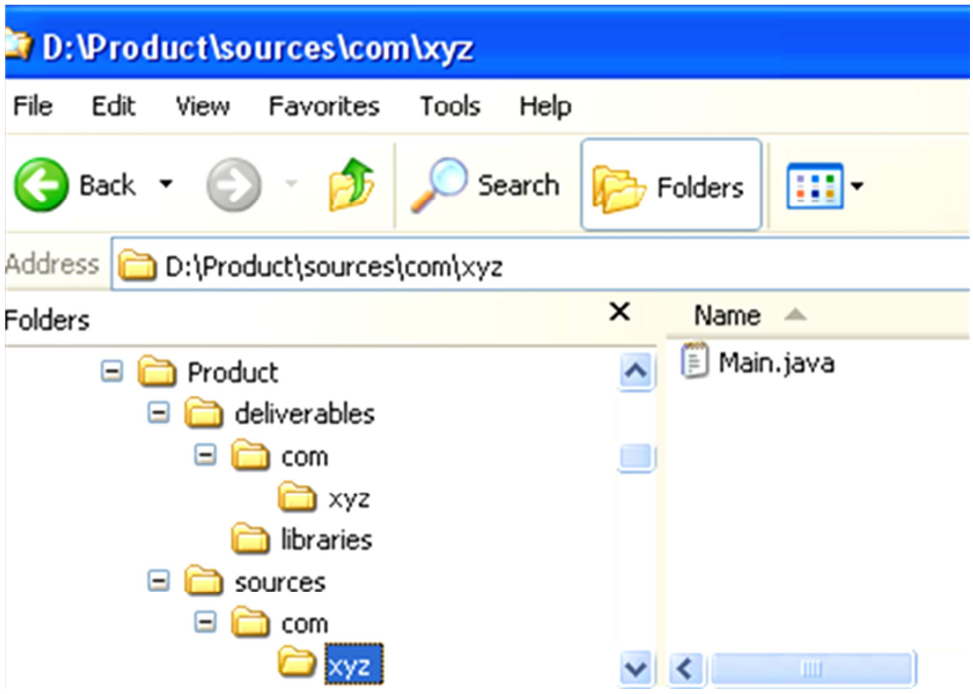
a) Le service de fichier

Le service de fichier est un service destiné au **stockage des fichiers créés, modifiés ou supprimés par les usagers de l'entreprise** lors de la réalisation de leur mission dans l'entreprise. D'une certaine manière, **un tel service est le réceptacle de toute la connaissance de l'entreprise**. Les collaborateurs bénéficient d'espaces, partagés ou personnels, hébergés sur le serveur de fichiers commun. L'avantage est que l'entreprise centralise toute la connaissance et peut régulièrement assurer les sauvegardes de ces éléments précieux du système d'information. Il permet également **de garantir en toute confiance l'accès aux informations** qu'il détient puisque ce service s'accompagne d'un service d'**authentification préalable**.

La centralisation des répertoires partagés permet à l'administrateur de gérer chaque répertoire pour ces utilisateurs. Il veille au maintien de la place disponible sur les serveurs puis il administre des règles de profils d'usage afin de garantir le bon usage de ces espaces de stockage.

À l'heure actuelle, le système de gestion de fichier déployé dans les entreprises est assuré à hauteur de 64 % par les serveurs *Microsoft*, le reste étant composé de serveurs *Linux*, *AIX IBM*, etc.

Schéma n° 49 : Un exemple de gestion de fichier



Source *: OPECST*

⚠ Les espaces de stockage personnels sur des serveurs de l'entreprise facilitent de cette façon **l'incrustation de la vie privée des collaborateurs dans l'entreprise** au travers de ces répertoires et il est légitime de **s'interroger sur les conséquences qui en découlent au regard des aspects légaux et normatifs**.

⚠ À l'inverse, **les collaborateurs non connectés à ce service détiendraient une connaissance professionnelle qui ne serait pas déposée sur le système d'information de l'entreprise**. C'est le cas, bien souvent, des terminaux mobiles comme les ordinateurs portables ou les *smartphones*.

⚠ Enfin, les ressources sont mutualisées afin d'être hébergées dans les centres de données mêlant des données de configurations du système avec des données des utilisateurs. Or, **tous les services d'une même entreprise ne peuvent partager toutes les données**. La nécessité d'un système d'habilitation plus fin se fait ressentir.

b) Le service de navigation

Le service de navigation est au cœur des services Internet, il permet d'accéder à la majorité des services, il pourrait très bien être le seul outil de navigation pour accéder aux services de messagerie, annuaire, etc.

Le premier principe d'un client *web* ou navigateur repose sur le protocole *HTTP* (*HyperText Transfer Protocol*). Il s'agit d'un client léger dans le sens où l'outil est universel, faiblement paramétré du côté de l'utilisateur. La requête est élaborée par le client à partir d'une *URL*.

Une *URL* est une donnée entrée par l'utilisateur composée de plusieurs parties :

Schéma n° 50 : Un exemple d'*URL*



***Source** : Internet*

- le protocole qui définit le langage *HTTP* et permet l'échange de page au format *HTML* (*HyperText Markup Language*). Il est le plus utilisé mais il est possible d'échanger *via* de nombreux autres protocoles comme *https*, *ldap*, *ftp*, etc. ;

- un identifiant et un mot de passe transmis pour se connecter à un serveur sécurisé ainsi que pour spécifier un profil d'accès ; ⚠ mais cette méthode ne s'emploie plus car les traces permettraient de le déchiffrer ;

- le nom du serveur hébergeant la ressource demandée ou son adresse *IP* ;

- le numéro de port associé au service, comme déjà mentionné ci-dessus ;

- le chemin d'accès à la ressource pour préciser l'emplacement de la ressource et, en particulier, le nom du répertoire et du fichier.

Au niveau de l'entreprise, les accès aux services *web* se font par l'accès à l'Intranet de l'entreprise ou encore par la navigation Internet.

⚠ La capacité du *webmaster* est d'une grande importance, il guidera le plus précisément possible les usagers dans leur navigation afin de leur **éviter de taper des adresses où des erreurs qui entraînent de mauvais usages**.

c) Le service de messagerie

Le service de messagerie, à la différence des services de messagerie instantanée, permet de réaliser une communication dite « *stop and wait* », adaptée au rythme de chacun. **Le service de messagerie majoritairement déployé dans les entreprises est celui de *Microsoft*** (environ 64 % en France). La solution logicielle libre, *Zimbra*, est également de plus en plus déployée dans les entreprises publiques.

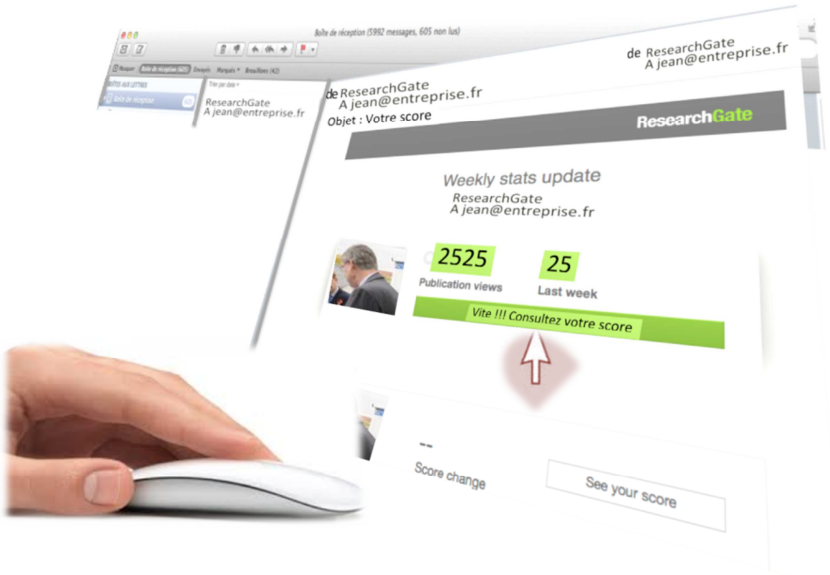
Un même client de messagerie peut configurer plusieurs messageries, y compris des messageries externes.

⚠ Cette capacité introduit des **éléments de la vie privée des collaborateurs dans l'entreprise** et inversement des **fuites des éléments de l'entreprise dans les messageries privées des collaborateurs**.

Le principe de la messagerie a fait de grands pas en avant depuis une décennie : transmission d'un message accompagné de pièces jointes présentes sous de multiples formats (des photos, des *URL*), afin de partager rapidement des avis, des conseils ou des émotions.

⚠ Ces caractéristiques ont révolutionné les pratiques. Néanmoins, elles entraînent de **nombreuses possibilités d'usages non souhaités**.

Schéma n° 51 : Interaction aisée entre les services : illustration de la messagerie et des services *web*



Source *: OPECST*

d) Le service d'annuaire

Le service d'annuaire répertorie l'ensemble des collaborateurs de l'entreprise afin d'associer certaines caractéristiques comme leur numéro de téléphone, leur fonction, etc. Ce service assimilé à un service « pages blanches » de l'annuaire de *La Poste* peut être couplé au service d'authentification de l'entreprise pour contrôler les accès aux ressources partagées. **Dans la plupart des entreprises, l'annuaire est celui de *MS Active Directory*.**

Du côté de l'usager, la structure globale du service d'annuaire ne lui apparaît pas directement ; il parvient difficilement à se représenter ce service, seuls les noms lui sont accessibles. Souvent, **l'usager ignore où sont stockés les noms des contacts de sa messagerie et de son annuaire** ; *a fortiori* si l'annuaire est géré par les administrateurs réseaux.

⚠ La connaissance des bases de l'annuaire représente une somme d'informations qui, exploitées de façon inventive, pourrait conduire à un **usage non souhaité**.

4. Les services applicatifs liés aux métiers de l'entreprise

Certaines applications non encore disponibles dans les environnements collaboratifs reposent sur des applications dites propriétaires.

De nombreuses applications ont bien souvent été développées pour les besoins spécifiques de telle ou telle entreprise. Ces développements sont assurés par des sociétés de service spécialisées dans leur domaine.

⚠ Les langages ainsi que les architectures ont répondu à un besoin exprimé à un moment donné par l'entreprise, mais pour certaines, les évolutions fulgurantes des technologies des systèmes d'information ont rendu ces **applications moins bien adaptées qu'elles ne l'étaient à l'origine**.

Pour d'autres entreprises, les développements ont été réalisés à bas coût et ont entraîné des failles qui ont pu être exploitées par la suite. En outre, les contraintes et la **lourdeur des développements** n'ont pas toujours permis leurs adaptations.

Afin d'éviter de tels écueils, les directions informatiques ont fait appel à des logiciels dits « intégrés ». C'est le cas notamment de logiciels *Enterprise Resource Planning* (*ERP*) intégrant la gestion des ventes, de la facturation, de la comptabilité, de la paie, des finances mais également de la production liée aux systèmes industriels. **Le marché actuel est partagé entre *SAP*, *ORACLE Application*, *Peoplesoft / JDE***.

Ce genre de logiciels est muni, dès sa conception, d'une multitude de fonctions.

⚠ Lors d'une phase coûteuse de mise en place répondant au mieux au besoin de l'entreprise, **des fonctions non utiles pour l'entreprise peuvent ne pas être désactivées**, par ignorance ou par négligence de l'expert. Or, **elles peuvent laisser la place à des usages non souhaités**.

« **Le monde de l'informatique industrielle et le monde de l'informatique générale sont de plus en plus connectés**. Quant à l'informatique industrielle et l'informatique embarquée, un exemple l'illustre : un *Airbus* a déjà sept points d'entrée : un lien lors des incidents logistiques, un lien avec l'usine ou avec *Air France*, un autre avec les passagers, un avec la police, etc. L'année prochaine votre voiture, votre réfrigérateur auront leurs entrées ; cela est irréversible. Donc, **le nombre d'entrées dans le système va se multiplier probablement par dix en moins de dix ans. Sans affoler les foules, c'est tout de même un sujet de préoccupation.**

L'Internet a représenté des progrès fantastiques de productivité et de croissance mais cela apporte aussi des vulnérabilités. C'est aussi une chance pour l'industrie de développer de nouveaux produits. C'est un monde qui est assez fragmenté entre des grands groupes très spécialisés et une myriade de PME fragiles et subcritiques qui n'ont pratiquement pas accès à l'export. C'est un domaine où on a beaucoup d'atouts mais aussi beaucoup de choses à faire ».

M. Hervé Guillou
Président, Conseil des industries de confiance et de sécurité (CICS)
26 février 2014
Auditions. Tome II du présent rapport

CHAPITRE V - LA SÉCURISATION DU SYSTÈME D'INFORMATION D'UNE ENTREPRISE

Comme décrit au chapitre III, pour l'échange humain et l'échange numérique, l'échange s'accompagne d'un objet, l'enjeu de l'échange : un bien ou un service, c'est, en tout premier lieu, une ressource précieuse. L'environnement présente de nombreux dangers qui conduisent chacun à mettre en place des mesures de protection. L'approche fondamentale de la sécurité en général développe des mesures de protection. Qu'en est-il pour la protection des systèmes d'information de l'entreprise ?

I. PRINCIPES DE SÉCURITÉ D'UN SYSTÈME D'INFORMATION

L'approche fondamentale de la sécurité consiste à concevoir les composants d'un système d'information en vue d'assurer et maintenir les propriétés de disponibilité, d'intégrité et de confidentialité (DIC).

A. D'UNE VISION STRATÉGIQUE À UNE VISION OPÉRATIONNELLE

Un modèle de défense est constitué d'**une triple vision** : **stratégique, organisationnelle et opérationnelle**.

- La vision stratégique élabore les **principes de défense** du système d'information. Elle repose sur plusieurs principes généraux afin d'assurer le maintien des objectifs de sécurité fixés.

Le premier principe recouvre tous les autres, il définit une politique de **globalité** dont la mission est la **surveillance des opérations de sécurité de manière uniforme dans l'espace et dans le temps**.

Le second principe est celui d'**unité** qui ne rend visible qu'**une seule autorité, une seule politique commune aux valeurs partagées** et ne laisse s'instaurer aucune division sémantique.

Le troisième principe définit un **périmètre de sécurité** de la force de défense ainsi que sa **présence permanente**.

Enfin, la division temporelle et spatiale nécessaire au déploiement de ces principes doit être assurée par une **décentralisation des forces de défense dans le respect du principe de globalité**.

• La vision organisationnelle met en place l'**organisation humaine** ; elle définit les responsabilités des personnes, les gouvernants de la sécurité, en vue du maintien de la sécurité.

Ces personnes doivent être choisies en fonction de **critères professionnels** établis afin d'assurer un respect sans condition de la loi. Leur rôle est l'anticipation des menaces et des événements dangereux, la planification de plans à dominante protectrice et préventive, l'application des plans et la conformité avec les lois et normes, la circulation des informations visant la défense du système, leur contrôle, la conduite des opérations de crises. Leur mission sera de veiller à écarter les dangers et, en particulier, d'**agir pour protéger les ressources vitales au système défendu** et prendre les mesures qui satisfont au mieux les besoins des usagers et leurs objectifs.

• La vision opérationnelle définit et applique des **tactiques**. La sécurité opérationnelle, enrichie de mécanismes de surveillance hébergés au sein d'un **centre de sécurité opérationnel** ou *Security Operations Center (SOC)*, permet d'accomplir au quotidien les activités de sécurité curatives mais également préventives à court terme. Elle incorpore la **gestion de la menace**, la **veille** et l'**analyse de vulnérabilités** ainsi que l'**investigation**.

B. LES TROIS PROPRIÉTÉS FONDAMENTALES DE L'ÉTAT DE SÉCURITÉ

Une propriété de sécurité caractérise la valeur d'un ou plusieurs états pour lesquels la sûreté de fonctionnement d'un système est satisfaite et en dehors desquels elle est défaillante.

Trois propriétés sont recherchées : la **disponibilité**, l'**intégrité** et la **confidentialité** plus connues sous l'acronyme DIC. Néanmoins, d'autres propriétés de sécurité peuvent être considérées à partir de ces trois propriétés de base, c'est le cas par exemple de la confidentialité (« *accountability* ») qui mémorise au sein de « journaux d'événements » les activités des usagers ou des machines.

• La disponibilité représente l'aptitude d'un système à ne pouvoir être employé que par des **personnes, entités ou processus habilités,** autorisés dans les conditions d'accès et d'usage normalement prévues par des administrateurs du système eux-mêmes habilités. Elle garantit le fonctionnement et ne le diffuse pas aux personnes, entités ou processus non autorisés ; elle a recours à des services de sécurité comme l'**authentification**, les **sauvegardes**, etc.

L'indisponibilité peut résulter d'atteintes majeures à l'intégrité du système, de défaillances de l'environnement technique ou humain contribuant à son fonctionnement.

La disponibilité se contrôle à partir de métriques définies par les personnes habilitées en fonction des habilitations des usagers. Par exemple,

la disponibilité d'un service est mesurée par le nombre de requêtes par seconde qu'il traite ; une atteinte à la disponibilité entraînera une diminution conséquente ou un arrêt total dans leur traitement. Il peut également s'agir d'un changement non autorisé des droits d'usages qui rend l'usage de ce service indisponible.

⚠ Les **vulnérabilités en déni de service** des équipements peuvent conduire à des attaques en déni de services. Dans les deux cas, **les requêtes ne sont plus à même d'être traitées**. Mais une attaque en déni de service peut également se produire par d'autres biais. Un arrêt d'un serveur après une panne électrique entraîne un déni de service.

• L'intégrité garantit que les savoirs, données, informations ou configurations n'ont **pas été modifiés par des personnes, entités ou processus non autorisés**, qu'ils ne le seront que par des personnes, entités ou processus habilités et que les données n'ont **pas été modifiées accidentellement ou intentionnellement sans autorisation**.

⚠ **La modification d'une donnée par un individu non autorisé peut appeler, en retour, des comportements non souhaités par les usagers légitimes mais souhaités par un attaquant à des fins de manipulation**. C'est le cas d'un courriel « suspect » forgé par un individu ; l'insertion d'une *URL* malicieuse en est une illustration.

Lors de la sécurisation d'un système d'information, ces exigences de sécurité conduisent à se poser plusieurs questions relatives :

- aux habilitations et à leurs liens avec les biens du système ;

- aux habilitations et à leurs liens avec les personnes, processus, entités ;

- aux habilitations et à leurs liens avec les activités autorisées : se connecter, lire un fichier, etc. ;

- à la gestion des historiques pour suivre les activités passées ;

- à l'identification et à l'évaluation des biens : savoir, donnée, configuration ;

- aux chaînes de liaison, également appelées dépendances, qui présentent des processus ou des acteurs humains susceptibles d'interagir avec d'autres.

• La confidentialité garantit qu'un savoir, une donnée, une information ou configuration ne sont **pas révélés à des personnes, entités ou processus non autorisés** mais le seront aux personnes, entités ou processus en fonction de leurs habilitations.

Les révélations de paquets *IP* constituent une atteinte à la confidentialité dans la mesure où une adresse *IP*, les informations contenues

dans ces paquets n'ont pas, par défaut, d'habilitation propre : l'usage d'une adresse *IP*, par exemple, n'est pas lié à une identité.

C. LES FONCTIONS DE SÉCURITÉ

La sécurité du système d'information repose sur plusieurs fonctions :

- la prévention comprend les politiques de sécurité pour spécifier les **conditions d'utilisation du système** ainsi qu'une **architecture de bastions** pour constituer une ligne de défense la plus robuste possible. Les experts et les architectes de sécurité en sont les acteurs clés ;

- la surveillance des systèmes met en œuvre des opérations de **détection** et d'**analyse** lors de violations de politiques de sécurité, émettant dans ce cas une **alarme** en vue d'informer l'analyste de sécurité ;

- l'analyse repose sur des raisonnements pour comprendre la source de l'écart de sécurité par rapport à la norme et définir s'il s'agit d'un incident ; la connaissance des chaînes de liaisons ou des dépendances entre processus et humains est une question essentielle ;

- la réaction, plutôt orientée vers la recherche de « symptômes », utilise les résultats issus de la détection et de l'analyse ; la décision constitue la phase clé pour **définir et organiser les contre-mesures, parades et actions de reconfiguration** ;

- l'investigation, plutôt tournée vers la recherche des causes de l'incident et sa remédiation ; cette étape permet de **reconstituer le mode opératoire pour remédier en profondeur à l'incident** – l'investigation permet également de reconstituer la scène et le mobile du criminel afin d'aider la justice dans la **collecte de preuves** nécessaires de l'existence d'un délit ou d'un crime ;

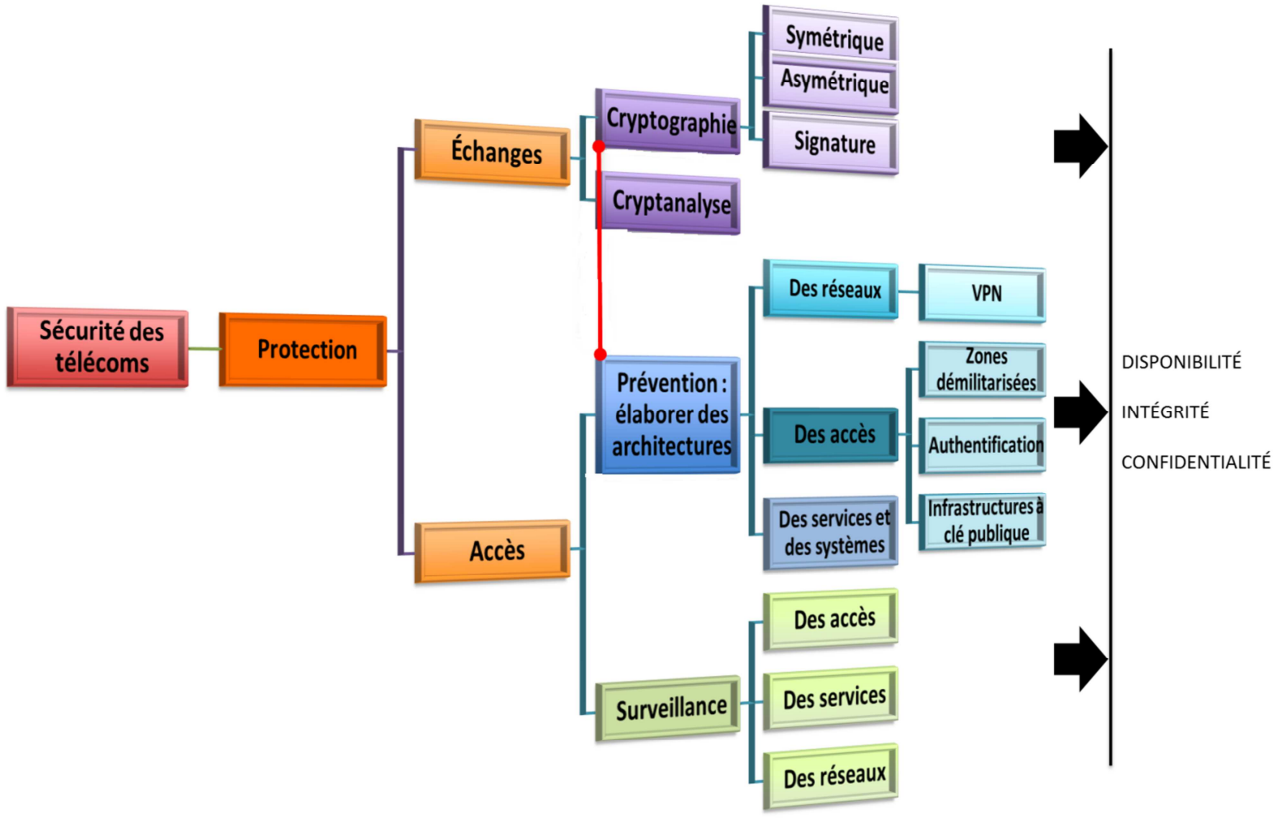
- la répression renforce les actes de la prévention ; elle est menée par des **acteurs judiciaires**.

D. ORGANISATION DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS

Dans ce contexte fortement dynamique, et afin de conserver la maîtrise des systèmes, les domaines technologiques de la sécurité des télécommunications sont variés et regroupent à la fois, pour la plupart, des techniques éprouvées et d'autres faisant l'objet de travaux de recherche afin d'anticiper les failles de sécurité.

Ces technologies visent **à assurer de manière drastique le maintien, à chaque maillon de la chaîne de sécurité, ses propriétés de disponibilité, d'intégrité et de confidentialité**. Afin de parvenir à surveiller un tel système, tous les mécanismes doivent être conçus en vue de fournir aux systèmes de surveillance la capacité de conserver la maîtrise de ces trois propriétés fondamentales.

Schéma n° 52 : Organisation de la sécurité des télécommunications orientée vers le maintien de la disponibilité, de l'intégrité et de la confidentialité



Source *: INSA*

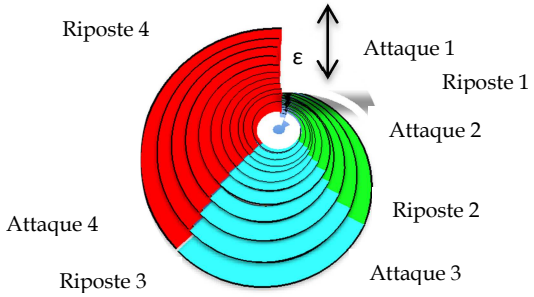
⚠ **Lors de la conception des biens et/ou services informatiques, l'absence de mécanismes de sécurité permettant d'alerter les administrateurs nuirait à leur supervision** et favoriserait les atteintes par surprise aux propriétés de disponibilité, d'intégrité et de confidentialité.

E. L'IMPÉRATIF D'AMÉLIORATION CONTINUE

L'échange ouvre de nouvelles opportunités pour l'évolution de l'entreprise mais l'expose par là-même à des attaques externes ou internes. L'entreprise évolue dans un rapport de force entre un système d'attaque et un système de défense.

Néanmoins, ce rapport est bien souvent inégal en matière de sécurité informatique car **les attaquants ont souvent « un coup d'avance »** et une connaissance accrue des systèmes d'information, si bien que **les changements d'états produits par le système d'attaque appellent de la part du système de défense un processus d'amélioration continue**. À chaque étape, l'amélioration représentée dans la figure ci-après par la lettre ε, garantit par une activité de reconfiguration permanente les propriétés de disponibilité, d'intégrité et de confidentialité du système jusqu'à la prochaine attaque.

Schéma n° 53 : Élévation continue du niveau de la sécurité du système d'information à protéger



Attaque 1 : **Copie illicite de fichiers** sur le répertoire du système de l'utilisateur par connexion depuis le poste du pirate Internet.
Riposte 1 : **Mise en place de règles de pare-feu** pour bloquer les connexions externes non souhaitées.

Attaque 2 : **Envoi d'un programme malveillant** sur le système de l'utilisateur : ce programme initialise une connexion vers le poste pirate pour une **copie illicite de fichiers**.
Riposte 2 : **Mise en place d'un antivirus** sur le système de l'utilisateur afin de détecter et d'éradiquer les programmes malveillants.

Attaque 3 **: Envoi d'un courriel piégé** à l'utilisateur par le pirate lui demandant de se connecter sur son site – ce qui permettra une copie automatique et illicite des fichiers de l'utilisateur.
Riposte 3 : Sensibilisé aux courriels malveillants, **l'utilisateur ne répond pas mais**, dans la mesure où un message d'erreur n'est pas retourné à l'attaquant, **l'adresse « courriel » de l'utilisateur est *ipso facto* confirmée.**

Attaque 4 : Le pirate forge un **courriel malicieux par ingénierie sociale** afin d'inciter l'utilisateur à ouvrir ce courriel par ignorance, réflexe, peur, etc. Bien que sensibilisé aux courriels malveillants, l'utilisateur, manipulé, exécute la demande du pirate.
Riposte 4 : L'utilisateur **cherche les moyens d'annuler l'action** qu'il a imprudemment déclenchée sur ordre d'un inconnu.

***Source** : OPECST*

Dans cet affrontement qui mêle des acteurs humains et cybernétiques, **l'inventivité semble caractériser l'humain**. ⚠ **C'est pourquoi l'introduction de machines dans cette spirale doit être maîtrisée, sinon, les risques de dérive pourraient entraîner une perte totale du contrôle du système d'information**.

« Nous pouvons penser qu'il s'agit là d'une utopie et que l'agresseur aura toujours une longueur d'avance.

Nous sommes actuellement confrontés à des problèmes simples : *primo*, on ne trouve que ce que l'on cherche ; *secundo*, lorsque l'on détecte une attaque, c'est que cette dernière a déjà réussi ; *tertio*, les équipements de détection d'attaque informatique ne sont pas souverains.

Il existe un État dominant en matière d'équipements de détection. **Il est donc nécessaire de développer à notre tour des outils de détection**, afin de faire face à d'éventuelles attaques venues de ce pays. Le Programme investissements d'avenir a mis à la disposition des équipementiers français les fonds nécessaires.»

M. Christian Daviot
Chargé de la stratégie auprès du directeur général, ANSSI
26 juin 2014
Auditions. Tome II du présent rapport

II. MISE EN ŒUVRE DE LA PRÉVENTION DANS LE SYSTÈME D'INFORMATION D'UNE ENTREPRISE

« Je vais partager avec vous ma vision d'ingénieur sur le *big data* et la sécurité. **Certains ajoutent la sécurité aux quatre piliers du futur cyberespace** que sont le *cloud*, la mobilité, les réseaux sociaux et le *big data*. M. Ross Anderson (Université de Cambridge, *Computer Laboratory*) résume ainsi la situation : « ***Les vainqueurs sont ceux qui, dans un premier temps, ignorent la sécurité au profit de la facilité, puis, dans un second temps, verrouillent leur écosystème numérique*** *plutôt que de nous protéger des méchants.*»

M. Philippe Wolf
Ingénieur général de l'armement
19 juin 2014
Auditions. Tome II du présent rapport

La phase de prévention n'est pas suffisante en matière de maîtrise d'un environnement technologique, néanmoins, elle s'avère indispensable dans la mesure où **la mise en œuvre d'une sécurité par conception est toujours supérieure**, ne serait-ce que pour en appréhender les risques et mettre en place leur surveillance par conception.

⚠ **À l'heure actuelle, la mise en place d'une surveillance par conception fait cruellement défaut dans les entreprises du fait d'un déploiement pragmatique massif des équipements numériques en leur sein depuis plusieurs années**.

La phase de prévention comprend la mise en place de politiques de sécurité pour spécifier les conditions d'utilisation du système, des architectures de bastions pour délimiter la ligne de défense du système et en

élaborer les mécanismes de contrôle d'accès pour qu'elle reste la plus robuste possible.

A. POLITIQUES DE SÉCURITÉ DE L'ÉTAT ET DES ENTREPRISES

Le modèle de défense nationale a été conçu par les gouvernements afin de protéger la nation des agresseurs externes et internes. Le code de la défense énonce le fondement du modèle de défense français en son article 1111-1 : « *La politique de défense a pour objet d'assurer l'intégrité du territoire et la protection de la population contre les agressions armées. Elle contribue à la lutte contre les dangers susceptibles de mettre en cause la sécurité nationale…* ».

C'est dans ce cadre que, récemment, la Politique de Sécurité des Systèmes d'Information de l'État (PSSIE), diffusée sous forme d'une circulaire du Premier ministre du 17 juillet **2014** a fixé les **règles de protection applicables aux systèmes d'information de l'État**. Ce texte est issu des travaux de l'ANSSI s'appuyant sur sa propre expérience en matière de prévention et de réaction aux attaques informatiques ainsi que sur celles de participants ministériels. **La PSSIE recommande le respect de dix principes**.

- Opérateurs de confiance sur le système d'information :

Lorsque la maîtrise de ses systèmes d'information l'exige, l'administration fait appel à des opérateurs et des prestataires de confiance.

- Analyse de risque :

Tout système d'information de l'État doit faire l'objet d'une analyse de risques permettant une **prise en compte préventive de sa sécurité**, adaptée aux enjeux du système considéré. Cette analyse s'inscrit dans une **démarche d'amélioration continue de la sécurité du système, pendant toute sa durée de vie**. Cette démarche doit également permettre de **maintenir à jour une cartographie précise des systèmes d'information en service**.

- Planification des ressources pour la sécurisation :

Les moyens humains et financiers consacrés à la sécurité des systèmes d'information de l'État doivent être **planifiés, quantifiés et identifiés** au sein des ressources globales des systèmes d'information.

- Authentification forte :

Des moyens d'authentification forte des agents de l'État sur les systèmes d'information doivent être mis en place. **L'usage d'une carte à puce doit être privilégié**.

« **La politique de sécurité des systèmes d'information de l'État (PSSIE) impose l'utilisation des moyens d'authentification forte (dont la carte à puce) dans le cas de données sensibles**, ce qui est plus sûr qu'un simple mot de passe. Il faut ensuite gérer tous les cas usuels et quotidiens de perte de la carte, ne pas l'oublier, penser à la récupérer etc. **Cette vraie contrainte doit être intégrée avec son coût initial et ses contraintes quotidiennes** d'absence de perte et de procédures à mettre en œuvre, notamment pour retrouver sa carte d'accès lorsqu'elle a été perdue.»

M. Thiébaut Meyer
Responsable de la sécurité des systèmes d'information, Présidence de la République
27 février 2014
Auditions. Tome II du présent rapport

- Surveillance :

Les opérations de gestion et d'administration des systèmes d'information de l'État doivent être **tracées et contrôlées**.

- Respect de la PSSIE dans la mise en place des mesures de protection :

La protection des systèmes d'information doit être assurée par **l'application rigoureuse de règles précises** qui font l'objet de la PSSIE.

- L'agent et le respect des règles :

Chaque agent de l'État, en tant qu'utilisateur d'un système d'information, doit être informé de ses **droits et devoirs** mais également **formé et sensibilisé à la cybersécurité**. Les mesures techniques mises en place par l'État dans ce domaine doivent être connues de tous.

- L'administrateur du système d'information et le respect des règles :

Les administrateurs des systèmes d'information doivent appliquer, après formation, les règles élémentaires d'**hygiène informatique**.

- Labellisation par l'ANSSI de produits informatiques :

Les produits et services acquis par les administrations et destinés à assurer la sécurité des systèmes d'information de l'État doivent faire l'objet d'une **évaluation** et d'une **attestation préalable** de leur niveau de sécurité, selon une procédure reconnue par l'ANSSI (labellisation).

- Localisation des données sensibles :

Les informations de l'administration considérées comme sensibles, en raison de leurs besoins en disponibilité, intégrité ou confidentialité, sont **hébergées sur le territoire national**.

B. MISE EN PLACE D'UNE ARCHITECTURE POUR LA SÉCURISATION DU SYSTÈME D'INFORMATION

L'architecture pour la sécurisation du système d'information d'une entreprise est conçue à partir d'une ligne de défense périmétrique dont le pare-feu est la pièce maîtresse complétée par des zones d'accès plus ou moins réglementées en fonction de la sensibilité des ressources à protéger.

1. La ligne de défense périmétrique traditionnelle

La mise en œuvre d'un modèle de défense repose sur une vision tactique qui consiste à élever une ligne de défense et à la protéger des agressions externes.

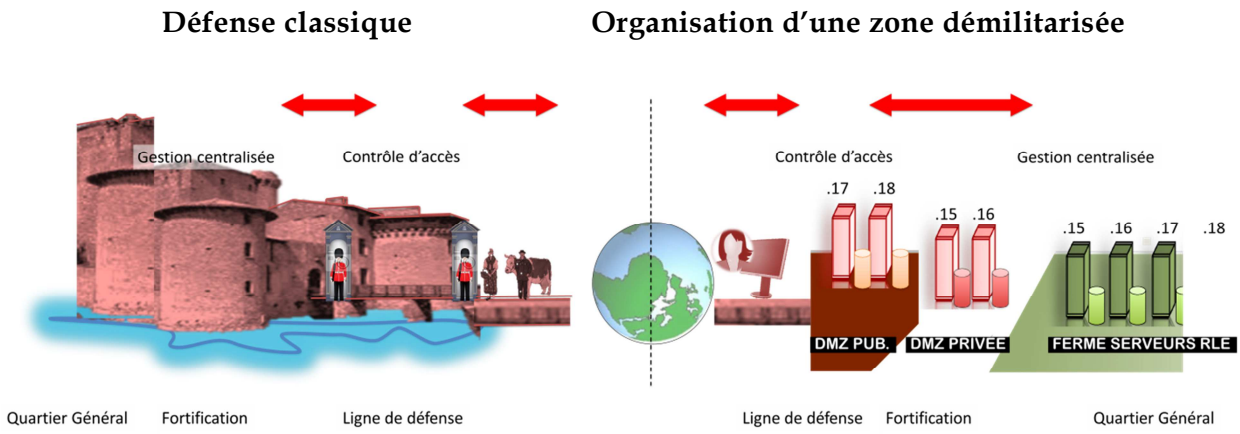
L'image périmétrique traditionnelle est celle des villes fortifiées dont la sécurité reposait sur des accès contrôlés concentrant les flux entrants et sortants ainsi qu'une surveillance continue en tout point : portes, fenêtres, remparts. Les vigiles sont placés sur des bastions déployés afin qu'ils soient reliés entre eux pour se surveiller et communiquer avec un code commun.

Une zone démilitarisée (*Demilitarized Zone – DMZ*) forge sa robustesse sur une **défense périmétrique** liée à l'implantation physique de ses composants. Elle est conçue pour analyser les flux réseaux entrants et sortants sur des canaux indépendants.

Le modèle de sécurité de l'échange numérique applique ces mêmes principes. Au sein d'un système d'information, **la ligne de défense est élaborée au travers d'une zone démilitarisée dont l'objectif est de concentrer les flux entrants et sortants du système d'information en un point unique**.

Le filtrage de ces flux est concentré en un point dont l'élément technique de base est le pare-feu (*firewall*).

Schéma n° 54 : Comparaison de modèles de défense



***Source** : OPECST*

2. Le pare-feu comme pièce maîtresse

La pièce maîtresse d'une zone démilitarisée (*DMZ*) est constituée d'un pare-feu. Entrant par le biais de l'accès *WAN (Wide Area Network)*, **chaque paquet fait l'objet d'une analyse fine** avant d'être autorisé au transit sur le système. Plus encore, **le pare-feu conserve en mémoire plusieurs paquets afin de valider leurs liens éventuellement suspects**.

Un pare-feu est utilisé principalement en coupure, en bordure du réseau privé d'entreprises et du réseau public. Il contient un ensemble de **règles prédéfinies permettant soit d'autoriser uniquement les communications ayant été explicitement autorisées soit d'empêcher les échanges qui ont été explicitement interdits**.

Le choix de l'une ou l'autre de ces méthodes dépend de la politique de sécurité adoptée par l'entité désirant mettre en œuvre un filtrage des communications. La première méthode est la plus sûre mais elle impose toutefois une définition précise et contraignante des besoins en termes de communication.

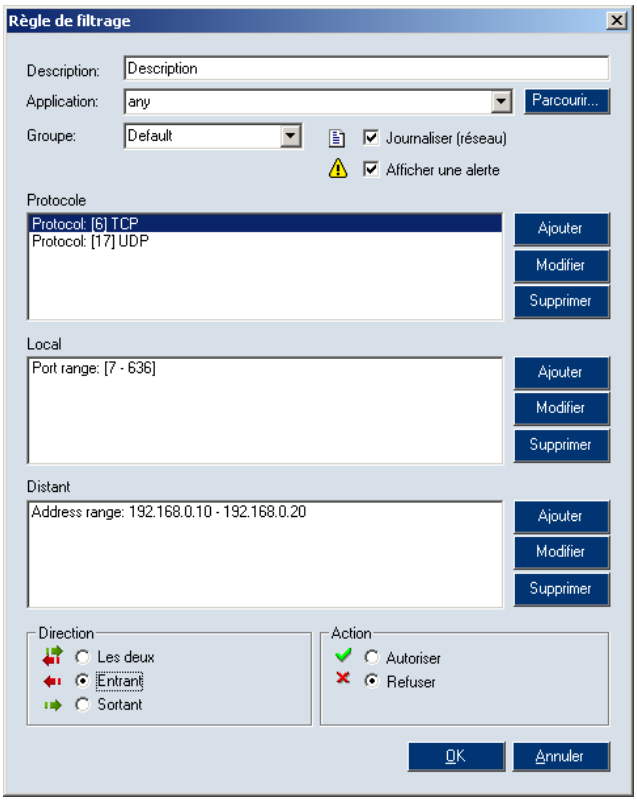
Un pare-feu emploie **deux types de filtrage : applicatif ou par paquets**. Les paquets contiennent des en-têtes : adresse *IP* source et destination, type de paquet (*TCP*, *UDP*, etc.), numéro de port, etc. Lorsqu'une machine externe se connecte à une machine du réseau local, et vice versa, le pare-feu analyse les en-têtes des flux échangés.

Lorsque le filtrage est fondé sur les adresses *IP*, on parle de filtrage par adresse, tandis que le terme de filtrage par protocole est utilisé lorsque le type de paquets et le port sont analysés. Cette fois, les flux d'application à application sont filtrés au niveau du contenu.

⚠ **Le pare-feu est un système performant dans la protection du réseau, sous réserve d'une administration quotidienne**.

Le schéma ci-après présente l'interface d'administration des règles de pare-feu.

Schéma n° 55 : Exemple du paramétrage d'une règle de pare-feu



***Source** : Internet*

3. Les zones d'accès selon la sensibilité des ressources

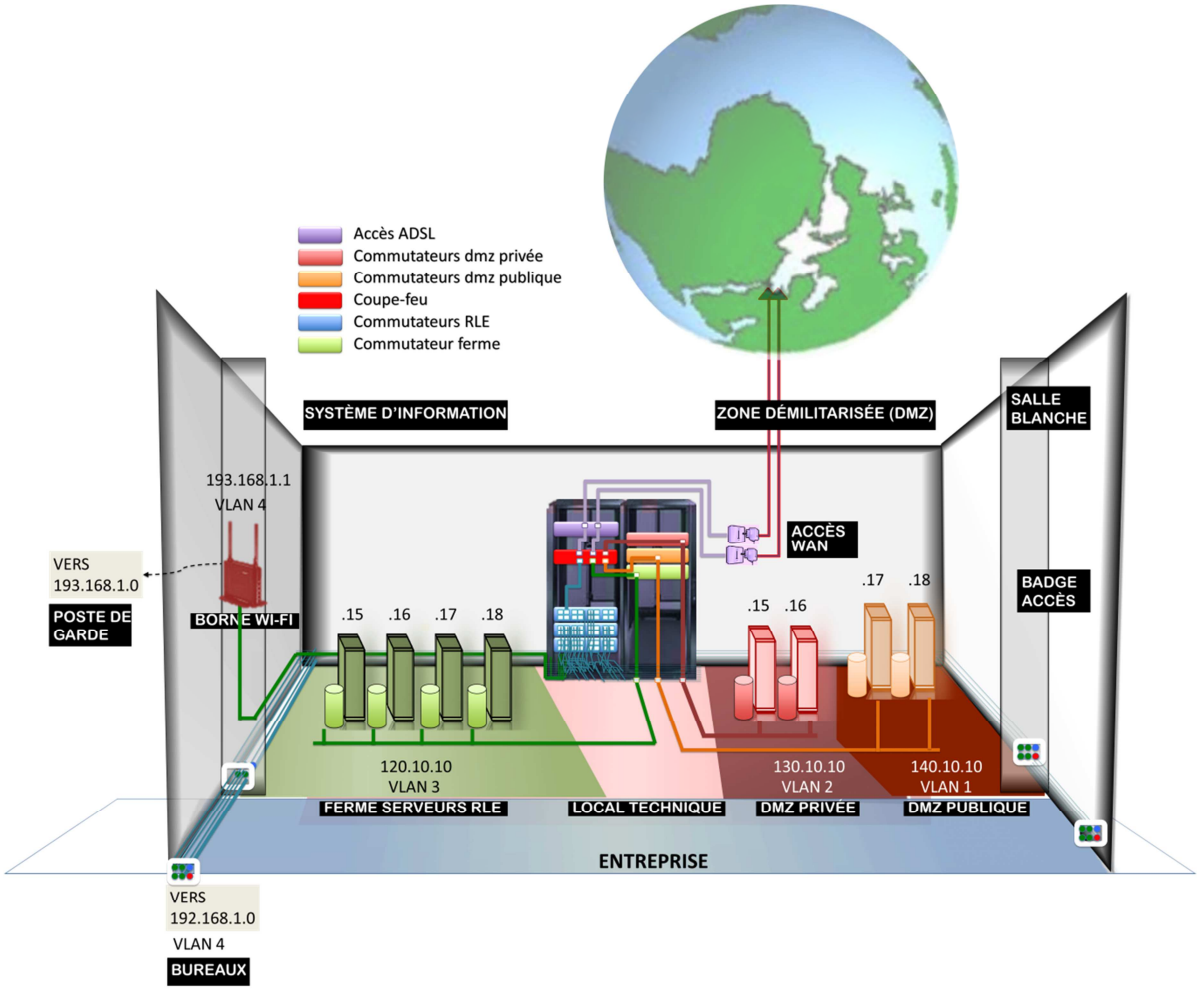
Afin de permettre de **déterminer un équilibre entre les besoins d'échanger et l'exposition aux menaces et vulnérabilités**, la zone d'interconnexion permet de définir **deux types de zones** :

- l'une plutôt ouverte aux internautes et potentiellement aux ennemis : les systèmes sont dits « **sacrifiables** », il s'agit de **serveurs accessibles au public** comme ceux du e-commerce ou *web* ou *FTP*. On y trouve également des données techniques pour le besoin de services comme les *DNS* et *SMTP* (*Simple Mail Transfer Protocol*) ;

- l'autre plutôt ouverte aux partenaires et potentiellement amis, hébergeant également des données communes et propres aux zones publiques et privées comme les certificats ou les serveurs d'authentification.

La première étape sera d'**effectuer un cloisonnement entre privé et public à chaque niveau : câblage, réseau, applicatif**. À des fins de surveillance, **des sondes** seront déployées sur les points stratégiques de la *DMZ*.

Schéma n° 56 : Architecture de sécurisation d'un système d'information



***Source** : OPECST*

⚠ Aujourd'hui, les gouvernants des systèmes d'information atteignent leurs limites puisque **l'énorme quantité des alertes émises par les sondes de surveillance sont transmises de manière désordonnée et engendrent l'impossibilité de surveiller**, c'est-à-dire d'interpréter le sens des multiples alertes émises par les sondes de surveillance.

4. Les antivirus

Un antivirus est **un logiciel sous forme de programme**, développé par un éditeur de logiciel, **qui analyse des flux systèmes, réseaux ou**

applicatifs. Il joue le rôle d'un filtre ; il extrait du flux le contenu **qu'il compare à des modèles de référence** qu'il connaît, plus connus sous le nom de signature.

Si les valeurs sont identiques cela signifie qu'il a trouvé un virus. Dans ce cas, l'antivirus stocke le fichier dans un espace spécifique appelé quarantaine et envoi une alerte à l'administrateur afin qu'il analyse par lui-même cette anomalie. L'administrateur prendra ensuite les mesures nécessaires.

Certains antivirus nécessitent d'être testés pour prouver leur capacité d'interception. Il existe des **sites d'autotest d'antivirus** mais cette fonction devrait intégrer les logiciels. De même, il devrait être possible de tester ces signatures

« **Un antivirus est là pour protéger mais il ne peut être infaillible. En revanche, ce système global sera au-dessus de toutes les strates d'information.**

Le contrat moral que DAVFI (Démonstrateurs d'antivirus français et internationaux) a avec l'État est de pouvoir **fournir un outil qui va bien plus loin que ce que font aujourd'hui les antivirus**. Nous sommes très bien partis pour y parvenir ; les résultats sont très encourageants. La première partie des modules, actuellement testée, permet déjà de faire beaucoup plus que ce que permettaient les antivirus actuels, en particulier sur les capacités de **détection de codes inconnus**, qui est le vrai défi technique et le vrai besoin opérationnel. »

M. Jérôme Notin
Président, NOV'IT
19 février 2014
Auditions. Tome II du présent rapport

C. CARACTÈRE DE L'AUTHENTIFICATION FORTE

De la signature avec l'empreinte du pouce, dans le commerce à Babylone, moins de 3 000 ans avant Jésus-Christ, aux premiers équipements de contrôle d'accès des années 1980, la notion d'identité et de reconnaissance est une notion humaine fondamentale. Plusieurs modèles ont été proposés dès les années 1970 pour aborder la mise en œuvre des principes de contrôle d'accès. Le modèle de contrôle d'accès de Bell Lapula (1975) est le modèle de référence encore utilisé aujourd'hui.

« **Le problème majeur est celui de l'authentification de l'interlocuteur.** Cela concerne aussi l'administration. Par exemple, quand le fisc notifie un redressement à un particulier, il y a des personnes qui vont vérifier s'il s'agit réellement du fisc mais d'autres non. L'origine de la messagerie électronique semble faire foi.

Le problème de l'authentification de celui qui vous parle, qui vous appelle ou de celui à qui vous voulez parler ou avec lequel vous souhaitez échanger, est un problème majeur. **Aujourd'hui, face à cela, nous sommes totalement sous-équipés. Pourtant, il y a de petites sociétés, françaises ou étrangères, qui ont mis au point des systèmes d'authentification performants. Au niveau national, il va falloir rechercher un système qui donne satisfaction à tout le monde et le mettre en place en l'imposant progressivement en commençant par l'administration.**

Pour les déclarations fiscales aujourd'hui, les formalités débutent par un certificat d'identification, suivi de l'entrée de plusieurs codes. Les services des impôts sont bien les seuls à prendre de telles précautions. Cela étant, si les services des impôts se font prendre, ils ne le diront jamais.

Dans les entreprises, il faut déjà mettre en place un système d'authentification interne pour vérifier si ce sont bien les employés, les clients et les sous-traitants de l'entreprise avec lesquels on entre en contact.

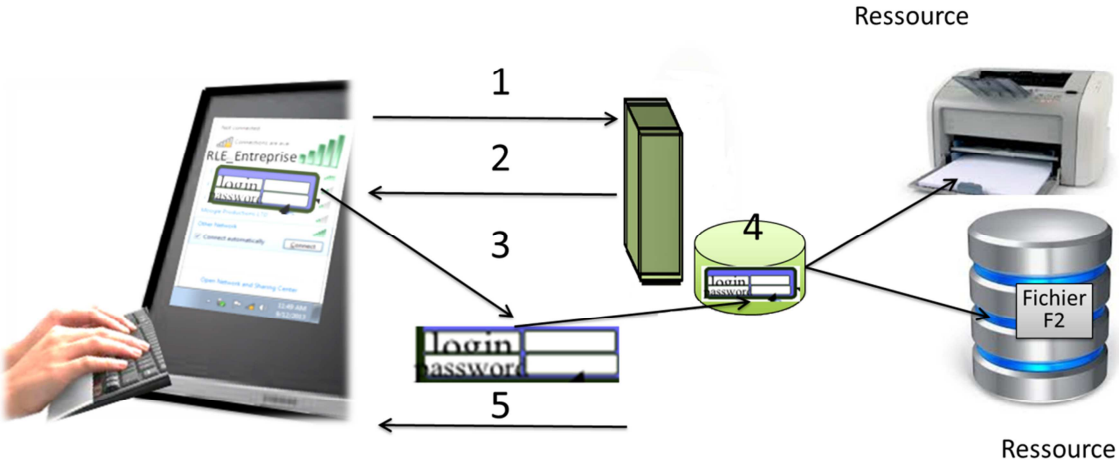
Les grandes entreprises sont également au cœur du problème avec des sous-traitants qui gravitent autour d'elles. Leurs systèmes de sécurité sont connectés avec celui de l'entreprise principale avec laquelle ils ont des échanges permanents, donc des interconnexions. **Si ces sous-traitants n'ont pas mis en place des systèmes de sécurité sérieux, ces sous-traitants vont constituer des lieux de passage pour les *hackers* cherchant à entrer dans le système principal.** Ce problème existe aussi pour toutes les petites PME et PMI qui travaillent dans l'orbite des grandes entreprises. »

M. Alain Juillet
Président, Club des directeurs de sécurité des entreprises (CDSE)
19 mars 2014
Auditions. Tome II du présent rapport

1. Le mécanisme d'authentification

<u>Le contrôle d'accès</u> est la pierre angulaire pour le maintien de la confidentialité. Lors de cette opération (schématisée ci-après), le client (1) contacte le serveur qui lui retourne une réponse appelée défi (2) en ce sens que le client doit prouver son identité en relevant ce défi (3) ; le serveur vérifie et accepte, ou non, l'accès (4) ; le client reçoit alors l'information recherchée (5).

Schéma n° 57 : Protocole d'authentification avec défi entre un client et un serveur pour le contrôle d'accès aux ressources réseaux



Source *: OPECST*

⚠ **Ce mécanisme d'authentification n'est pas suffisant pour garantir que les informations contenues n'ont pas été lues ou manipulées par un tiers**.

L'intégrité est le second volet développé dans les modèles de contrôle des flux. De nombreuses attaques visent la « captation des identifiants ».

Ces identifiants sont des éléments précieux qui constituent une condition clé en vue de la pénétration d'un système. Pour cette raison, les échanges 1, 2, 3 et 5 du schéma ci-dessus peuvent être chiffrés lors des opérations d'authentification pour élever le niveau de protection jusqu'à une plus grande robustesse.

⚠ De l'ingénierie sociale jusqu'aux attaques de l'homme dans le milieu, des écoutes passives d'un réseau à l'hameçonnage, des attaques par dictionnaire aux attaques par force brute, **l'authentification et, en particulier, les identifiants sont visés par une grande part des attaques informatiques**. C'est pourquoi **les processus pour la génération des identifiants, puis pour leur vérification, constituent les étapes probablement les plus sensibles**.

2. L'identification

Afin de vérifier les identifiants d'un client souhaitant accéder à des ressources dont il contrôle l'accès, un serveur d'authentification doit posséder des éléments de vérification des identités. Pour ce faire, le client et le serveur ont réalisé une étape commune préalable de **distribution du couple *login*/mot de passe**. Cette phase constitue l'identification.

Les protocoles d'identification visent à optimiser la phase d'exposition lors de la distribution et la vérification des identifiants puis à renforcer les éléments de preuves d'une identité.

Un mécanisme d'identification respectera plusieurs propriétés et plusieurs conditions afin de maximiser l'exposition.

a) Propriétés pour l'authentification de l'identification

Pour optimiser la phase de distribution et de vérification des identifiants, et éviter les attaques fondées sur une usurpation d'identité, **un protocole d'identification et d'authentification devra respecter plusieurs propriétés**.

La non-répudiation, proche de l'imputabilité, assure que **la source qui émet les données** ne peut pas contester leur émission ; elle **doit être identifiée et identifiable sans réserves**.

Le non-rejeu, ou non réutilisation de l'objet, garantit que les ressources telles que la mémoire centrale ou les zones de stockage sur disque peuvent être **réutilisées en préservant la sécurité**.

L'audit est la capacité à collecter des informations sur l'utilisation des ressources pour superviser ou adresser une **facture** à un utilisateur suivant sa consommation.

Une alarme garantit que les relations spécifiques entre différentes **données** sont maintenues et remontées **sans être altérées**.

b) Facteurs de complexité pour l'identification

La phase d'identification repose sur des éléments de preuve constitutifs d'une identité purement humaine. **Pour élaborer une identité numérique, il faut extraire des éléments de l'identité tels qu'ils soient uniques, évidents, non ambigus et authentifiables de façon sûre**.

C'est pourquoi cette étape favorisera les facteurs de preuve plus ou moins faibles ou forts élaborés à partir d'éléments d'identités humains de nature mémorielle, physique et/ou physiologique.

1. « Ce que je connais », qui représente un **élément mémoriel**, est un élément **faible** car il repose sur un élément du souvenir comme un mot de passe ou un instrument de musique préféré.

2. « Ce que je possède », qui représente un **élément matériel**, est un élément **fort** car il fait appel à une référence comme une carte d'identité ou une carte à puce avec un certificat.

3. « Ce que je montre », qui représente un **élément corporel**, est un élément **fort** car il fait appel à une référence physique comme une empreinte digitale, vocale, gestuelle, biométrique.

4. « Ce que je fais », qui représente une connaissance sur les **habitudes comportementales** comme un geste habituel ou une signature, est un élément **fort**.

En outre, **la combinaison de plusieurs de ces facteurs élève de façon importante leur complexité** en introduisant, par ce biais, un point dur face à des attaques en vol d'identité.

⚠ Au lieu de recourir à ces facteurs de preuve ou de les combiner, bien souvent, **la technique la plus déployée pour s'authentifier repose sur le *login*/mot de passe alors qu'il ne protège pas suffisamment les utilisateurs et/ou les processus**.

3. La gestion des identités

La gestion des identités est un processus clé de la sécurité de l'entreprise. Elle permet de regrouper l'ensemble des prérogatives d'un collaborateur sur le système d'information.

Tous les processus informatisés comme la messagerie, la gestion des ressources humaines, les affectations d'équipements informatiques pour les collaborateurs, sont regroupés en un point afin d'affecter des autorisations.

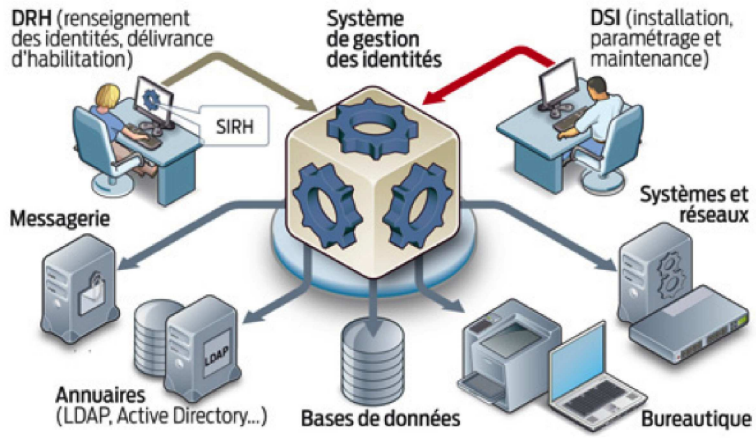
La gestion des identités permet également de remettre la gestion des collaborateurs sous la direction des ressources humaines alors que souvent elle se trouve encore sous la responsabilité de la direction informatique.

⚠ Néanmoins, la mise en place de cette fonction doit se déployer avec prudence afin de **ne pas omettre de bloquer ou d'autoriser certaines ressources**, ce qui pourrait entraîner des usages non souhaités du système d'information.

Afin de regrouper l'ensemble des utilisateurs d'une même entité, une base de données commune est constituée au sein de laquelle chaque utilisateur sera vu comme un objet. Afin de classer chacun d'entre eux, on utilise **un annuaire**. L'annuaire suit une organisation hiérarchique afin de s'adapter aux multiples formes de l'organisation de l'entreprise.

La norme la plus déployée est la **norme X.500** qui permet de définir une structure hiérarchique de l'annuaire.

Schéma n° 58 : La gestion des identités dans l'entreprise comme base fédératrice des informations des collaborateurs



Source : http://pro.01net.com/editorial/540500/la-gestion-des-identites/

4. Le protocole d'authentification

La **cryptographie** est utilisée pour diminuer l'exposition des identifiants lors de leurs transferts ; elle peut être combinée avec la **biométrie** pour renforcer la complexité des éléments de preuve.

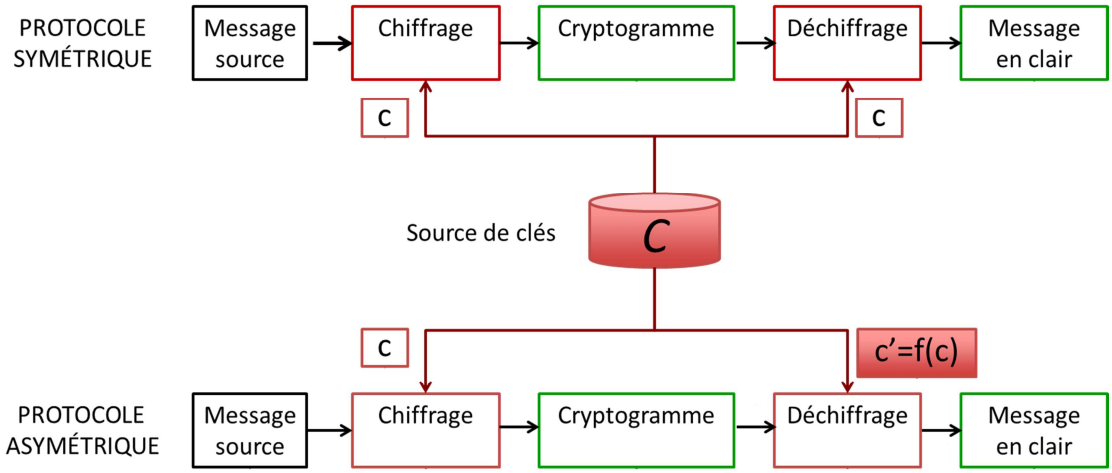
a) Principe cryptographique

Le principe d'un cryptosystème repose sur la transformation d'un message source en un cryptogramme à l'aide d'**une clé** tout en conservant certaines propriétés en vue de son déchiffrement. La clé est calculée à l'aide d'algorithmes et de fonctions mathématiques plus ou moins complexes ; dans le cas d'un cryptosystème asymétrique, les deux clés sont liées par une fonction mathématique.

Le premier protocole de **cryptographie asymétrique** permettant de distribuer une clé cryptographique *via* le réseau a été proposé par Diffie-Hellman en 1978 dans l'objectif d'authentification et non uniquement de protection pour le transport. Ce protocole permet de **générer des clés entre le serveur et le client sans transférer celles-ci *via* le réseau**. Il permet, en outre, de **créer un lien mathématique entre l'émetteur du message et le possesseur de la clé**, ce qui permet d'en assurer les propriétés de non-répudiation équivalant au principe d'accusé de réception employé pour garantir la source et le destinataire d'un courrier postal.

De plus, le protocole utilise **une paire de clés, dépendantes entre elles**, **chacune étant spécialisée** dans les opérations de chiffrement ou de déchiffrement, d'où la qualification d'asymétriques.

Schéma n° 59 : Comparaison d'un cryptosystème symétrique avec un cryptosystème asymétrique



***Source** : OPECST*

b) Chiffrement et clé

Transformer un message en cryptogramme n'est pas une fin mais une étape ; le processus de chiffrage vise un double objectif : **le chiffrage s'effectue dans le but de déchiffrer facilement tout en étant peu exposé pendant le transport**.

Pour rendre efficace le déchiffrement, **les opérations s'effectueront sur des flux binaires tant pour la clé que pour le message**. Le principe de base repose sur deux opérations : le *XOR* et la concaténation. Selon le principe de base suivant :

En algèbre de Boole, la fonction OU exclusif également appelée *XOR* (*eXclusive OR*, en anglais) est un opérateur logique. Une fonction *XOR* appliquée à son propre résultat permet de retrouver son résultat initial. Par exemple, la fonction « *XOR* 1 » appliquée à 0 donne 1, en appliquant « *XOR* 1 » sur 1, cela donne 0. La table de calcul ci-après exprime les règles booléennes de cette fonction.

Schéma n° 60 : Table de calcul de la fonction booléenne *XOR* (ou exclusif)

A	B	Out
0	0	0
0	1	1
1	0	1
1	1	0

***Source** : Internet*

Les fonctions cryptographiques transforment un message en flux binaire, procèdent à son découpage en blocs pour l'adapter à l'application d'algorithmes cryptographiques et appliquent des opérations de *XOR* avec la clé préétablie. Néanmoins, les algorithmes utilisent des fonctions de plus en plus complexes pour la transformation des clés et des flots de données.

Il faut chiffrer en combinant une clé binaire à un flux binaire tel que le protocole soit suffisamment complexe pour ne pas révéler tout ou partie des identifiants et suffisamment structuré pour le déchiffrement.

5. Les principaux protocoles d'authentification

a) Login/mot de passe

Le protocole ci-après présente un protocole d'authentification avec défi. Ce protocole est amplement déployé parce qu'il est simple à mettre en œuvre.

Dans le cas d'une ouverture de session *login*/mot de passe, l'utilisateur reçoit de la part du serveur une mire de « *login* » afin qu'il puisse entrer son nom et son mot de passe.

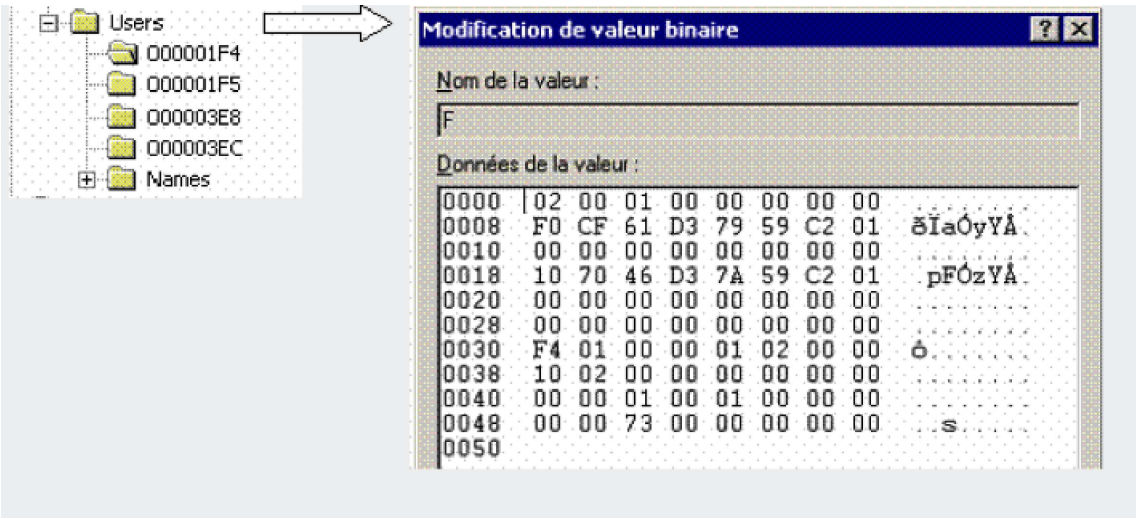
Schéma n° 61 : Mire de *login*/mot de passe



***Source** : Windows*

Afin d'en permettre le fonctionnement, le serveur est configuré au préalable pour qu'il puisse connaître les mots de passe correspondant à l'identifiant de l'utilisateur. **Un espace de stockage est réservé sur le serveur pour stocker l'ensemble des identifiants (*login* et mot de passe) de l'entreprise**. **Cet espace est particulièrement protégé et les mots de passe sont chiffrés** pour prévenir un accès illite sur ce serveur, rendant les identifiants illisibles comme le présente la figure ci-après :

Schéma n° 62 : Espace de stockage des *login*/mots de passe sur un serveur



***Source** : Windows*

Ainsi, le serveur ne connaît-il que la valeur chiffrée du mot de passe. **Au moment de l'authentification, le client chiffre le mot de passe**, d'une part, pour le garder confidentiel lors du transport et, d'autre part, pour que le serveur puisse le comparer à la valeur qu'il détient dans sa base.

En cas de succès de la comparaison entre la valeur chiffrée fournie par le client et la valeur chiffrée détenue par le serveur, l'authentification est prononcée.

b) One Time Password (OTP)

La technique de l'*OTP* a pour but de **n'utiliser un mot de passe qu'une seule fois, un autre mot de passe étant fourni à chaque session ultérieure**. Un premier déploiement est réalisé, il s'agit de la phase préalable de réglage, puis une carte matricielle détenue par le client permet de calculer le code au moment de l'ouverture de session (*login*). L'exemple ci-après présente une carte matricielle dynamique calculée par un terminal synchronisé avec le serveur d'authentification.

Ce principe, très déployé par les entreprises, garantit le chiffrement fort ainsi que la certitude que le serveur est authentique. ⚠ Néanmoins, il ne permet pas de garantir que l'utilisateur est légitime en cas de vol de la clé.

Schéma n° 63 : Technique du mot de passe à usage unique



***Source** : OPECST*

c) Certificat numérique

Un certificat numérique résout le problème de l'authenticité des acteurs d'un échange. Il repose pour ce faire sur un **cryptosystème asymétrique**.

(1) Principe d'un cryptosystème asymétrique

Ce principe, par conception, énonce que, étant donné deux clés dépendantes l'une de l'autre, **un message déchiffré avec l'une des deux clés prouve qu'il n'a pu être chiffré qu'avec sa clé complémentaire**.

Ces deux clés sont appelées respectivement : **clé publique** du fait qu'elle peut être publiée à tous et **clé privée** du fait que la sécurité complète du cryptosystème repose sur sa confidentialité.

L'avantage est que **le lien qui unit les deux clés repose sur une fonction mathématique complexe** (logarithmes discrets, factorisation de nombres premiers) à laquelle on associe la clé de chiffrement comme paramètre. Pour déduire la clé, l'attaquant devrait trouver l'une des solutions parmi un très grand nombre d'autant que les valeurs de clés seront générées à partir de très grands nombres premiers.

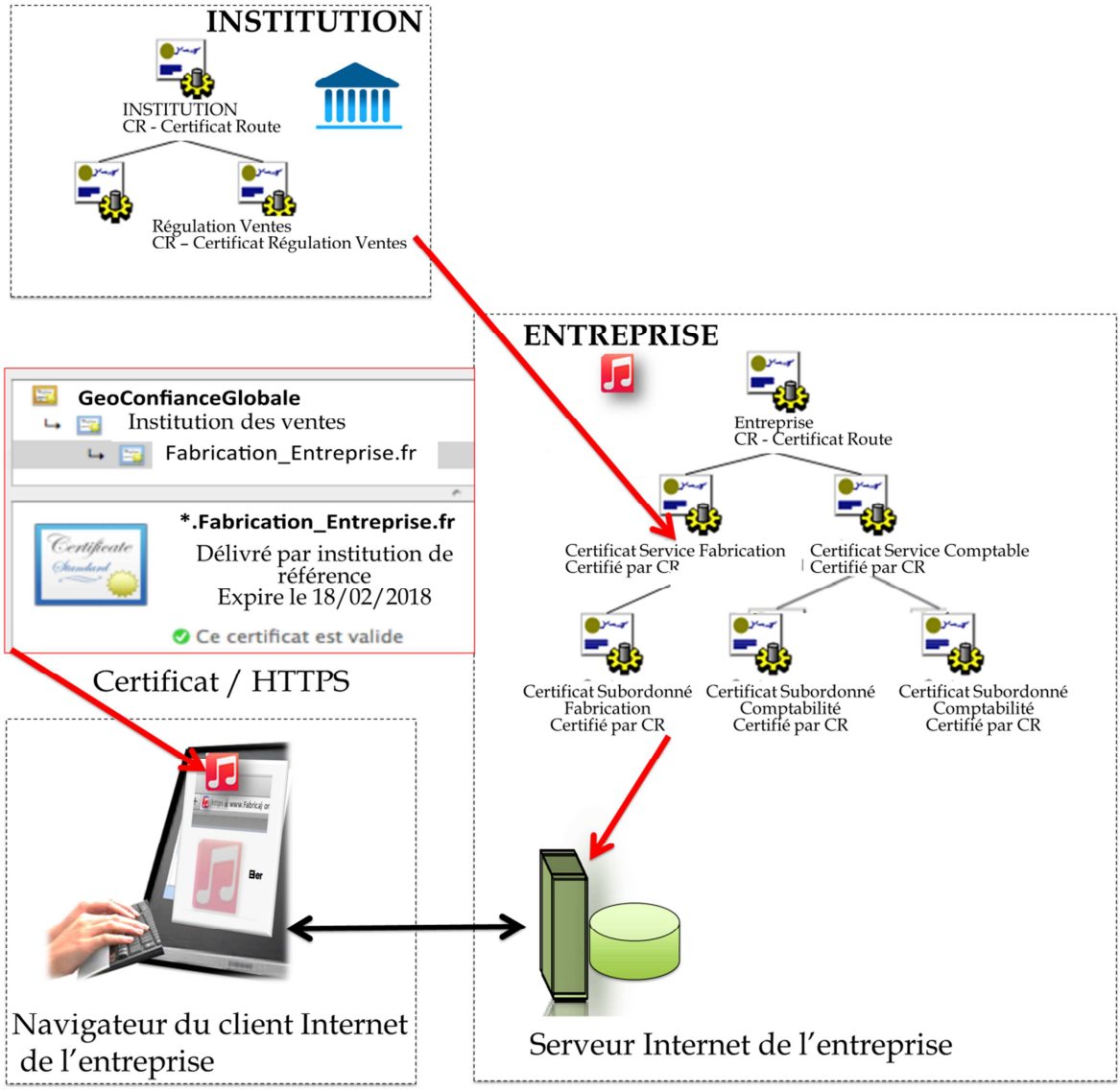
(2) Infrastructure à clé publique

⚠ La seule faiblesse est néanmoins d'assurer l'authenticité du certificat lors de sa génération. C'est dans ce but que l'on déploie des infrastructures complexes de certificats appelées *Public Key Infrastructures (PKI)*.

« Il convient d'identifier les technologies importantes pour la sécurité numérique des entreprises et de la nation, telles que **les *public key infrastructures (PKI)*** – qui sont des systèmes d'authentification ou de chiffrement –, afin d'**investir dans les offres les plus fiables** et d'**encourager leur production en France**. »

M. Ahmed Bennour
Directeur des systèmes d'information, Areva
26 juin 2014
Auditions. Tome II du présent rapport

Schéma n° 64 : Architecture à clé publique ou *PKI* d'une entreprise régulée par une institution



Source *: OPECST*

(3) Recours à une méthode à clé publique–clé privée avec signature pour la sécurisation des messages

Phase 1 : les outils de sécurisation des messages:

1- Anne-Yvonne et Bruno élaborent chacun une **clé privée** et une **clé publique.**
2- Anne-Yvonne et Bruno obtiennent chacun un **certificat** de leur **clé publique** auprès d'une **autorité de certification** – il peut s'agir de la même autorité ou de deux autorités différentes.
3- À partir de l'ordinateur de chacun, **plusieurs fonctions cryptographiques** peuvent être utilisées, c'est en particulier le cas **des fonctions de hachage**. On suppose qu'Anne-Yvonne et Bruno disposent des mêmes fonctions.

Phase 2 : l'échange des outils de sécurisation des messages

1- Anne-Yvonne adresse **sa clé publique** – qui peut se comparer à un cadenas ouvert dont seule Anne-Yvonne détient la clé privée – ainsi que **le certificat associé** à Bruno et inversement.
2- Chacun peut **contrôler le certificat** pour vérifier qu'il s'agit bien de la clé publique de l'autre.

Phase 3 : l'envoi d'un message sécurisé et de son empreinte

1- Anne-Yvonne **chiffre le message** qu'elle souhaite adresser à Bruno avec **la clé publique de Bruno** – le cadenas ouvert adressé par Bruno.
2- Anne-Yvonne **hache son message et signe** le résultat obtenu **avec sa clé privée** de façon à obtenir **une empreinte signée.**
3- Anne-Yvonne **adresse son message chiffré** et **l'empreinte signée** de ce message à Bruno.

Phase 4 : la réception du message sécurisé et de son empreinte, lecture et authentification

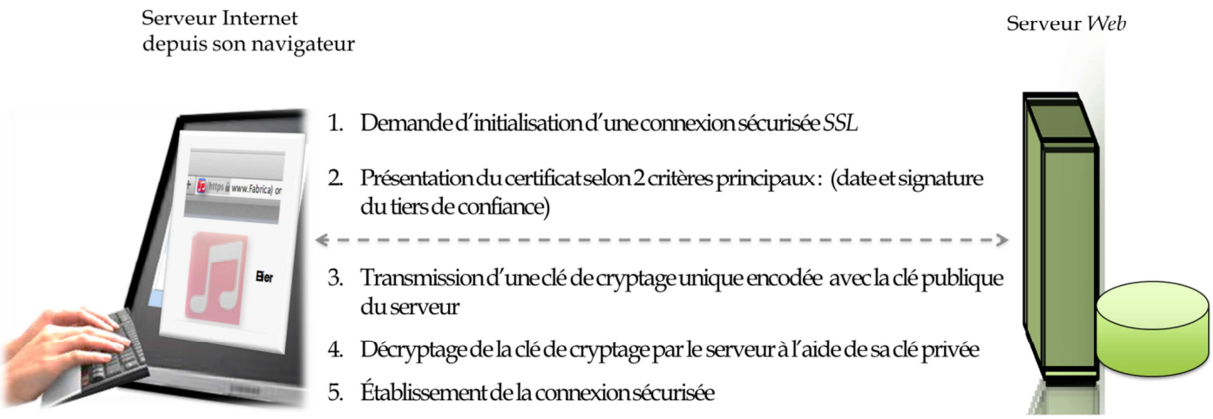
1- À la réception du message chiffré par Anne-Yvonne au moyen de la clé publique de Bruno, Bruno **déchiffre ce message avec sa clé privée.**
2- Bruno **hache le message** d'Anne-Yvonne pour obtenir **une empreinte.**

3- Bruno **compare l'empreinte** adressée par Anne-Yvonne à celle obtenue par lui pour vérifier leur similitude.
4- Pour avoir **la certitude** qu'il s'agit bien d'**un message d'Anne-Yvonne**, Bruno vérifie, avec **la clé publique** d'Anne-Yvonne, qu'il s'agit bien de la **signature d'Anne-Yvonne**.

(4) Application de l'utilisation d'un certificat aux services *web*

Ce principe permet de garantir l'authenticité du message puisqu'un message reçu et déchiffré avec une clé n'a pu être émis que par le détenteur de la clé complémentaire. Ce principe est utilisé dans les protocoles fondés sur les certificats. Le **protocole *SSL (Secure Sockets Layer)*** utilisé dans de nombreux mécanismes d'authentification sur Internet applique ce principe.

Schéma n° 65 : Garantie de l'authenticité d'un message au moyen d'un certificat



Source *: OPECST*

(5) Biométrie

La biométrie fait intervenir un facteur physique supplémentaire, rendant l'**authentification forte**. Généralement, la biométrie a recours à plusieurs méthodes de reconnaissance fondées sur une caractéristique ou un comportement unique : empreintes digitales, rétine, réseau veineux, voix, signature comportementale, ADN.

D. HABILITATIONS

Les habilitations concernent les droits que les utilisateurs obtiennent sur les ressources informatiques. Celles-ci sont de tous types allant d'un simple fichier à une imprimante ou un scanner.

Les ressources les plus sensibles, à savoir les données de l'entreprise, sont souvent mutualisées. L'intérêt des habilitations sera de permettre l'accès discrétionnaire à ces informations à l'aide de profils.

1. La définition des habilitations

Pour accorder les habilitations, l'administrateur définit des types de profils correspondant à des niveaux d'autorisations associant des ressources (biens) à des actions possibles comme la lecture, l'écriture, la modification, etc. Une fois ce profil défini, l'administrateur pourra associer le nom de l'utilisateur à ce profil.

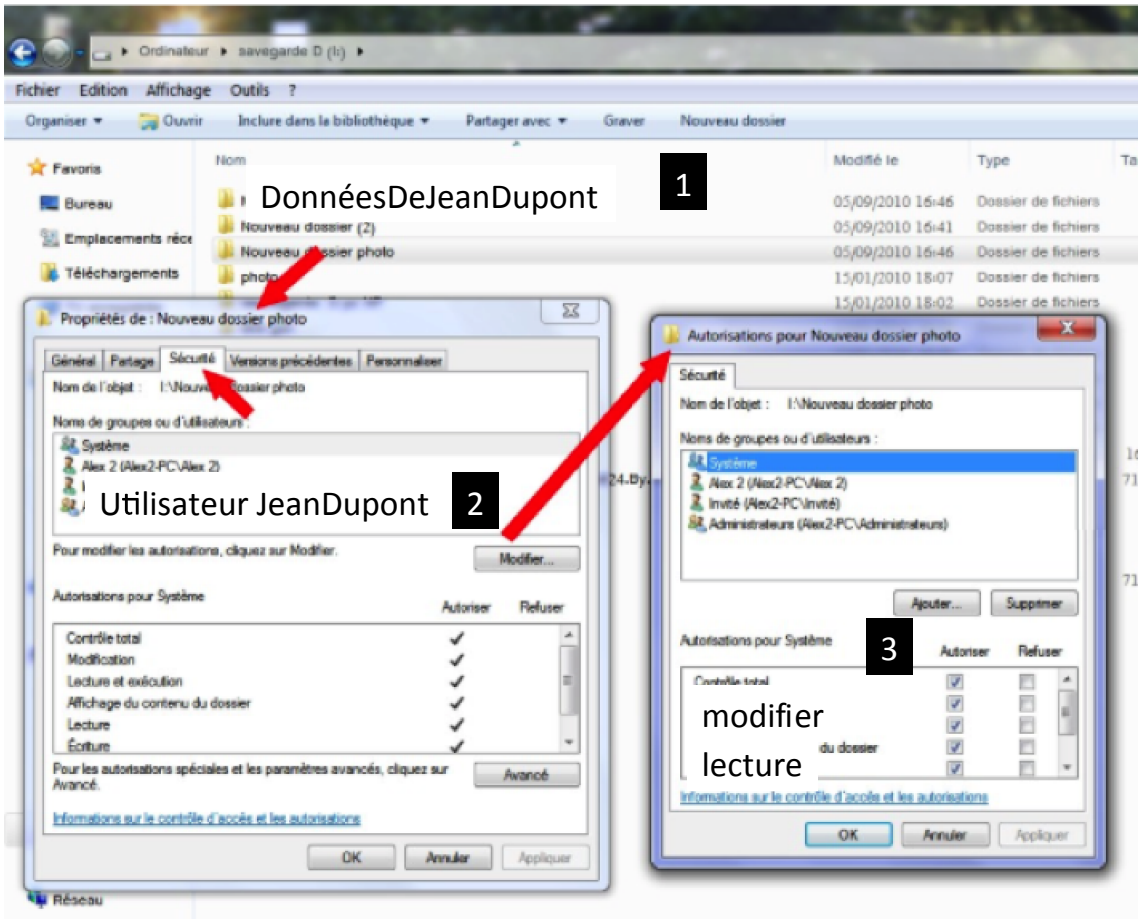
1. L'administrateur choisit la ressource à protéger ;

2. L'administrateur choisit l'utilisateur à habiliter au sein de l'annuaire de l'entreprise ;

3. L'administrateur définit les actions sur cette ressource que cet utilisateur aura le droit et la possibilité d'effectuer.

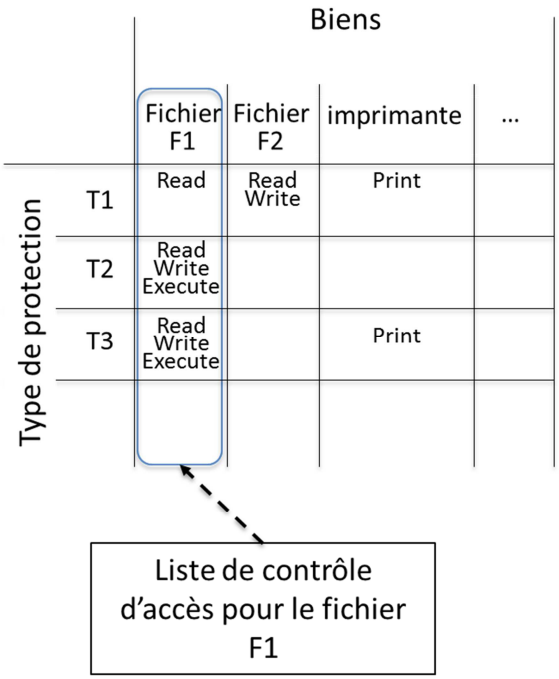
Lorsque l'utilisateur Jean Dupont se connecte, il accède à cette ressource.

Schéma° 66 : Utilisation de profils d'accès pour les habilitations



Source *: OPECST*

Schéma n° 67 : Exemple d'une grille de profil autorisation/ressources



***Source** : OPECST*

2. L'accès aux répertoires

Le principe des mécanismes d'autorisations repose sur les **protocoles d'authentification**. Une fois authentifié, le serveur affecte la ressource demandée à l'utilisateur : la ressource peut être une imprimante, un fichier ou un répertoire virtuel.

Il existe de multiples protocoles de gestion des autorisations au sein d'un réseau, propriétaires ou libres.

L'exemple ci-après détaille le protocole *Kerberos* et son architecture d'autorisation. Ce protocole est implanté par *Microsoft* dans son système d'annuaire et de gestion de fichiers *Active Directory*.

Les différentes étapes pour obtenir une ressource passent par une authentification classique (1-3) puis par une obtention des droits sous forme d'un ticket (4-5).

1 : accès au service *Kerberos* et authentification du client ;

2 : gain d'un ticket pour accéder au service de ticket ;

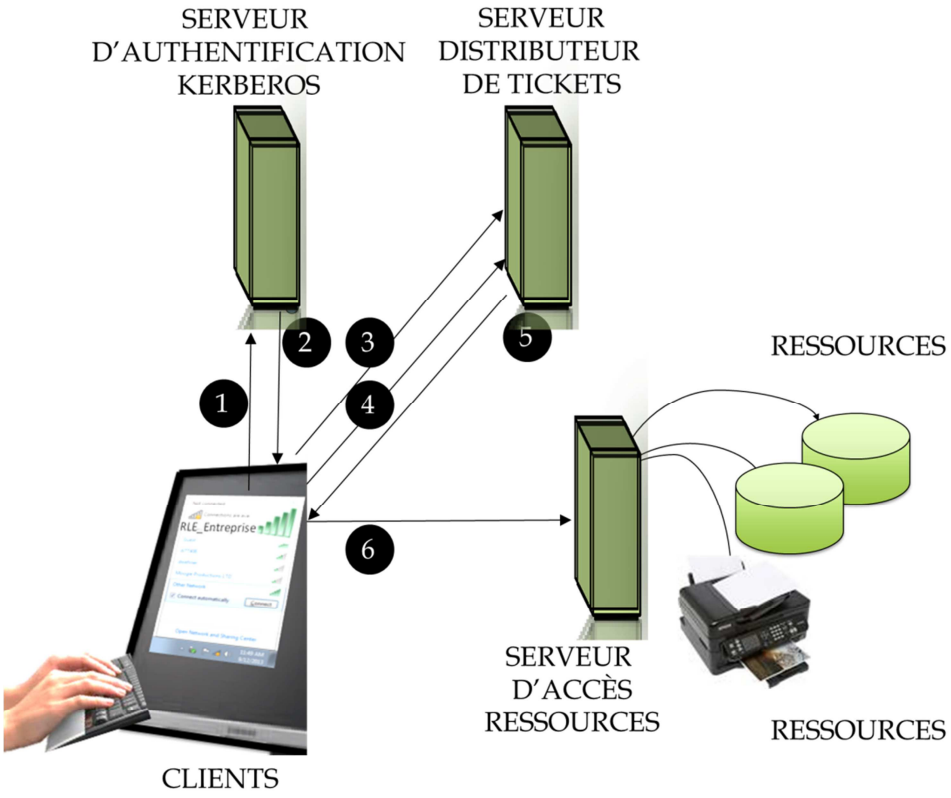
3 : authentification par le serveur de ticket ;

4 : demande d'accès au serveur de ressource ;

5 : gain d'un ticket d'accès au serveur de ressource ;

6 : accès autorisé au serveur de ressource.

Schéma n° 68 : Processus d'authentification *Kerberos* en vue de l'obtention d'habilitation sur des ressources partagées



***Source** : OPECST*

La navigation sur des ressources mutualisées est impossible du fait de la gestion des droits.

⚠ Néanmoins, une attention particulière doit être portée au quotidien à cette gestion car **une erreur de la part de l'administrateur pourrait entraîner des visites non souhaitées sur des répertoires sensibles**.

⚠ En outre, **l'administration de ce protocole est parfois difficile du fait d'usagers appartenant à plusieurs profils**.

Une cartographie des droits devrait aider l'administrateur à améliorer la consistance des habilitations.

E. ARCHITECTURES ET PROTOCOLES POUR DES TUNNELS D'INTERCONNEXION SÉCURISÉS

1. Les architectures pour des tunnels d'interconnexion sécurisés

Dans certaines situations, les données des entreprises doivent transiter *via* des réseaux étendus. L'attrait du coût d'Internet a amené les constructeurs et éditeurs de logiciels à proposer de nouveaux principes pour sécuriser les architectures.

Un réseau est dit virtuel lorsqu'il relie deux réseaux physiques d'entreprise (RLE) par une liaison tendant à être considérée comme privée : seuls les ordinateurs des réseaux locaux de part et d'autre du *VPN* peuvent échanger, se voir, accéder aux données partagées.

Dans le but de sécuriser les données transmises, il est nécessaire d'utiliser des protocoles de mise en place de tunnels sécurisés dits de *tunneling*, c'est-à-dire permettant de **créer une enveloppe opaque pour tous excepté pour ceux qui possèdent les habilitations pour l'emprunter**.

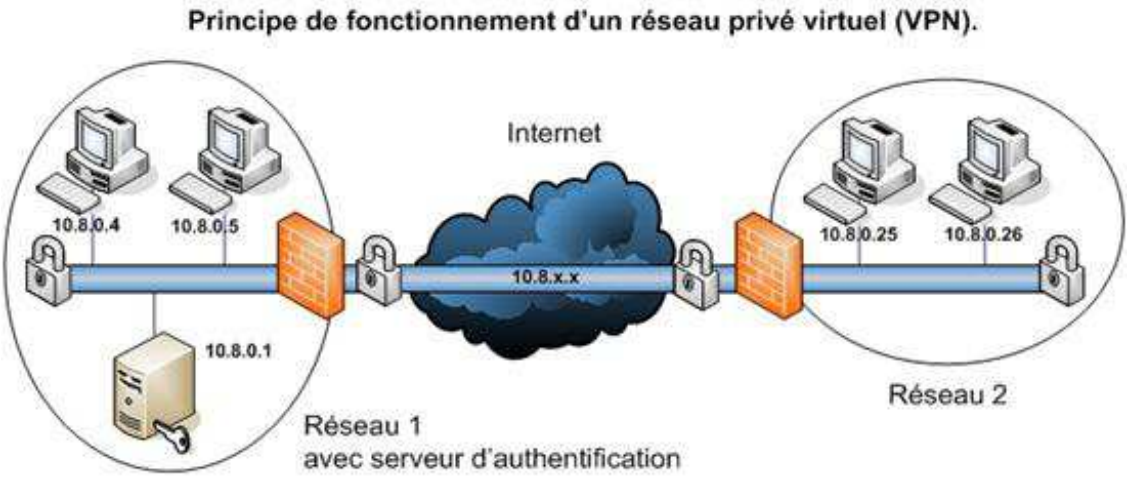
Le chiffrement est amplement utilisé pour créer un tunnel. On distingue les *VPN* de niveau 2 dont la quasi-totalité de l'en-tête de la trame est chiffrée (*Layer Two Tunneling Protocol L2TP*) des *VPN* de niveau 3 (*IPSec*), où les adresses sources et destinations peuvent circuler en clair, et de ceux de niveau 5 *(SSL : Secure Sockets Layer).*

Le réseau privé virtuel ou *Virtual Private Network (VPN)* représente aujourd'hui la technologie la plus employée et la plus robuste, en particulier lorsqu'elle s'accompagne de la certification des interlocuteurs, machines et usagers, *via* des certificats signés. Si le *VPN* permet d'obtenir une liaison sécurisée à moindre coût, en revanche, il ne permet pas d'assurer une qualité de service comparable à une ligne louée.

Le *VPN SSL*, utilisé pour les accès distants constitue une solution souple permettant un accès simple, rapide et sécurisé aux données du réseau d'entreprise, mais plus adapté à des **travailleurs en mobilité** (télétravailleurs, utilisateurs nomades, etc.).

À ce jour, le *VPN IPSec* reste **la solution la plus robuste et la plus agile** pour interconnecter des sites ou des réseaux distants. C'est la solution retenue dans le cadre du nuage numérique privé afin d'interconnecter le site du client avec celui de son hébergeur dans le nuage.

Schéma n° 69 : réseau privé virtuel (*Virtual Private Network*) entre deux sites distants



Sources : INSA Département Telecom – « Analyse et remédiation d'attaques sur un Cloud » PFE de Sara Alami Idrissi et Jose Antonio Carmona Gonzalez (2013)

Parmi les autres technologies permettant de relier des sites distants, les liaisons spécialisées constituent des liens non mutualisés, réservés à une entreprise, dont le coût est devenu dissuasif même si **leur principe de sécurisation est à ce jour le plus robuste**.

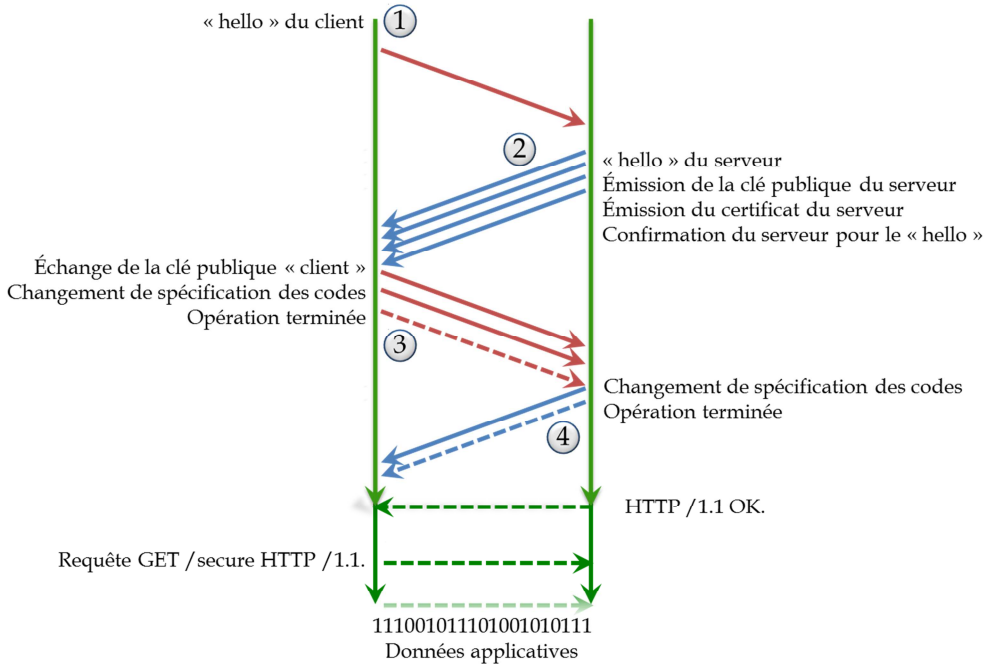
2. *SSL* : le maintien de la connexion sécurisée sur *TCP/IP*

Afin de véhiculer les données en dehors de l'entreprise de façon sécurisée, la mise en place de liaisons sécurisées constitue le moyen le plus employé.

L'idée est d'établir une relation unique entre la source et son destinataire à l'aide d'un **protocole « bout-en-bout »**.

Deux phases successives vont donc s'accomplir : d'abord l'établissement d'un **canal logique** entre la source et le destinataire rendu **hermétique** par le biais de protocoles de chiffrement ; puis le transfert de données chiffrées dans ce canal.

Schéma n° 70 : Maintien d'une connexion sécurisée sur *TCP/IP*



***Source** : OPECST*

« Les Allemands ont également pris l'initiative d'émettre leurs normes de sécurité. Ils ont recommandé que ce soit une norme nationale largement répandue. J'ai émis exactement la même idée auprès du ministère du redressement productif. J'aurais beaucoup apprécié que ce soit une norme européenne, mais il est possible de créer, ou en tout cas d'utiliser les normes existantes « adaptées », pour faire en sorte que ce soient des normes européennes ou nationales et qu'elles soient très sûres.

On sait, par exemple, qu'**il y a des failles très importantes dans le *SSL*, une norme massivement utilisée et que l'on continue malgré tout à utiliser**. Comme c'est une norme vieillissante, il a tendance à disparaître, mais c'est une norme percée qui continue à être utilisée. »

M. Gilles Babinet
Responsable des enjeux de l'économie numérique pour la France (*French Digital Champion*), Commission européenne
19 juin 2014
Auditions. Tome II du présent rapport

CHAPITRE VI – LES FAILLES ET LES ATTAQUES NUMÉRIQUES COMPROMETTANT LA SÉCURITÉ DES ENTREPRISES

Après avoir décrit le milieu hostile dans lequel évoluent les entreprises, pas toujours à même de concevoir leur sécurité numérique, incluant des vulnérabilités matérielles ou humaines et des attaques de natures différentes contre le système d'information des entreprises, vos rapporteurs ont choisi d'examiner plus particulièrement les attaques complexes et les attaquants chevronnés puis les moyens d'anticiper ces agressions et d'y faire face.

I. UN MILIEU HOSTILE

Au-delà des failles de sécurité inhérentes aux réseaux ou aux produits numériques utilisés et de l'exploitation de ces failles au cours de cette utilisation déjà mentionnée aux chapitres précédents, les quelques exemples ci-après, relevés dans l'actualité, montrent que ces failles peuvent être contenues dans des produits numériques très grands publics auxquels l'accoutumance a fini par donner un air familier, et donc une aura de sécurité parfois trompeuse.

La presse se fait de plus en plus l'écho de la découverte de failles de sécurité numériques significatives.

« *Comment éviter d'être victime sur le* web *de* ***la faille de sécurité «*** **Heartbleed** *». Touchant des sites populaires, ce* bug *nécessite de* ***changer ses mots de passe***. » Le Monde - 13-14 avril 2014.

« *Une faille de sécurité découverte dans le navigateur Internet de* Microsoft. ***Un défaut permettrait une exploitation à des fins malveillantes*** **d'Internet Explorer**. » Le Monde – 30 avril 2014.

Ces failles peuvent également exister au cœur des entreprises voire même des États.

« Lorsque **le ministère de l'économie et des finances a été attaqué** à la veille d'un sommet entre chefs d'État, il avait été jugé que cela n'était pas un sujet marginal même si aucun chiffrage n'avait pu être donné en termes d'impact.»

[...]

« **L'attaque par le virus *Stuxnext* contre les centrifugeuses du complexe militaro-industriel iranien a cassé la constitution d'une force nucléaire** ; de même, *Saudi Aramco* a eu 30 000 ordinateurs détruits. »

M. Jean-Marie Bockel
Sénateur, membre de la Commission des affaires étrangères, de la défense et des forces armées du Sénat
5 février 2014
Auditions. Tome II du présent rapport

Mais qu'est-ce au juste qu'une faille de sécurité numérique ? D'où peut-elle provenir ? Les développeurs de logiciels, les concepteurs de matériels et réseaux, ou les matériels et réseaux en eux-mêmes sont-ils seuls responsables ? Les usagers du numérique ont-ils leur part de responsabilité dans l'exploitation de ces failles ?

Comme l'enjeu de l'entreprise est de développer sa capacité à inventer et créer, par l'échange, l'entreprise apporte une réponse à ce défi ; elle crée de la richesse, produit, vend, communique, évolue. Néanmoins, ces enjeux sont également ceux de ses concurrents, voire de ses ennemis, des individus ou des organisations hostiles avec lesquels elle échange et contre lesquels elle devra lutter.

Au sein d'un tel écosystème où la technologie devrait être l'atout incontesté des entreprises, les aider dans leur décision, accélérer leur production, les guider dans leurs achats, porter leur image, assurer leur cohésion, le rôle que joue parfois la technologie est encore incertain. Qui la maîtrise ? Peut-elle devenir une menace sérieuse pour la productivité de l'entreprise ?

Qui sont les victimes ? Tous les acteurs des sphères sociétales mais également tous les acteurs de la sphère technologique. Des éditeurs de logiciels aux fabricants d'objets connectés, tous sont susceptibles de devenir des victimes.

Qui sont les gagnants ? Les cybercriminels ou les organisations en réseau, toujours plus ingénieux pour exploiter l'immaturité des technologies, développent leurs activités dans le cyberespace tandis que ces menaces entraînent également des gains énormes pour d'autres acteurs.

A. LES VULNÉRABILITÉS

Les uns les exploitent, les autres les subissent. Gagnants ou victimes, ils ont tous en commun leurs liens avec les vulnérabilités des systèmes numériques. La connaissance actuelle sur ces vulnérabilités est immense et la façon dont est organisée cette connaissance a été largement étudiée.

« La plupart du temps, on se rend compte que la conception des systèmes est suffisante en termes de sécurité, car de nombreuses attaques ne sont pas très « fortes ». Elles deviennent performantes dès lors que l'architecture d'ensemble n'a pas été bien pensée. **Il faut diffuser la culture de sécurité parmi les entreprises, et particulièrement les PME, qui présentent une vulnérabilité particulière.** »

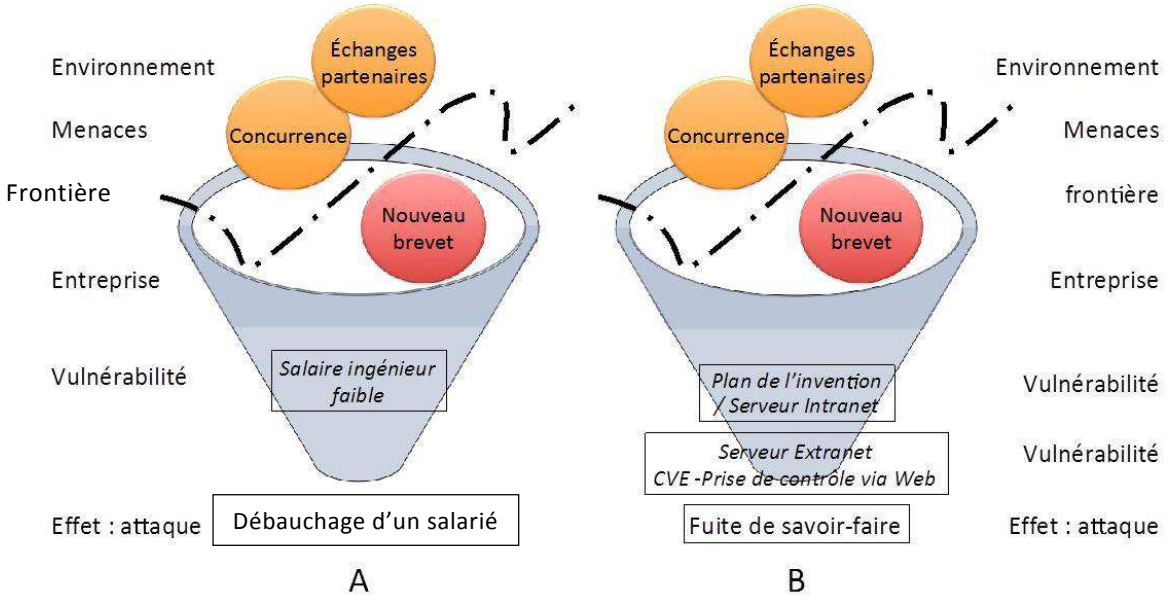
M. Jean-Luc Beylat,
***Président,* Pôle Systematic Paris-Région**
26 juin 2014
Auditions. Tome II du présent rapport

1. Les vulnérabilités et menaces

Une vulnérabilité caractérise un état défaillant accidentel ou intentionnel provoqué, lors de la conception, du développement ou encore durant les opérations d'exploitation du système d'information et susceptible d'être exploité par un individu malveillant. **La vulnérabilité est portée par la cible**.

La notion de vulnérabilité peut souvent entraîner des confusions avec celle de menace (*threat*). La vulnérabilité peut être considérée comme figée face au phénomène qui la révèle alors que **la menace est un état qui dépend du contexte dans lequel évolue la cible**. Ainsi, une faute de développement sur un logiciel est-elle une vulnérabilité alors qu'une faute de développement intentionnellement provoquée par un développeur concurrent sera une menace.

Schéma n° 71 : Comparaison du modèle entrepreneurial de risque complet menace / vulnérabilité / attaque avec le modèle numérique



***Source** : OPECST*

Le schéma ci-dessus présente un modèle de menace/vulnérabilité/attaque parmi la multitude qui existe, dont la nature dépend de nombreux paramètres. Autant la détection de menaces en nombre infini peut se révéler impossible, autant **la détection de vulnérabilités liées aux systèmes peut être structurée**.

Dans cette optique, l'identification des vulnérabilités repose sur un processus complexe d'analyse.

Les propriétés de sécurité reposent sur le maintien de la disponibilité, de l'intégrité et de la confidentialité. Une vulnérabilité sera évaluée en fonction de sa capacité à être exploitée par un individu malintentionné.

Par ailleurs, l'identification d'une vulnérabilité s'effectue bien souvent après un premier effet car **la découverte d'une vulnérabilité est longue, complexe, onéreuse et parfois liée au hasard**.

⚠ En outre, **une vulnérabilité peut avoir un effet local d'origine globale**. Par exemple, un sous-traitant est sollicité pour paramétrer un logiciel réputé fiable pour le compte d'une entreprise mais, lors de cette adaptation par le sous-traitant, une vulnérabilité inédite apparaît.

Enfin, certains acteurs pourraient trouver un intérêt à développer un climat de méfiance vis-à-vis de certaines technologies concurrentes des leurs, ou, au contraire, à masquer la présence de certaines vulnérabilités.

« **Il n'est pas rare de trouver des vulnérabilités suspectes qui ressemblent bien plus à des portes dérobées (*backdoors*) laissées volontairement.** C'est, par exemple, le cas d'un certain nombre de commandes cachées par les opérateurs (notamment *Huawei)*, qui permettent de réactiver ou de désactiver certaines fonctionnalités à distance. »

M. Badi Ibrahim,
Directeur des opérations, P1 Security
26 juin 2014
Auditions. Tome II du présent rapport

Pour toutes ces raisons, **la détection de vulnérabilités et leur diffusion doit être mutualisée voire effectuée par un service institutionnel**.

2. La veille comme processus d'analyse des vulnérabilités

Le principe de la veille est né aux États-Unis d'Amérique vers la fin des années 1980 à la suite d'incidents de sécurité informatique.

« Dans le cadre du projet 2Centre, les besoins en formation liés aux nouveaux métiers de la sécurité ont été recensés comme, par exemple, celui de **disposer de personnes qui vont intervenir sur les incidents, d'analystes également en charge de la veille, de testeurs d'intrusion** – pour trouver les failles avant les attaquants – et, également, d'ingénieurs en charge de la réponse aux incidents, pour les *CERT* – comme il y en a dans les grandes entreprises, comme, par exemple, les banques (la Société Générale, la Banque de France, ou autres). L'ANSSI envisage de recruter environ deux cents spécialistes de la sécurité tandis que les effectifs du Centre d'analyse de lutte informatique défensive (CALID) de la DGA, devraient passer de quarante à quatre-vingts personnes très prochainement.» En effet, **pourquoi attendre d'être attaqué ? Le centre de la DGA sert justement à repérer les failles avant d'être attaqué et à riposter**. »

M. Reza El Galai
Ingénieur projet cybersécurité, Conférence des directeurs des écoles françaises d'ingénieurs (CDEFI)
19 mars 2014
Auditions. Tome II du présent rapport

a) Les acteurs de la gestion des incidents

Dès cette époque, l'organisation de la gestion des incidents a été mise en place afin de **permettre un enrichissement communautaire des vulnérabilités des systèmes informatiques**.

Parmi les principaux acteurs et organismes qui ont déployé des efforts pour y parvenir doit être mentionné en premier le *National Institute of Standards and Technology* (*NIST*) accompagné du *Mitre*, organisme à but non lucratif concentré sur l'**identification mondiale des failles de sécurité**.

Depuis octobre 2014, le *Mitre*, proche du *Massachussetts Institute of Technology* (*MIT*), gère les listes de vulnérabilités pour le *NIST*. Le *Mitre* est historiquement une entité sans but lucratif ayant pour mission de fournir l'ingénierie technique pour le gouvernement nord-américain avec un focus sur les besoins de défense. **Avec le *NIST*, le *Mitre* aide les entreprises à sécuriser leurs infrastructures et données critiques en encourageant une collaboration public/privé pour identifier et résoudre les menaces complexes de la cybersécurité**.

De leur côté, les éditeurs de logiciels dont les développements sont à l'origine des failles s'emploient à corriger celles-ci.

Enfin, les *CERT/CC* (*Computer Emergency Response Team Coordination Center*), organismes spécialisés et agréés, **interviennent en urgence sur les incidents de sécurité informatique**.

Les *CERT* sont organisés et certifiés en vue d'accomplir les activités suivantes :

- centralisation des tickets d'incidents de sécurité sur les réseaux et les systèmes d'information ;

- analyse et traitement des incidents : solutions, échanges d'informations, études techniques ;

- enrichissement de la base de vulnérabilités ;

- diffusion d'information sur les mesures et les bonnes pratiques ;

- coordination des actions avec les autres acteurs impliqués dans l'incident.

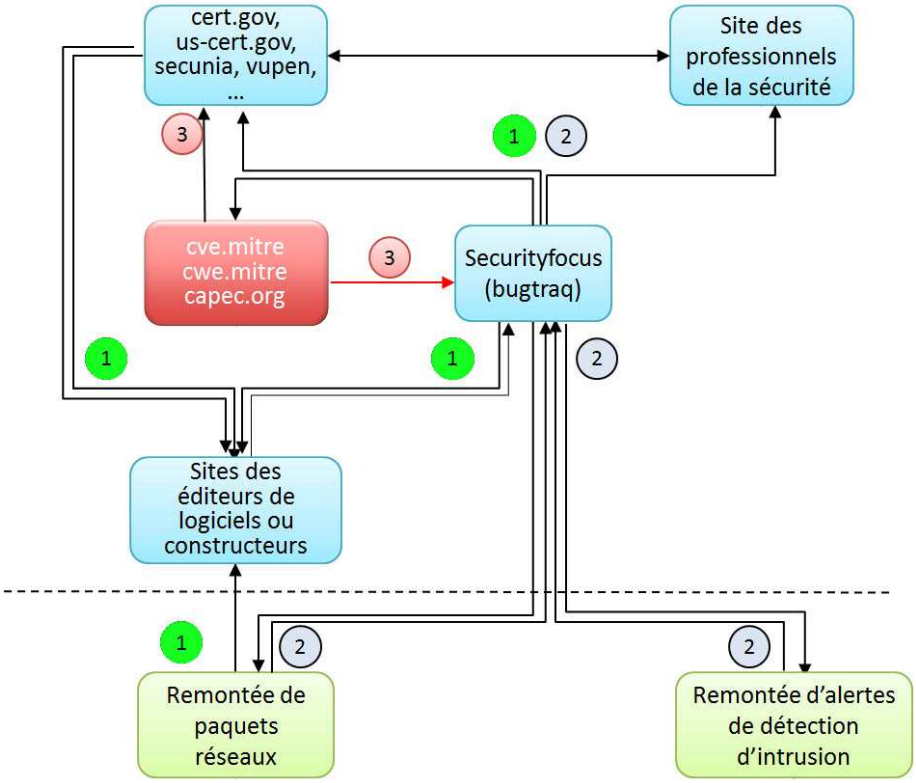
Les professionnels de la sécurité sont des utilisateurs des informations fournies par les *CERT* ;

Le site des « *bugtraq* » du « *SecurityFocus* » est destiné à la publication grand public des « *bugs* » et failles.

b) Processus d'enrichissement des connaissances

Le schéma ci-après présente le flux de traitement des vulnérabilités au sein de l'écosystème failles/attaques/correctifs.

Schéma n° 72 : Écosystème failles / attaques / correctifs



Source *: OPECST*

L'éditeur de logiciel ou le constructeur d'équipement détecte une faille à partir d'informations réseaux (1), puis analyse cette faille. Afin de permettre un déploiement à grande échelle, il diffuse également l'information auprès du *SecurityFocus* sous forme d'un **bulletin d'information** encore appelé *bugtraq*, il informe également les *CERT*.

À partir de cette étape, la **mise à jour du correctif** sera suivie par le *bugtraq*, comme le représente, dans le schéma ci-après, le champ « *update* ». Le *bugtraq* est transmis au *Mitre* symbolisé par la base de référence *CVE* afin d'associer un identifiant unique à cette faille**.**

Le *Mitre* détient de cette façon une liste exhaustive à l'échelle mondiale des vulnérabilités. Le *Mitre* énumère les vulnérabilités dans un format universel : (*CVE, Common Vulnerabilities and Exposures*), les référence et les diffuse vers les *CERT* et le site du *SecurityFocus* (3). Dans le schéma ci-après, dans la fiche de droite (3e ligne), le champ « *CVE* » représente ce genre d'identifiant.

Schéma n° 73 : Référencement d'une vulnérabilité *CERT-SecurityFocus*



***Source** : Internet*

La vulnérabilité une fois référencée, une relation s'instaure entre ces différents acteurs avec, au centre, l'éditeur de logiciel pour engager la correction de la vulnérabilité.

Dans le second scénario (2, dans le schéma de l'écosystème failles/attaques/correctifs), seul le point d'entrée change puisque le *bugtraq* est motivé par une alerte issue de « *logs* » de détection d'intrusion. Cela signifie que, dans le scénario 2, l'incident est un incident de sécurité.

Schéma n° 74 : Le *CERT–FR* valide la vulnérabilité découverte initialement



CERT-FR

uvernemental de veille, d'alerte et de réponse aux attaques informatiques

S . G . D . S . N
Agence nationale
de la sécurité des
systèmes d'information

Paris, le 09 décembre 2014
N° CERTFR-2014-AVI-512

aire suivie par :

RT-FR

AVIS DU CERT-FR

jet : Multiples vulnérabilités dans plusieurs produits DNS

STION DU DOCUMENT

Tableau 1: Gestion du document

Référence	CERTFR-2014-AVI-512
Titre	Multiples vulnérabilités dans plusieurs produits DNS
Date de la première version	09 décembre 2014
Date de la dernière version	-
Source(s)	Bulletin de sécurité PowerDNS du 08 décembre 2014
	Bulletin de sécurité unbound du 08 décembre 2014
	Bulletin de sécurité ISC du 08 décembre 2014
Pièce(s) jointe(s)	Aucune

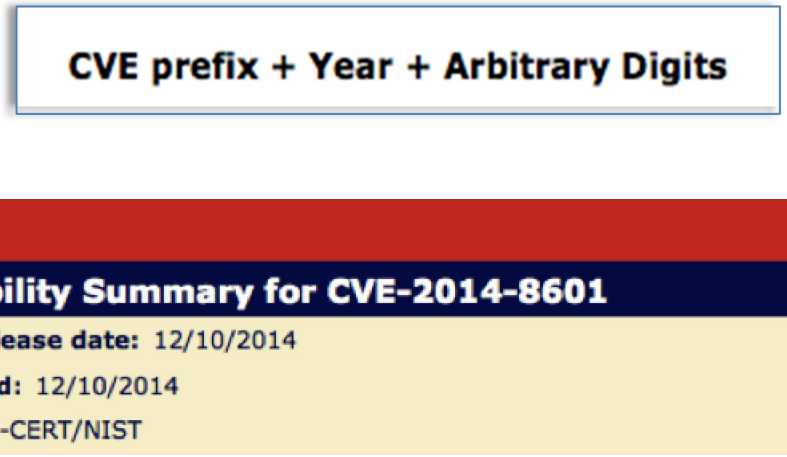
e gestion de version détaillée se trouve à la fin de ce document.

***Source** : CERT*

c) Identification des vulnérabilités

Dans sa mission globale, le *Mitre* est chargé d'attribuer les numéros d'identification des vulnérabilités. Le processus est celui d'un processus d'adressage au niveau mondial à l'aide d'une gestion centralisée. L'identifiant repose sur trois champs : le préfixe *CVE*, l'année, et un numéro d'ordre dans l'année.

Schéma n° 75 : Identifiant *CVE* à partir du site du *Mitre*

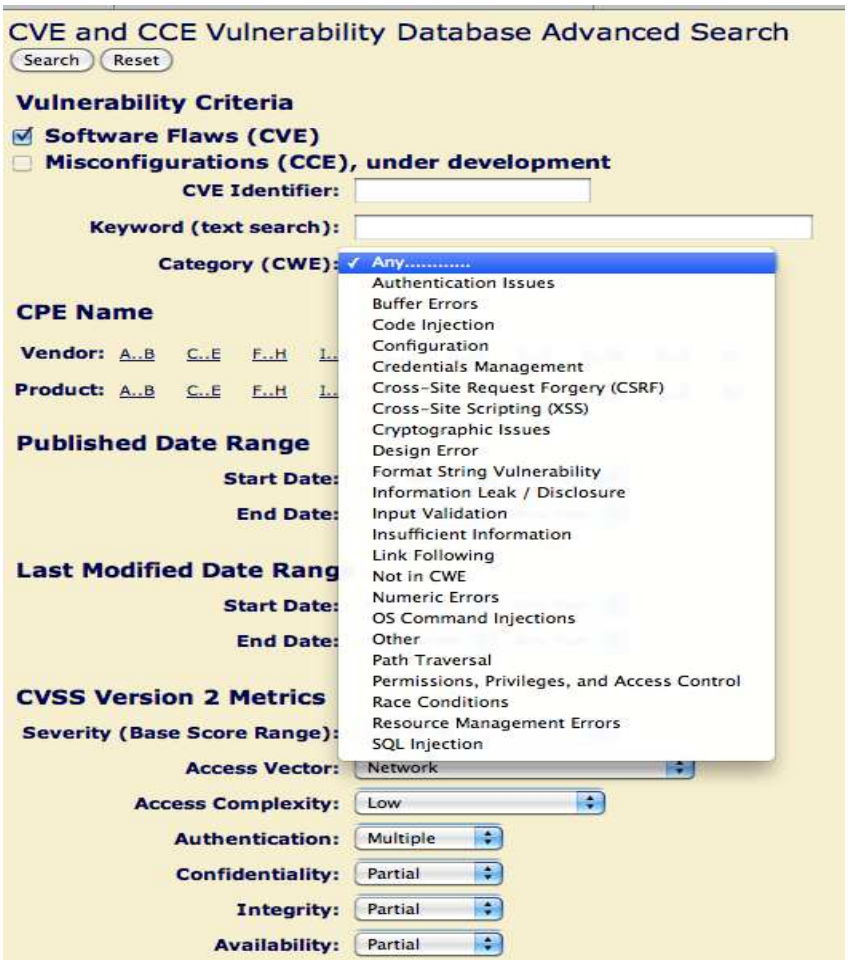


***Source** : MITRE*

d) Classification des vulnérabilités

Le référencement des vulnérabilités à l'échelle mondiale est l'atout des acteurs de la cybersécurité dans leur démarche défensive, tout du moins il le deviendra à condition d'en permettre leur exploitation.

Schéma n° 76 : présentation des classes de base d'une vulnérabilité



***Source** : CERT*

Depuis plusieurs décennies, ces acteurs, le *Mitre*, le *NIST*, *SecurityFocus*, se sont penchés sur la question des vulnérabilités ; de nombreuses classifications ont émergé. Actuellement, comme le présente la page du site du *Mitre* ci-dessus, on dénombre **plus de vingt-trois classes de base pour décrire les vulnérabilités**. En particulier, la classe *Cross-Site Scripting* (XSS, à la huitième ligne de la liste figurant dans le schéma ci-dessus) à l'origine de nombreuses attaques.

Cette classification évolue ; dernièrement, le *NIST* a proposé un nouvel identifiant *CVE* avec de nouvelles classes et prépare par ailleurs une classification destinée à la gestion des activités au sein d'un centre d'informatique en nuage.

3. La vulnérabilité dite « *zero-day* », à corriger en zéro jour

Une vulnérabilité *zero-day* est une vulnérabilité nouvelle, découverte à l'occasion de son exploitation par un attaquant. Elle est

souvent présente dans un logiciel et est généralement liée à une erreur de programmation simple, mais elle peut également se révéler dans un système ou un équipement.

Elle se nomme *zero-day* parce que la correction logicielle de la vulnérabilité n'est pas disponible ou n'a pas pu encore être testée pour son application au moment où elle est découverte. **Le développeur en charge du correctif possède le minimum de temps, soit zéro jour, afin de proposer au plus vite aux usagers une solution fiable** et enrayer la propagation de l'attaque. Jusqu'à l'introduction du correctif, la vulnérabilité sera dite *zero-day*.

Lorsque le scénario 1 du schéma ci-dessus intitulé « écosystème failles/attaques/correctifs », est utilisé, pour de multiples raisons, il est possible de ne pas révéler la faille, la vulnérabilité dite *zero-day*.

Comme toujours, une faille de sécurité suscite également de nouvelles formes d'exploitation, on parle de nouveaux modèles d'affaires. La découverte d'une vulnérabilité peut se monnayer auprès de gouvernements souhaitant mener une cyberguerre ou d'organisations animées d'intentions malveillantes. En effet, une faille non publique qui ne sera pas corrigée par l'éditeur de logiciel ou le programmeur, n'en aura qu'un effet plus fort. Cela a été le cas du fameux virus *Stuxnet* par exemple, *a priori* développé conjointement par les États-Unis d'Amérique et Israël, ou encore *Aurora* qui ont développé quatre vulnérabilités *zero-day* pour pénétrer les systèmes.

⚠ Si une faille informatique n'est pas publiée, ou connue du grand public, et donc non corrigée par l'éditeur du logiciel visé, le pirate ou *hacker* qui compte exploiter la faille bénéficie d'un **effet de surprise total** : il peut alors prendre le contrôle d'un ordinateur, d'un logiciel ou d'un réseau, voire effectuer une attaque par déni de service, sans que la structure visée n'ait eu le temps de s'y préparer.

B. ANALYSE GLOBALE DES RISQUES DANS LES ÉCHANGES NUMÉRIQUES

La conjonction des failles et des menaces peut entraîner des conséquences considérables sur les systèmes d'information des entreprises. Lors de leurs échanges numériques, les interlocuteurs s'exposent, mettant en jeu la disponibilité, l'intégrité et la confidentialité des objets et/ou des interlocuteurs pendant leur transport. Pour cette raison, **les faiblesses portent sur les points d'entrée et de sortie des systèmes de transport ainsi que sur les personnes qui les utilisent**.

Le principe de l'analyse de risques consiste à **regrouper les éléments d'évaluation en vue de mieux contrôler ces faiblesses et de rendre les**

activités d'une entreprise les plus sûres possible, sachant que la sécurité complète ne peut être garantie.

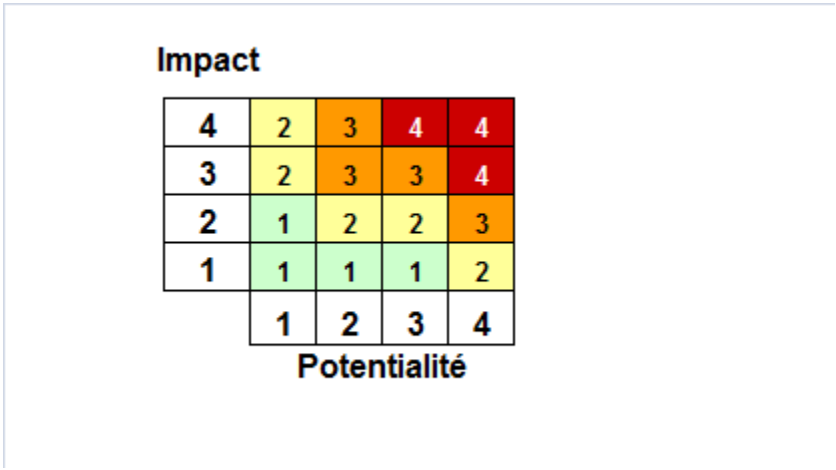
L'évaluation de cet état le plus sûr possible repose donc sur deux éléments clés :

- la potentialité d'un incident qui se mesure généralement par l'historique de faits similaires survenus ou l'exposition particulière d'un élément du système d'information.

- l'impact d'un incident qui se mesure généralement à l'aide d'une évaluation financière.

Le schéma ci-après représente la règle de décision pour un événement. Un impact de niveau 4 et une potentialité de niveau 4 entraînent un risque de niveau 4 pour l'entreprise : celle-ci s'engage à le traiter alors qu'un incident rare mais d'impact élevé ne représentera qu'une priorité de niveau 2 dans le traitement du risque.

Schéma n° 77 : Règle de décision pour le traitement d'un risque pour une entreprise



***Source** : Méhari – CLUSIF*

Néanmoins, si l'emploi de méthodes d'analyse de risque reste un atout considérable pour obtenir une connaissance objective de l'environnement d'une entreprise, ce processus est lourd face aux besoins d'agilité des entreprises pour assurer leur sécurité au quotidien.

1. L'identification des éléments pour l'analyse des risques

Pour mener cette analyse, les différents niveaux de l'entreprise doivent être étudiés.

Chaque entreprise détient des biens et services qui en font sa valeur. **Les biens au sein du système d'information sont des données, des informations, des savoirs ou des savoir-faire**.

> « En effet, ***Total*** **a établi un régime de classification des données en quatre catégories** : jusqu'au niveau 2, il est possible d'utiliser le nuage mais, au-delà de 2, pour des raisons de sécurité, il est interdit de recourir au nuage. »
>
> ***M. Patrick Hereng***
> ***Directeur des systèmes d'information et télécommunications, Total***
> *6 mars 2014*
> *Auditions. Tome II du présent rapport*

L'analyse de risque étudie l'exposition de ces biens et services vis-à-vis de leurs vulnérabilités ou des menaces qu'ils occasionnent.

Les services représentent les algorithmes pour diffuser ces biens ou les produire sous une forme transportable (conditionnement). L'ensemble des services mis en œuvre dans un même objectif de production forme un processus.

Les processus sont les savoirs et savoir-faire de l'entreprise pour produire ou transformer des valeurs en favorisant la circulation des biens et des services.

Le système d'information de l'entreprise se compose majoritairement de processus et d'actifs, les premiers visant à valoriser les seconds.

Du point de vue des échanges, **les services représentent les algorithmes pour diffuser le bien ou le produire sous une forme transportable (conditionnement)**.

Du point de vue de l'analyse des vulnérabilités, l'exposition des processus et actifs a lieu sur des points particuliers du système d'information.

Il est donc nécessaire d'identifier et localiser les mémoires qui hébergent les actifs, les lieux d'exécution des processus ou des services qui y sont rattachés ainsi que leurs points d'échanges, leurs réseaux de transports et d'interconnexions qui favorisent leurs circulations.

a) Identification des actifs

L'analyse de risque devrait porter sur l'ensemble de ces actifs en abordant leur niveau de sensibilité face aux atteintes en confidentialité, intégrité et disponibilité (DIC). Les méthodes d'analyse de risque facilitent l'identification des actifs à l'aide des classifications qu'elles proposent.

Par exemple, la méthode Méhari développée par le CLUSIF est une méthode pour aider les entreprises à mener une analyse de risque de leur système d'information. Elle propose une analyse des processus du système d'information d'une entreprise : la facturation, la production, etc. Pour chaque processus, elle permet de classifier les actifs selon plusieurs catégories : les services impliqués, les applications, les données, les fichiers, les documents papiers, les messages électroniques et papiers.

Ce travail d'analyse est fastidieux et s'avère difficile à automatiser.

b) Localisation des mémoires des actifs et des services

Il est important d'**identifier les différentes localisations** intervenant, directement ou non, dans la valorisation des actifs et des services de l'entreprise.

Ces éléments clés du système d'information sont portés par différentes entités :

- **sites administratifs** composés des mémoires physiques ou numériques (ordinateurs) ; **sites industriels** composés des mémoires physiques ou numériques (ordinateurs, *MES*, etc.) ; ordinateurs portables des personnels mobiles ; téléphones portables ou *smartphones* ; clés *USB* ; capteurs ; etc.

Les **collaborateurs** sont également à inclure comme éléments clés de la mémoire et des services de l'entreprise.

Il s'agit aussi d'**identifier les composants de la chaîne de liaison** car il est important de déterminer si ce composant est :

- privé, et, dans ce cas, il devrait être **possible d'en garder la maîtrise à l'aide de règles et politiques de sécurité** ;

- public et/ou mutualisé, et alors l'accès devient ouvert à tout le monde sans restriction ou à des groupes ; **la robustesse des composants dépend de facteurs externes, humains et technologiques, difficiles à maîtriser**.

Au-delà, **il convient d'analyser la sécurité de la chaîne de liaison du système d'information de l'entreprise connectée** pour identifier les éléments impliqués dans les opérations de transport et, en particulier, de conditionnement/déconditionnement. **Ce sont les points d'échanges qui constituent majoritairement les points sensibles aux intrusions et aux fuites d'information.**

(1) Interconnexions

• Les interconnexions privées entre différents sites : interconnexion « site administratif - site industriel » articulée autour de la « boucle locale-Internet-boucle locale - site industriel » ; interconnexion « site administratif – opérateur » reposant sur la « boucle locale-Internet-boucle locale du côté de l'opérateur » ; interconnexion « site industriel – opérateur » reposant sur la « boucle locale-Internet-boucle locale du côté de l'opérateur » ;

• Les interconnexions publiques entre différents sites : interconnexion « réseau mobile – Internet » ; interconnexion « réseau mobile – RTC » ; interconnexion « Internet – RTC ».

(2) Réseaux locaux ou distants

Les différents supports fédérant ces interconnexions sont :

• Les supports privés : réseau local sans fil pour les utilisateurs de l'entreprise ; réseau local industriel sans fil composé de capteurs.

• Les supports publics : réseau Internet composé des réseaux d'accès, ou boucle locale, reliés au cœur réseau Internet ; réseau 3G ou 4G mobile composé des réseaux d'accès par le biais des antennes et du cœur de réseau ; réseau RTC.

(3) Interconnexions privées/publiques

La valorisation des actifs et des services implique des échanges avec des acteurs externes, ce qui les rend vulnérables.

Du fait des technologies de l'information, le transport de ces actifs et services suppose qu'ils soient **transformés sous une forme binaire**, la seule compatible avec le médium.

Ces médias sont parfois publics ; dans ce cas ces flux seront alors davantage exposés.

Au sein d'un système d'information d'entreprise, **l'analyse de risque implique la connaissance de chaque flux en identifiant leurs interlocuteurs ainsi que la nature des actifs transportés**.

Parmi ces éléments clés, certains constituent des points d'échanges avec l'extérieur, ceux-ci pouvant être publics et mutualisés : vie publique et privée des personnels de l'entreprise avec l'extérieur ; *DMZ* publique du site administratif ; accès Internet des ordinateurs portables des personnels mobiles ; accès Internet des téléphones portables des personnels mobiles.

Au sein d'un système d'information étendu, une multitude de services et de flux sont échangés. L'analyse de risque propose une méthode pour les identifier de façon exhaustive puis les classifier. Il s'agit d'une **matrice de flux** précisant la fonction qu'il assure, son sens **-** public vers privé

ou inversement **-**, son origine, sa destination ainsi que la nature des informations qu'il transporte. Une fois les flux identifiés, ils peuvent être analysés en fonction de leur source et destination afin de **mettre en œuvre des politiques pour les autoriser ou les bloquer**.

Le tableau ci-après illustre les différents éléments requis pour mener une analyse de risque. Par exemple, le flux de messagerie fait intervenir des flux de type *DNS*, *SMTP*, *HTTPS*. Leur description permet d'identifier des règles de contrôles qui pourront être appliquées au moment de leur transit en *DMZ* publique.

Schéma n° 78 : Énumération des flux d'usages et techniques standards et correspondance avec leur numéro de port *TCP/IP*

SENS	TYPE DE FLUX PAR N° DE PORT	USAGES	DESCRIPTION
EXTERNE VERS *DMZ* publique (entrants)	*DNS*	INFRASTRUCTURE	Requêtes de résolution de noms venant d'un proxy d'authentification des Internautes (EXTERNE)
	SMTP		Réception de messages livrés par les serveurs de l'Internet
	HTTPS	USAGE	Requêtes de navigation sécurisées provenant d'Internautes sur le serveur *web* sécurisé du réseau INTERNE
INTERNE VERS EXTERNE (sortants)	*SMTP*	INFRASTRUCTURE	Envoi de messages du serveur de messagerie du réseau INTERNE vers les serveurs de l'Internet
	DNS		Requêtes de résolution de noms *DNS* provenant du réseau INTERNE
	HTTP	USAGE	Requêtes de navigation des utilisateurs du réseau INTERNE vers des serveurs *web* de l'Internet
	FTP		Requêtes de transferts de fichiers sollicitées par les utilisateurs du réseau INTERNE vers des sites de l'Internet
	HTTPS		Requêtes de navigation sécurisées provenant d'Internautes sur le serveur *web* sécurisé interne
	LDAP		Requêtes des services d'annuaire pour la vérification des identifiants des utilisateurs du service *web* en *DMZ*
INTERNE VERS *DMZ*	*HTTPS*	GESTION	Administration distante des serveurs en *DMZ* publique
	SSL		Tunnel *VPN* pour l'administration des serveurs en *DMZ* privée et publique
	ICMP		Autorisation de valider la présence de serveurs en *DMZ* publique

***Source** : OPECST*

Cette analyse des flux sera utilisée par les administrateurs de la sécurité afin de mettre en place les règles de filtrage d'un pare-feu. Ces

règles représentent une part importante des politiques de sécurité de l'entreprise.

2. L'évaluation des risques

L'évaluation des risques repose également sur de nombreuses classifications. Elle regroupe plusieurs **catégories principales** qui peuvent évoluer en fonction de l'activité et des spécificités de l'entreprise, à savoir : indisponibilité passagère de ressources, destruction d'équipements, performances dégradées, destruction de *software*, altération de logiciels, altération de données, manipulation de données, divulgation de données ou d'informations, détournement de fichiers de données, perte de fichiers de données ou de documents, sinistre immatériel total, non-conformité à la législation et à la réglementation.

L'évaluation des risques combine l'évaluation des impacts et des probabilités d'occurrence d'un scénario.

a) Évaluation des impacts

Pour chaque service, Méhari (CLUSIF) propose d'identifier les différents points d'échange constitués des éléments de l'architecture.

Chaque actif est évalué en fonction de son besoin en disponibilité, intégrité et confidentialité (DIC).

Par exemple, la ligne « gestion commerciale » peut indiquer une sensibilité de niveau 4 concernant l'application, les données locales et échangées, les courriers échangés et une sensibilité de niveau 2 et 3 pour leur disponibilité.

b) Évaluation de la potentialité

Pour chaque scenario, Méhari évalue la probabilité d'occurrence de chacun d'entre eux.

Schéma n° 79 : Probabilité d'occurrence des événements

Évaluation de la potentialité des événements - Exposition naturelle								
Type	**Code type**	**Événement**	**Code**	***P=1 très improbable***	***P=2 plutôt improbable***	***P=3 plutôt probable***	***P=4 très probable***	***STATUS-EXPO***
Accidents								
Accident grave d'environnement	AC.E	Foudroiement	AC.E.Fou		x			**2**
		Incendie	AC.E.Inc		x			**2**
		Inondation	AC.E.Ino	x				**1**
Accident matériel	AC.M	Panne d'équipement	AC.M.Equ			x		**3**
		Panne d'équipement de servitude (alimentation électrique, alimentation en fluide, etc.)	AC.M.Ser		x			**2**
Absence volontaire de personnel	AV.P	Conflit social avec grève	AV.P.Gre		x			**2**
Erreur de conception	ER.L	*Bug* bloquant dû à une erreur de conception ou d'écriture de programme (interne)	ER.L.Lin				x	**4**
Erreur matérielle ou de comportement du personnel	ER.P	Perte ou oubli de document ou de médias	ER.P.Peo			x		**3**
		Erreur de manipulation ou dans le suivi d'une procédure	ER.P.Pro			x		**3**
		Erreur de saisie ou de frappe	ER.P.Prs			x		**3**
Incident dû à l'environnement	IC.E	Dégât dû au vieillissement	IC.E.Age			x		**3**
		Dégât des eaux	IC.E.De			x		**3**
		Dégât dû à la pollution	IC.E.Pol		x			**2**
		Surcharge électrique	IC.E.Se		x			**2**
Incident logique ou fonctionnel	IF.L	Incident d'exploitation	IF.L.Exp			x		**3**
		Bug bloquant dans un logiciel système ou un progiciel	IF.L.Lsp		x			**2**
		Saturation bloquante pour cause externe (ver)	IF.L.Ver			x		**3**
		Virus	IF.L.Vir				x	**4**

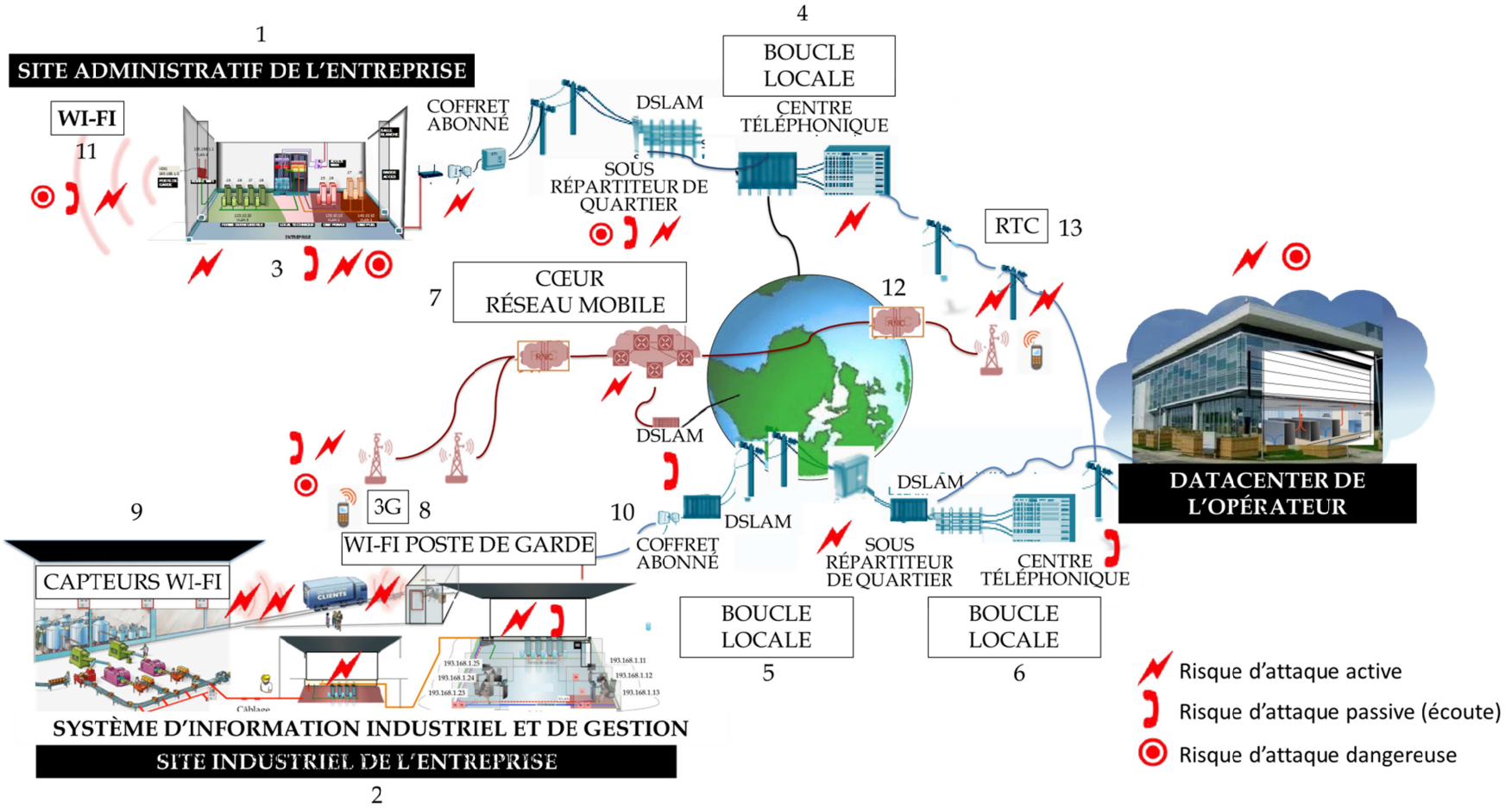
***Source** : Méhari (CLUSIF)*

3. L'analyse des vulnérabilités

Le schéma de l'analyse globale des risques numériques de l'entreprise illustre les différents points d'entrée et angles d'attaques susceptibles d'être exploités par une personne malveillante contre un système d'information d'entreprise.

Afin d'identifier ces vulnérabilités très variées, chaque composant du système d'information doit être audité. Un audit consiste à sonder un système en le confrontant aux différents *scenarii* d'attaques possibles.

Schéma n° 80 : Analyse globale des vulnérabilités numériques de l'entreprise



***Source** : OPECST*

⚠ Complexité de l'audit

Un audit doit être mené de façon méthodique par un expert du domaine. Méhari a identifié **quatorze domaines d'expertise** couvrant des domaines aussi variés que les équipements systèmes, les réseaux, les logiciels ou encore la conformité des normes et lois. Chaque domaine comporte plusieurs centaines de *scenarii*, ce qui montre qu'**un audit mené de façon exhaustive appellerait plus de quatre mille points de contrôle**.

Schéma n° 81 : Exemple d'un questionnaire d'audit de sécurité

Questionnaire d'audit : Organisation de la sécurité		1	variante						
Référence	Question	R-V1	R-V2	R-V3	R-V4	P	Max	Min	Typ
01A	Rôles et structures de la sécurité								
01A01	*Organisation et pilotage de la sécurité générale*								
01A01-01	Tous les domaines concernés par la sécurité ont-ils un responsable désigné [sécurité informatique et télécom, sécurité générale de l'environnement de travail (documents, télécopie, téléphone), sécurité physique générale des sites et locaux] ou un interlocuteur privilégié [DRH pour les actions de sensibilisation, la formation, les contrats de travail, la gestion des comptes utilisateurs et des droits d'accès divers, le traitement (punitif) des opérations délictueuses ou illicites et la négligence interne] ?	0				4	2		E1
01A01-02	Existe-t-il, pour chacun de ces responsables, une définition de fonction précisant, en particulier, ses finalités, responsabilités et interfaces avec les autres domaines de sécurité ?	0				4			E2
01A01-03	Les actions de ces responsables font-elles l'objet d'un tableau de bord et d'un suivi régulier ?	0				4			E2
01A01-04	Existe-t-il un comité ou une structure regroupant l'ensemble des responsables de sécurité, tous domaines confondus, en charge de coordonner les diverses actions et de prendre toute décision transverse, et se réunissant régulièrement ?	0				2			R1
01A01-05	La démarche de sécurité est-elle clairement reconnue et soutenue par la Direction générale ?	1				2			E2
01A02	*Organisation et pilotage de la sécurité des systèmes d'information*								

***Source** : Méhari (CLUSIF)*

L'évaluation des risques représente un travail d'analyse fastidieux difficile à automatiser.

« Alors, nous disposons de la mise en place de normes *ISO* 27001 et suivantes, de la prise de conscience des directions générales, de la détection et du contrôle par l'ANSSI avec la loi de programmation militaire, des chartes informatiques, de la sensibilisation des personnels. Mais **les entreprises n'ont pas tout cela.** Éventuellement, elles ont la charte. **Il faut leur proposer des chartes types et peu coûteuses parce qu'elles n'ont pas les moyens de payer pour avoir un vrai service.** De plus, une entreprise entre vingt et cent cinquante salariés n'a pas la complexité d'une grande entreprise. En tout cas, il faut sensibiliser les entreprises à la sécurité numérique et les inciter fortement à notifier les violations de données à caractère personnel. »

Me Éric Caprioli
Docteur en droit, avocat à la Cour d'appel de Paris, vice-président, Club des experts de la sécurité de l'information et du numérique (CESIN)
19 juin 2014
Auditions. Tome II du présent rapport

⚠ Cartographie statique du système d'information

Bien que les méthodes actuelles d'audit se situent à un niveau technologique élevé capable de déceler de nombreuses failles, l'audit se heurte à **trois difficultés majeures** :

- **l'obsolescence accélérée de l'audit** : l'audit produit une vision instantanée de l'état d'un système, devenant inexacte dès le premier changement (ajout d'un disque, d'une mémoire ou changement de configuration, etc.) ;

- **la variété excessive des technologies** : **l'audit doit permettre de déceler simultanément des vulnérabilités sur des systèmes récents et anciens** ce qui suppose une connaissance de la constitution progressive du système d'information ;

> « De leur côté, **les opérateurs d'importance vitale seront tenus de cartographier leurs systèmes**. Vous pouvez mettre au défit un grand industriel de vous montrer à quoi ressemble ses systèmes d'information, notamment ses systèmes d'information industriels. **En général, les industriels ne savent même pas comment est configuré leur système, où sont les interconnexions, les passerelles vers Internet. Le flou est assez abyssal. C'est également le cas des administrations.** L'obligation de cartographier est donc absolument importante. »
>
> ***M. Pascal Chauve***
> ***Conseiller du Secrétaire général de la défense et de la sécurité nationale (SGDSN)***
> *19 juin 2014*
> *Auditions. Tome II du présent rapport*

- **une vision partielle** : dans la pratique, l'audit s'intéresse à une analyse excessivement locale qui fait courir le **risque de potentielles zones d'ombres non auditées**.

> « Avant, le chiffrement supposait d'intercepter la transmission. L'arrivée de l'informatique a révolutionné cela. Snowden a révélé que c'étaient moins les algorithmes qui protégeaient, comme des sortes de portes blindées de systèmes informatiques, que la solidité des murs autour des portes, trop souvent aujourd'hui les équivalents de murs en carton. Dès lors, **plutôt que de s'attaquer à la porte blindée, il est plus facile de découper le mur à l'aide d'un *cutter*. La plupart du temps, les normes américaines permettent d'extraire ce qui est sur l'ordinateur au moyen, par exemple, d'une porte cachée (*backdoor*) située sur le disque dur ou dans le système d'exploitation (*firmware)*. Il faut donc avoir une vision globale de la sécurité incluant les portes et les murs**.»
>
> ***M. Éric Filiol***
> ***Directeur du laboratoire de cryptologie et de virologie opérationnelles***
> *2 avril 2014*
> *Auditions. Tome II du présent rapport*

4. L'analyse de nouvelles vulnérabilités pour une informatique en nuage (*cloud computing*)

Ces menaces concernent tous les modèles de service, sauf la menace « *abus et utilisation malveillante du cloud* » qui ne concerne que les modèles *IaaS* et *PaaS*.

En effet, **il n'y a pas réellement de menace spécifique au nuage informatique car toutes existent déjà mais, généralement, elles sont amplifiées dans cet environnement** où il se produit une relative perte de contrôle sur les données et services ; ce contrôle étant délégué au fournisseur d'autant plus s'il est multilocataire.

Ce dernier offre une gestion des liens réseaux ou encore l'hébergement d'un de ses sites *web*. Pour cela, l'entreprise doit négocier les règles de gestion en signant un contrat de service.

D'où la nécessité, encore une fois, d'**établir un contrat de service (ou *SLA*) entre toutes les parties impliquées, qui définit le niveau de responsabilité de chacune**.

Les menaces diverses sont répertoriées ci-après.

a) Violation de données

- ⚠ **Mauvaise conception de la base de données** d'un service en nuage multilocataire.
- ⚠ **Accès aux données confidentielles** de tous les clients, vol de données.

b) Perte ou fuite de données

⚠ **Manque de vigilance**, perte de clé, mesures de récupération de données (*back up*) non implémentées par le fournisseur de nuage.

⚠ **Vol des données stockées** dans le nuage par des pirates, ou **pertes involontaires** pour différentes raisons (oubli de sauvegarde, mais aussi en cas de catastrophe naturelle, incendie, etc.).

c) Détournement de compte/de service

En raison de **mots de passe pas assez complexes**, réutilisation fréquemment répétée des mots de passe, hameçonnage, fraude et exploitation des vulnérabilités des logiciels.

⚠ D'où l'**espionnage possible** des activités et opérations, de l'utilisation en question, la manipulation de ses données, le renvoi d'informations falsifiées.

d) Interfaces et APIs non fiables

Utiliser de faibles *API*. La sécurité et la disponibilité des services en nuage dépendent de la sécurité de ces interfaces.

⚠ Sinon, il y a un **risque d'exposition à l'altération de données, de divulgation d'information, de contournement de la politique de sécurité**.

e) Déni de service

Il existe des **vulnérabilités des serveurs** *web*, des bases de données, ou des ressources en nuage. **Inonder un service en nuage de requêtes** permet d'empêcher des utilisateurs légitimes d'accéder à leurs données ou aux applications.

⚠ **Le client se trouve alors contraint de couper lui-même l'accès à son service** pour éviter de se ruiner, puisque la facturation est à l'usage et donc fonction du nombre de requêtes.

f) « Traîtres » malveillants

Le **manque de transparence** sur les procédés et procédures des fournisseurs de nuage ainsi que sur leurs normes de recrutement peut avoir des conséquences néfastes.

⚠ **Accès aux données confidentielles et contrôle des services en nuage** par un adversaire – pirate amateur, agent du crime organisé ou espionnage industriel.

g) Abus et utilisation malveillante du nuage

Le **modèle d'enregistrement souple aux services** proposé par certains fournisseurs de nuage *IaaS* manque de contrôle.

⚠ D'où de possibles **cassages de mot de passe et de clés**, des dénis de service, de l'hébergement de données malveillantes, de contrôle des réseaux de « zombies ».

h) Manque de prévoyance

Adopter le modèle du nuage suppose d'avoir analysé auparavant les risques et les conséquences.

⚠ Mais il n'y a **pas assez de formations dispensées aux employés sur l'utilisation du nuage**. D'où une **vulnérabilité à tous types d'attaques**.

i) Problèmes liés à la mutualisation

Ces problèmes peuvent provenir de **cloisonnements faibles** entre les différentes machines virtuelles – et donc entre les différents clients –, et d'un hyperviseur faible.

⚠ **Dans le cadre du nuage mutualisé, possibilité d'incidence sur les opérations des autres « colocataires »**, accès à des données leur appartenant, à leur trafic réseau.

En conclusion, **les échanges ne peuvent être fiables et sécurisés – ramenant le risque à un niveau d'attaque minimal –, qu'à condition d'utiliser en permanence des technologies adéquates**.

À ce jour, **la technologie la plus répandue et la plus efficace** pour sécuriser ces échanges et permettre les accès distants est le ***VPN*** **(réseau privé virtuel**).

5. Les vulnérabilités des protocoles d'authentification

L'analyse de l'exposition s'effectue habituellement à partir de l'impact rapporté aux propriétés de sécurité.

Il existe une multitude de protocoles d'authentification. Pour choisir entre eux, le compromis entre la facilité de leur déploiement, leur rapidité face à leur robustesse en constitue le principal élément.

Une comparaison entre quelques types de protocoles est esquissée ci-après.

a) Vulnérabilité du One Time Password (OTP)

Comme déjà indiqué, la technique de l'*OTP* consiste à **n'utiliser un mot de passe qu'une seule fois, un autre mot de passe étant fourni à chaque session**. Après le premier déploiement de la phase préalable de réglage, une carte matricielle détenue par le client permet de calculer le code au moment de l'ouverture de session (*login*).

En résumé, il y a l'utilisation d'un secret partagé, l'utilisation d'une carte matricielle (cryptographie symétrique), la non-répudiation n'est pas garantie à 100 % et le **coût limité**.

b) Certificat numérique

Il utilise la cryptographie asymétrique, sa non-répudiation est garantie et son **coût très élevé**.

c) Biométrie

Grâce à la reconnaissance d'une caractéristique ou d'un comportement unique, la non-répudiation est garantie et le **coût très élevé**.

II. LES ATTAQUES CONTRE LE SYSTÈME D'INFORMATION

L'actualité se fait l'écho, de plus en plus souvent, d'attaques numériques couronnées de succès portant sur des sites de plus en plus officiels, des sommes de plus en plus importantes ou concernant un nombre de personnes toujours plus grand.

Anecdotiques il y a quelques années, **ces attaques deviennent extrêmement professionnelles et ont tendance à se généraliser**. Les exemples cités ci-dessous ne portent que sur environ une année et donnent un aperçu de l'ampleur de ce nouveau phénomène dont il importe d'endiguer l'expansion.

Cela va être d'autant plus difficile que les attaques ne sont **pas forcément l'œuvre d'informaticiens extrêmement compétents**. De plus, **des logiciels de piratage grand public commencent à apparaître**.

Quelques exemples, bien loin d'être exhaustifs, d'attaques numériques récentes :

« *L'Armée électronique syrienne pirate «* Le Monde ». *Les hackeurs ont tenté de prendre la main sur le compte* Twitter *et de publier un message sur* Le Monde.fr. » Le Monde – 21 janvier 2015

« *Les* hackers *pro-islam » ciblent les sites français. Entre 20 et 30 groupes ont procédé à des cyberattaques. Peu d'entre eux se réclament du djihadisme »* Le Monde – 18 - 19 janvier 2015.

« *Vague internationale d'escroquerie au virement. Des entreprises du CAC 40 se sont fait voler jusqu'à 20 millions d'euros par un réseau franco-israélien.* » Le Monde – 12 novembre 2014.

« *Quinze personnes jugées dans « l'affaire de l'agence postale* ». Le Monde – 12 novembre 2014.

« *Qui est le* hacker *sioniste soupçonné d'avoir piraté* Rue89 *? Le site d'information a déposé deux plaintes après avoir fait l'objet de plusieurs attaques.* » Le Monde - 10-11 août 2014.

« *Rançonné par des pirates informatiques*, Domino's Pizzza *refuse de payer. Les données de 600 000 clients du spécialiste de la livraison de pizza ont été piratées.* » Le Monde - 19 juin 2014.

« *Vaste coup de filet contre les utilisateurs d'un logiciel grand public de piratage. Simple d'utilisation*, Blackshades *permet de prendre à distance le contrôle d'un ordinateur.* » Le Monde - 25-26 mai 2014.

« eBay, *nouvelle victime des pirates informatiques. Le site d'enchères a annoncé avoir fait l'objet d'une intrusion de grande ampleur : 145 millions de données de ses clients auraient été volées. Le* FBI *prévient que ces attaques vont se multiplier.* » Le Monde - 23 mai 2014.

« *Les hackeurs et le PDG au centre de la cible* ». **Les données personnelles de 70 millions de clients** et les **informations sur les cartes bancaires de 40 millions de clients** de l'**hypermarché nord-américain *Target*** ont été pillées par des pirates informatiques. Un problème de sous-investissement en matière de sécurité informatique et de systèmes de paiement a été diagnostiqué. *Le Monde* - 7 mai 2014.

En matière numérique, **tout ne saurait être qualifié d'attaque**. Les chiffres cités à cet égard sont souvent très exagérés. De plus, **les attaques les plus réussies sont celles non perçues par leurs victimes –** parfois durant des années. C'est la spécificité du risque numérique qu'une entreprise puisse rester dans l'ignorance d'une attaque informatique en cours et ne pas percevoir les conséquences à long terme de cette agression.

En réalité, le manque de maturité des systèmes et la fragilité dans leur conception ou leur implémentation ont produit de nombreuses vulnérabilités qui demeurent.

La confusion est souvent faite entre les notions d'attaques et de vulnérabilités.

Comme décrit au chapitre premier, l'ANSSI et le CLUSIF recensent des vulnérabilités et des attaques. Le *NIST*, avec le système *SCAP*, dresse des relevés quotidiens très complets des vulnérabilités des systèmes.

Ces observatoires se présentent sous forme de sites Internet, à l'échelle des pays, diffusant à un rythme quasi quotidien les nouvelles failles des systèmes et fournissant une base de classification et de recherche des vulnérabilités.

A. LA CLASSIFICATION DES ATTAQUES

Toutes ces attaques concernent des ressources physiques (objets précieux) ou humaines. De nombreux liens de dépendance existent entre ces ressources.

L'enjeu pour protéger ces ressources sera de comprendre cette notion de bien en tant que cible de l'attaque ainsi que les dépendances auxquelles elles sont soumises. Ainsi, une ressource n'est pas un système isolé, bien au contraire ; il s'agit donc d'exprimer une ressource par l'ensemble de ses interconnexions.

Toutes les attaques traditionnelles du domaine sociétal se retrouvent au sein de l'échange électronique, leur classification générale s'inspire des mêmes modes opératoires.

1. Les modes opératoires de base

Les modes opératoires de base d'une attaque numérique ne sont pas sans rappeler des techniques bien éprouvées, rappelées ci-dessous :

- mystification : **simulation du comportement d'une machine** pour tromper un utilisateur légitime et s'emparer de son nom et de son mot de passe (ex. : simulation de terminal) ;

- déguisement : accès illégitime consistant à **se faire passer pour quelqu'un d'autre** et obtenir les privilèges ou les droits d'accès de celui qu'on imite ;

- rejeu : consistant à pénétrer dans un système en envoyant la **reproduction d'une séquence de connexion préalable** d'un utilisateur légitime ;

- faufilement : attaque qui consiste à **franchir le contrôle d'accès en même temps qu'un utilisateur légitime** ;

- substitution : écoute sur une ligne, **interception de la demande de déconnexion d'un utilisateur légitime**, et bénéfice de la session en cours en se substituant à celui-ci ;

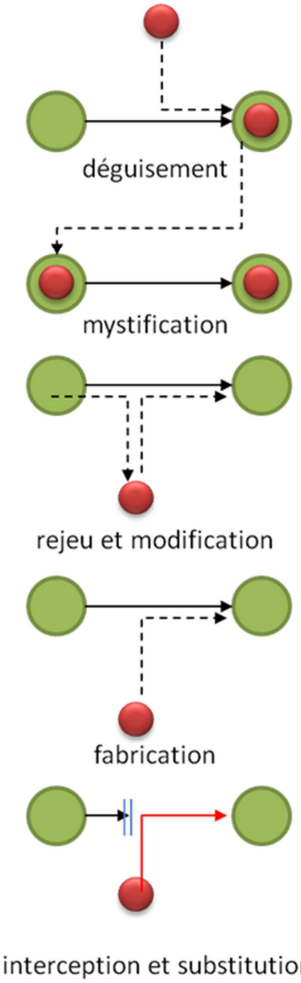
- saturation : attaque portant sur la disponibilité ; elle consiste à remplir une zone de stockage ou un canal de communication **jusqu'à ce qu'on ne puisse plus l'utiliser**.

2. Les modes opératoires combinés

Les attaques selon les modes opératoires de base étant bien souvent bloquées, les attaquants développent des modes opératoires combinant plusieurs attaques de base.

Le schéma ci-après présente (en clair) le comportement légitime et (en foncé) le comportement d'un attaquant.

Schéma n° 82 : Modes opératoires combinés pour une attaque avancée



Source *: INSA Télécoms*

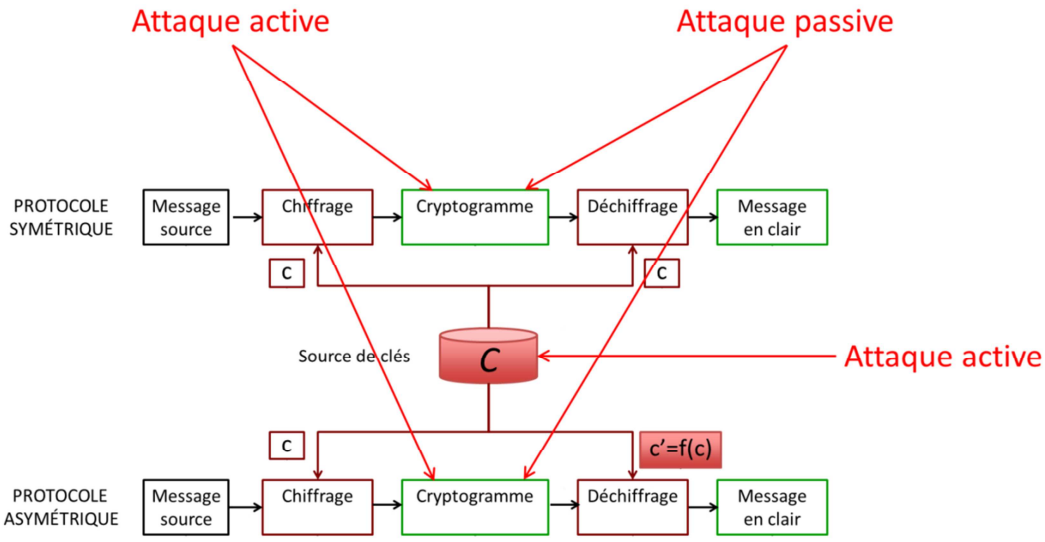
Le scénario du haut du schéma ci-dessus permet à l'attaquant de prendre la forme du comportement légitime ou de le simuler par le déguisement. Le scénario du milieu permet l'écoute passive pour capturer les éléments de l'identification ; il les analyse en les rejouant et les modifiant en vue de fabriquer une nouvelle identité adaptée au mécanisme d'accès. Le scénario du bas permet d'intercepter les éléments de l'échange en les rendant non fonctionnels pour la source, par exemple un déni de service, puis de profiter de son dysfonctionnement pour introduire ses propres éléments. Une attaque par fichier historique de navigation ou *cookie* est une illustration de ce principe.

3. Les attaques sur la confidentialité et l'intégrité

L'authentification constitue un élément central pour contrer les vulnérabilités. Ce processus constitue une garantie lors de l'échange de données ou de documents et l'analyse de l'exposition du processus d'authentification s'effectue habituellement à partir de l'impact rapporté au maintien des propriétés d'intégrité et de confidentialité.

Il existe une multitude de protocoles d'authentification, les uns présentent des avantages dans leur déploiement, les autres dans leur robustesse, **les protocoles tentent de parvenir à un compromis entre la facilité de leur déploiement, leur rapidité et leur robustesse**.

Schéma n° 83 : Comparaison entre deux types de protocoles d'authentification



***Source** : OPECST*

B. LES ATTAQUES COMPLEXES ET CIBLÉES

Les modes opératoires des attaques complexes et ciblées incorporent des actions légitimes d'usagers légitimes, ce qui rend ces attaques difficiles à détecter et analyser.

1. Les attaques complexes

La majorité des attaques numériques dangereuses se déroulent finalement en deux phases, une phase d'**ingénierie sociale** et une phase d'**attaques dites techniques** décrites précédemment.

L'ingénierie sociale permet d'acquérir de façon légitime des informations en vue d'un usage déloyal ou d'une escroquerie. **Ce mode opératoire n'est pas de nature technologique mais exploite les failles humaines et sociales.**

Le principe est d'obtenir d'une personne une information dont l'usage ne saute pas aux yeux de celui qui la transmet mais qui ne sera pas anodine, bien au contraire, pour celui qui tente d'obtenir de cette personne, un bien, un service ou des informations.

Toutes sortes d'exemples montrent chaque jour comment **l'usurpateur exploite des leviers psychologiques** pour parvenir à ses fins. C'est le cas de messages reliés à des sites pirates où l'enjeu de l'attaquant repose sur l'obtention d'un « clic » de sa cible.

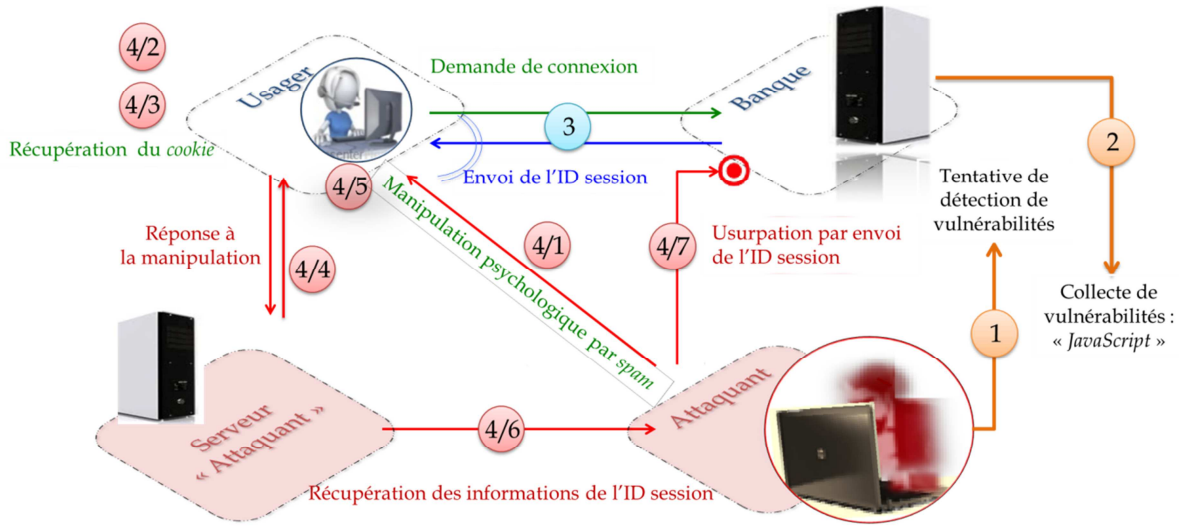
a) Dissection d'une attaque complexe de vol d'identifiant de session

Dans l'exemple du schéma ci-après de dissection d'une attaque complexe, l'attaquant va recourir à des astuces pour décider l'utilisateur à cliquer sur le lien envoyé avec le courriel (*spam*). Les attaquants apportent actuellement de plus en plus de soin pour forger leur courriel piégé : ils exercent une pression sur l'usager en proposant un gain d'argent ou en se faisant passer pour un service informatique, un banquier.

⚠ **L'emploi des historiques de navigation ou *cookies* est à l'origine de la majorité des problèmes de sécurité**.

Étant précisé que cet historique ou *cookie* est un **fichier détenu par un client et contenant des informations sur les échanges passés et en cours avec un site Internet**. L'identifiant écrit dans le *cookie* consigne le fait que le client a réussi l'authentification auprès du serveur mais sert surtout à se faire reconnaître par le serveur.

Schéma n° 84 : Dissection d'une attaque complexe de vol d'identifiant de session



***Source** : OPECST*

(1) L'attaquant en phase d'approche

La préparation menée par l'attaquant suppose la collecte d'informations.

Afin de mettre en place une stratégie, l'attaquant actif repère des sites qui gèrent les sessions à l'aide des exécutables *JavaScript*. Le schéma ci-dessus montre l'activité d'un utilisateur malveillant en quête de sites vulnérables aux attaques de type « *XSS* » :

L'attaquant commence par poster une critique sur les sites de commerce électronique (1), par exemple celui de l'organisme testé (ici, la banque).

Il constate que l'application *web* ne valide pas correctement l'entrée (2) ; il en conclut que l'application est vulnérable et qu'il pourra forger plus tard un identifiant au format *JavaScript*.

(2) La victime

Au cours d'un fonctionnement normal entre le client utilisateur de l'Internet (victime) et le serveur Internet de l'organisme (ici la banque, également victime), l'usager effectue des transactions d'achats sur le site de son organisme de crédit (3). La connexion au moyen de laquelle il a réalisé une authentification avec un nom et un mot de passe est sécurisée par le protocole *SSL*. L'usager obtient un *cookie* de la part du serveur.

Lors de chacune des phases d'authentification pendant laquelle l'usager fournit ses indications de nom et de mot de passe, le serveur a

généré un identifiant de session unique dont la validité se limite à la durée de la session (par défaut, une durée de session est de vingt minutes).

Lorsque le serveur envoie le nouvel identifiant à l'usager, celui-ci l'écrit dans le fichier *cookie* à la suite des identifiants précédents expirés. Quand la session expire, l'usager s'authentifie une nouvelle fois, un nouvel identifiant de session sera alors généré selon ce même processus. Le serveur n'utilise toujours que le dernier identifiant du *cookie*.

(3) L'attaquant

1) L'attaquant forge un message suffisamment rusé pour inciter l'usager à ouvrir une pièce jointe (4-1).

2) L'usager lit le message malfaisant conformément au plan de l'attaquant (4-2). Le *JavaScript* s'exécute. L'attaquant a déjà vérifié sa présence.

3) Le *JavaScript* accède au *cookie* correspondant à la session (4-3) et redirige le client vers un autre serveur, malveillant, en envoyant à celui-ci la session en paramètre (4-4).

⚠ 4) **La victime remarque que l'interface utilisateur du site de commerce électronique a disparu pendant deux secondes mais ne s'inquiète pas** (4-5).

5) **Le serveur malfaisant reçoit la session de la victime** et redirige celle-ci vers la page précédente (4-6).

6) **L'utilisateur malfaisant a maintenant quelques minutes pour accéder au compte de l'usager de la banque et y agir en son nom** (4-7).

Ce scénario montre l'une des nombreuses attaques en mesure d'exploiter des vulnérabilités liées aux développements des applications *web*. Ces vulnérabilités peuvent être volontairement masquées pour exploiter un jour une vulnérabilité « *zero-day* ».

⚠ **Les informations contenues dans les fichiers** (***cookies***) **sont dangereuses, elles sont à l'origine de la plupart des attaques**. De plus en plus d'activités, en particulier le nuage numérique, utilisent le principe des *cookies*. **Pour éliminer le danger, il suffirait de ne pas utiliser les *cookies***. Néanmoins, **comme ils renferment des renseignements précieux pour une exploitation commerciale, leur suppression n'est pas envisagée**.

b) À nouvelles technologies, nouvelles attaques

(1) Les attaques visant l'informatique en nuage

Dans les environnements de l'informatique en nuage, trois aspects clés ont introduit de nouvelles vulnérabilités :

- les données et services sont délégués ;

- le fournisseur est multilocataire ;

- un ou plusieurs fournisseurs seront responsables des données et services.

De nouvelles menaces concernent quasiment tous les modèles de service : *IaaS* , *PaaS* et *SaaS* ; **du fait de la perte de contrôle, les vulnérabilités des systèmes d'information classiques sont amplifiées**.

Multilocation :

⚠ La **violation de données** est une vulnérabilité technologique liée au défaut de conception, à l'heure actuelle, des bases de données multilocataires pour gérer les accès aux données ouvrant un risque important de vol de données.

Convivialité :

⚠ **La perte ou la fuite de données** est une vulnérabilité liée aux usagers qui, par ignorance ou manque de vigilance, pourraient perdre leurs clés de chiffrement ou leurs mots de passe sans mettre en œuvre des procédures de sauvegarde ou, peut-être mal implémentées par le fournisseur, ne prévoyant pas de processus de tests de restauration.

⚠ **Le manque de transparence de la part du fournisseur sur les processus et outils de stockage ou de partage ne fournit pas aux usagers un tableau de bord pour la supervision de leurs données**.

Accès non maîtrisés aux données :

⚠ La **destruction de données** est une vulnérabilité du fait de pirates ou d'origine involontaire comme l'oubli de sauvegarde ou la survenance d'une catastrophe naturelle, d'un incendie, etc.

⚠ Un adversaire accédant à des services du fournisseur peut se faufiler et **accéder à des données confidentielles**.

Gestion des identités et des politiques de sécurité :

⚠ Le **détournement de compte** est une vulnérabilité du fait du manque d'exigences dans les politiques de sécurité des mots de passe ou du fait d'opérations de « hameçonnage », de fraude et d'exploitation des vulnérabilités des logiciels.

⚠ **L'espionnage**, proche de l'intelligence économique, est une vulnérabilité du fait d'activités et d'opérations non maîtrisées de l'usager sur ses données, ou en réponse à des demandes non authentifiées.

⚠ **Le vol des données stockées** dans le nuage est une vulnérabilité du fait de la présence non détectée de pirates.

⚠ **L'altération des données et leur divulgation** est une vulnérabilité du fait de contournements de la part des usagers ou de pirates des politiques de sécurité en vigueur.

Services :

Le **manque de fiabilité des interfaces** entre les applications ou de mauvaises programmations les expose à des atteintes à leur intégrité et leur disponibilité.

⚠ Le déni de service de serveurs *web*, bases de données ou ressources dans les nuages informatiques sont des **vulnérabilités liées à des flux « tempêtes » de services mal configurés**. Les pirates inondent un service de requêtes pour empêcher les utilisateurs légitimes d'accéder à leurs données et/ou à leurs applications. Pour une entreprise dans cette situation, les conséquences seront une perte substantielle de son chiffre d'affaires, amplifiée s'il s'agit d'un serveur de paiement.

L'analyse des risques ne doit pas être occultée par le fait que **la responsabilité incombe au fournisseur de services**.

Cependant, **la formation des usagers ne doit pas être négligée** au prétexte que la responsabilité juridique incombe au fournisseur de services.

⚠ Le **manque d'exigences du fournisseur de service dans son plan de recrutement** peut entraîner la présence de pirates appartenant à des organisations criminelles.

Le modèle de nuage numérique adopté doit préserver des usages détournés et fournir les contrôles de base comme la complexité du mot de passe et celle des clés, la résistance aux dénis de service, le contrôle des données malveillantes potentiellement hébergées, le contrôle des réseaux de « zombies »

Mutualisation :

⚠ La **faiblesse du cloisonnement entre les machines virtuelles** (systèmes, routeurs, etc.) dans le cadre de la mutualisation peut entraîner des effets sur des usagers provoqués par le manque de fiabilité de ses « colocataires ».

(2) La sécurisation des objets connectés

Les objets connectés désignent des systèmes mobiles capables d'embarquer des capacités de traitements les rendant autonomes pour fournir un service.

Aujourd'hui, l'intérêt des objets connectés n'est plus à démontrer, ils envahissent d'ores et déjà le quotidien. **Le nombre d'objets connectés va s'accroître dans des proportions inimaginables.** Pour s'en tenir aux ordres de grandeur, assez divers, évoqués par les personnes entendues dans le cadre du présent rapport, il pourrait s'agir de **cinquante milliards d'objets**

connectés dans le monde avant 2020 (selon M. Patrick Hereng de *Total*), de **dix-huit à quatre-vingts milliards avant 2018** (d'après les études déjà citées de *Be Intelligence* ou de l'*IDATE*), de **cinquante milliards en 2050**, (d'après M. Christian Daviot de l'ANSSI) ou encore de l'hypothèse que, avec le développement futur du *big data*, il y aurait **mille fois plus d'objets connectés que d'humains** (selon M. Philippe Wolf, ingénieur général de l'armement). Ces quantités représenteront un chiffre d'affaires croissant très rapidement pour atteindre des montants extrêmement élevés. **Chaque personne pourrait être équipée d'une centaine objets connectés et chaque logement de cinq cents environ.** Certains téléphones portables possèdent déjà une cinquantaine de capteurs : gyroscope, etc.

Les perspectives qu'offrent ces nouveaux objets sont impressionnantes, tant dans le développement de nouveaux modèles d'affaires, prometteurs d'une économie florissante, que des services qu'ils vont rendre à l'Homme.

⚠ Néanmoins, **actuellement, ces systèmes ont été conçus au mépris de mécanismes sérieux de sécurisation**. La difficulté de les gérer reste également une préoccupation majeure.

⚠ **Ces objets sont déjà présents sur des sites industriels de criticité élevée**. Comment les entreprises et, en particulier, les opérateurs d'importance vitale, vont-elles pouvoir se protéger, d'autant qu'elles auront investi des sommes considérables dans des plans de sécurité et que ces petits objets viendront mettre en échec leurs efforts ?

« **Le ministre a demandé à l'ANSSI d'élaborer des normes de sécurité pour les systèmes de comptage intelligents**, sujet dont personne ne s'était saisi jusqu'alors. Aujourd'hui, **on s'aperçoit que les objets connectés peuvent être des portes d'entrée pour les attaquants informatiques lorsqu'ils ne sont pas forcément sécurisés et, lorsqu'ils sont sécurisés, ils ne sont pas forcément reconfigurables.** Il est important que des failles de sécurité ne puissent pas permettre la prise de contrôle de tels objets par des individus malveillants. »

Mme Cécile Dubarry

Chef du service des technologies de l'information et de la communication, Direction générale de la compétitivité, de l'industrie et des services (DGCIS)

26 mars 2014

Auditions. Tome II du présent rapport

2. Les attaquants chevronnés

Les attaques complexes mettant en évidence la vulnérabilité du numérique sont conçues par des individus possédant une certaine

psychologie que vos rapporteurs ont tenté de comprendre – tout en se limitant à un certain profil correspondant à un niveau technique très élevé.

a) La psychologie du hacker

La sécurité du numérique est généralement considérée comme menacée le plus gravement quand des *hackers* interviennent – ou, à l'inverse, protégée au mieux s'il est fait appel à des *hackers* – c'est pourquoi vos rapporteurs ont souhaité mieux connaître ce qui se cache derrière cette appellation censée expliquer nombre d'agissements incompris.

Hacker vient de hache. Il désigne **celui qui se sert d'une hache pour pénétrer dans un système informatique plutôt que de s'encombrer de mots de passe ou de protocoles**. Ce terme signifie aussi que des programmes, des logiciels peuvent être simplifiés jusqu'à offrir une structure plus simple, voire plus élégante, le *hacker* s'apparente alors davantage à l'**élagueur**.

Dans le premier sens, le *hacker* évoque **le cambrioleur**. Comme lui, il est un spécialiste de l'effraction de ce qui empêche d'entrer quelque part. Comme lui, il s'efforce de laisser le moins de traces possible de son effraction.

Toutefois, dans le contexte de la construction de l'Internet et de l'invention des micro-ordinateurs, ceux qui sont qualifiés de *hackers* ont joué un rôle inventif, créatif qui en fait bien plus que des cambrioleurs ou des élagueurs du numérique.

Au départ, **l'Internet a été conçu comme un lieu de liberté totale d'accès à l'information**, **à une information gratuite** – cette information incluait aussi l'accès aux modes de fabrication et de fonctionnement des composants, des ordinateurs, des réseaux et de ceux qui les utilisaient.

Mais il ne s'agissait pas d'informations gratuites sur tout le monde ni d'un accès à tout le monde.

Et c'est là que les *hackers* sont intervenus, notamment pour qu'existent les micro-ordinateurs face aux ordinateurs géants des grandes firmes informatiques.

Peu pris au sérieux à leurs débuts, les *hackers* sentaient que la mise à disposition de tous de micro-ordinateurs ne pouvait qu'advenir et ils se sont employés, par tous les moyens, comme mus par une obsession, à transformer leur intuition en réalité.

Souvent en cours d'études dans des universités américaines renommées mais également obsédés par l'informatique dès le plus jeune âge – parfois seulement vers la dizaine ou la quinzaine d'années – ceux qui devaient être appelés *hackers* mettaient gratuitement en commun leurs connaissances et considéraient que l'argent, le marché, tout interdit ne pouvaient que compromettre leur quête.

Parmi ces jeunes passionnés se trouvaient nombre d'inventeurs géniaux inconnus du public mais renommés dans le milieu de l'informatique et d'autres dont le monde entier connaît aujourd'hui le parcours et la fortune, en particulier :

- Steve Jobs et son associé M. Steve Wozniak à l'origine d'*Apple* ;

- M. Bill Gates, fondateur de *Microsoft*, qui, le premier, a estimé que l'ingéniosité technique des *hackers* méritait une juste rétribution.

Ces *hackers* ont fréquemment eu raison face à l'ordre établi des universités – dont ils manquaient souvent les cours, utilisant, sans autorisation et à des heures de fermeture, les ordinateurs et négligeant l'obtention des diplômes.

L'esprit *hacker* perdure aujourd'hui et pénétrer des systèmes informatiques demeure un défi à relever.

Défi d'autant plus excitant que des fabricants de matériel, des entreprises, des administrations, des États prétendent que leurs systèmes informatique sont sûrs, voire inviolables.

D'où de multiples pénétrations de systèmes par des *hackers* suivies de mises en garde, plus ou moins publiques, attirant l'attention sur des failles de systèmes informatiques.

Lorsque ces alertes ne sont pas prises au sérieux, lorsque la victime de ces attaques menace de répression, il arrive que la situation s'envenime.

À l'inverse, certaines firmes, certains États tirent immédiatement profit de ces alertes et vont même, parfois, jusqu'à engager les *hackers* ayant mis les failles en évidence.

Ces éléments montrent que, contrairement au cambrioleur, le *hacker* n'est pas d'abord mû par le désir de voler mais par celui de déjouer les barrières destinées à empêcher d'entrer. Un peu comme ces obsédés de la découverte du sous-sol parisien qui explorent toutes les entrées possibles de celui-ci souvent ignorées, là-aussi, des propriétaires des immeubles situés au-dessus de galeries ou de salles souterraines, de grottes.

C'est pourquoi des entreprises, des administrations, des États estiment qu'**un bon usage du *hacker* peut consister à l'embaucher pour, cette fois, aider à bâtir une protection dynamique d'un système informatique**.

Au cours de leurs visites et auditions, vos rapporteurs ont pu constater que des entreprises, voire des administrations, en charge de sécurité informatique avaient engagé des *hackers*, présentés toujours prudemment comme des « anciens *hackers* » comme s'il fallait rassurer l'interlocuteur et témoigner d'un supposé repentir. Il est à souhaiter, au contraire, qu'il s'agisse bien toujours de *hackers* en état d'inventivité maximale pour être à la hauteur des attaques à surmonter.

Ce rapide survol de la psychologie des *hackers* pourrait inspirer plusieurs propositions de recommandations comme :

- les prédispositions à l'informatique et à son usage n'attendent ni les années ni une formation officielle sanctionnée ou non par un diplôme, d'où la nécessité de **développer sensibilisation, éducation et formation à l'informatique dès le plus jeune âge** compte tenu du besoin très fortement croissant de spécialistes en ce domaine ;

- la nécessité de **repérer les *hackers*** pour bénéficier des retombées positives de cette tournure d'esprit particulière ;

- l'intérêt de **conserver en France les personnes dotées de talents de *hacker***. En effet, de plus en plus souvent, celles qui fondent de nouvelles petites entreprises innovantes dans le numérique sont majoritairement recrutées par des entreprises américaines ou engagées à l'étranger ;

- les *hackers* constituent aujourd'hui une richesse nationale dont il pourrait être tiré parti pour **renforcer la sécurité du numérique et la résilience à la suite d'attaques ayant abouti**.

« [...] **il existe une frange importante de jeunes *hackers*, qui constituent des ressources de premier ordre.** Ils sont loin d'être des autistes et il serait intéressant de les écouter. La France possède l'avantage majeur d'avoir de nombreux jeunes brillants dans le domaine du numérique même s'ils ne sont pas les plus diplômés. **Malheureusement, *Google* et d'autres sociétés étrangères sont actuellement en train de piller ce vivier de jeunes. Un sursaut national s'impose pour tirer parti de ces savoir-faire et de ces bonnes volontés.** À l'étranger, les États-Unis d'Amérique ou Singapour les accueillent à bras ouverts. »

M. Éric Filiol
Directeur du Laboratoire de cryptologie et de virologie opérationnelles
2 avril 2014
Auditions. Tome II du présent rapport

3. Les caractéristiques d'une cyberattitude

Vos rapporteurs ont insisté, dès le début de ce rapport, sur la différence entre le réel, le virtuel et l'imaginaire ; il est important de souligner que cette distinction, pas toujours aisée à opérer en pratique, a des effets sur le psychisme des utilisateurs du numérique.

« Le numérique est une chance incroyable, il offre à la jeunesse des possibilités de connaissance, de prise d'action sur le monde et de développement de la créativité qui sont remarquables. Mais il est aussi associé à un risque majeur. Pour le comprendre, il faut avoir à l'idée un concept clé de la cyberpsychologie : le concept d'immersion.

Quand on s'immerge dans un monde virtuel, dans un monde numérique, se produisent dans l'esprit d'un sujet des mécanismes tout à fait orignaux et spécifiques, qui ne sont pas réductibles à ce qui

se passe quand on joue à un jeu avec des petites figurines, quand on lit un livre, ou quand on regarde un film. **Avec le numérique, on est acteur d'une action virtuelle. Cela pose le sujet dans une position de responsabilité tout à fait particulière, puisqu'il accomplit à la fois une action réelle et une action qui se situe dans un monde virtuel. Il y a donc une sorte d'irresponsabilisation de l'acte** qui fait qu'il est dans un entre-deux, un espace transitionnel particulier.

Cet espace transitionnel peut avoir des effets intéressants. Les mondes virtuels sont, par exemple, utilisés pour soigner un certain nombre de jeunes qui ont des difficultés. Mais cet espace présente aussi des difficultés et des risques. J'ai identifié **cinq risques** : [...] la séduction traumatique, [...] les conduites addictives, [...] la subversion des institutions cadres, [...] la manipulation idéologique, [...] la confusion des valeurs. »

M. Benoît Virole
Docteur en psychopathologie, docteur en sciences du langage, membre de l'Observatoire des mondes numériques en sciences humaines (OMNSH)
19 juin 2014
Auditions. Tome II du présent rapport

4. La cybercriminalité

Les attaques de nature technique sont le privilège d'individus malveillants usant des technologies comme arme de persuasion. Ces individus, qui ne se confondent pas systématiquement avec les *hackers* décrits ci-dessus, sont des criminels particuliers dont les crimes relèvent de la cybercriminalité qui en étudie les différentes formes.

Le terme de « cybercrime » est récent puisqu'il fut pour la première fois employé, à l'occasion d'une réunion du G8 dont l'un des objets visait, en 1999, la défense des États contre les nouvelles formes électroniques du crime. Quelques années plus tard, une convention sur la cybercriminalité[1], STCE n° 185, a été proposée ; elle est aujourd'hui ratifiée par vingt-trois États, membres ou non membres, dont les États-Unis d'Amérique.

C'est la criminologie, encore appelée « science du crime », qui en étudie ses différentes formes en s'intéressant aux circonstances qui ont conduit un individu au crime. La criminologie se fonde sur les méthodes de la statistique descriptive pour identifier une certaine forme de la normalité et certaines typologies de la criminalité même si comme le précisait le père fondateur de ce concept, Émile Durkheim, ces modèles statistiques s'avèrent sans doute inexacts pour de multiples raisons, ne serait-ce que parce que les circonstances ne sont pas reproductibles.

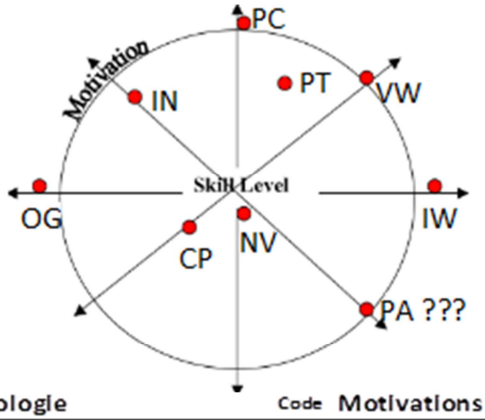
Toutefois, **la difficulté de mesurer les « cybercrimes » n'a fait que renforcer les menaces criminelles à l'encontre des sphères sociétales**. Depuis plus de deux ans, de nouveaux observatoires institutionnels

[1] *Convention sur la cybercriminalité du Conseil de l'Europe (STCE n° 185), ouverte à la signature en 2001 et entrée en vigueur le 1er juillet 2004. http://www.europarl.europa.eu/activities/committees/*

apparaissent et organisent une instrumentation de plus en plus pertinente des cybercrimes. Dès lors, les prochaines années seront déterminantes pour apporter une vision claire de la cybercriminalité et rétablir la confiance citoyenne.

La taxonomie de Marcus Rogers relève plusieurs profils caractérisés par deux critères : leur compétence et leur motivation. Il détaille huit profils allant du novice aux plus expérimentés dans leurs actes et dont l'intérêt est le gain ou la reconnaissance sociale.

Schéma n° 85 : Typologie des attaquants



Typologie	Code	Motivations
Novice (NV)	NV	reconnaissance
Cyber Punk (CP)	CP	image
Internals (IN)	IN	vengeance
Petty Thieves (PT)	PT	argent
Old Guard (OG),	OG	idéologie technologique
Virus Writers (VW)	VW	habileté
Professional Criminals (PC)	PC	argent
Information warfare (IW)	IW	patriotisme

***Source** : Marcus Rogers*

Vers la fin des années 1990, les objectifs des délinquants (cyberdélinquants de type novice ou *cyberpunk, NV* ou *CP*) ou criminels étaient alors variés mais rarement commerciaux, puisque le e-commerce balbutiait. Il s'agissait plutôt de défier les forces de l'ordre ou de se faire reconnaître par sa communauté en réalisant des exploits ; l'anonymat conférait une impunité naturelle aux auteurs de ces infractions.

Les nouveaux enjeux commerciaux, l'adhésion quasi universelle de l'Internet en tant que « compagnon du quotidien », l'expertise facilement partagée entre tous les acteurs, pour le bien et le mal, sont devenus cette fois le lot quotidien des *mafias* à la recherche de profits financiers. Elles se sont massivement organisées et installées autour des sphères de l'échange : sociétale et technologique. Ainsi le succès de l'échange électronique a-t-il rapidement fait naître les convoitises d'individus dangereux (de type *PC*, *PT*) agissant seuls ou en *mafias* profitant d'usagers maladroits ou d'administrateurs non encore aguerris à leurs techniques d'attaques.

Ces individus sont aux yeux de la loi des délinquants, des escrocs, parfois des criminels mais rendent-ils l'Internet dangereux ? Le développement de la criminalité de l'échange menace-t-il la sécurité des échanges électroniques ?

Tout d'abord, les vulnérabilités des systèmes, dont la fragilité a été accrue par la dextérité des *hackers* de type *VW* et *OG* et l'hétérogénéité des systèmes communicants, se sont rapidement développées, prenant des formes inquiétantes et encore peu connues : le mariage entre « robots attaquants » et « vers » ou « virus » active leur propagation et constitue de ce fait une attaque en masse sous le poids de laquelle la digue a du mal à ne pas céder.

III. LA FONCTION DE SURVEILLANCE DE LA SÉCURITÉ

L'étude de risque, aboutissant à une cartographie des risques, constitue pour l'entreprise un préalable à la construction de sa sécurité numérique en profondeur qui s'appuie également sur l'audit ou l'investigation. Cet ensemble d'informations détermine la nature de la sécurité opérationnelle à mettre en œuvre en réaction aux attaques numériques.

« Il n'est jamais question de sécurisation totale car ce serait faux et dangereux de laisser croire que l'environnement est parfaitement sécurisé d'autant qu'**il faut entretenir un certain sentiment d'insécurité, de la vigilance en permanence**. De plus, mieux que de se cantonner aux antivirus**, il faut procéder à une approche en profondeur** avec des barrières à l'entrée des réseaux, des murs (*firewall*) qui filtrent certaines informations avec des antivirus et **des moyens de supervision** pour constater si quelque chose d'anormal se produit, comme lorsqu'un ordinateur consulte trop souvent un autre ordinateur ou un serveur ; il est alors possible de savoir ce qui se passe. Des outils de chiffrage, des protections, des filtres sont mis en place à différents endroits au vu des besoins pour améliorer le niveau de sécurité jusqu'à un seuil acceptable. »

M. Éric Bruni
Chef du service de la sécurité de défense et des systèmes d'information, DGA
6 mars 2014
Auditions. Tome II du présent rapport

Face à l'escalade importante des failles de sécurité, le rôle de la sécurité opérationnelle devient primordial. La surveillance est l'un des piliers de la gestion des risques.

A. RECOURS À LA CARTOGRAPHIE DES RISQUES

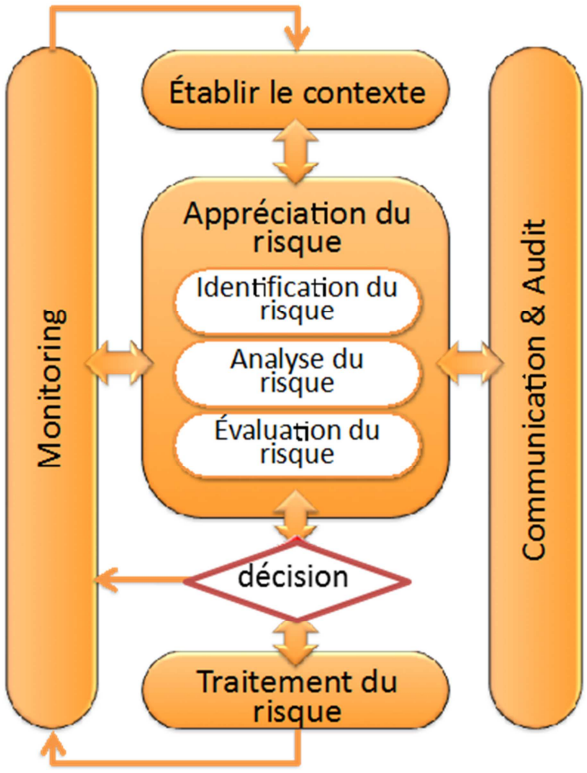
Depuis une vingtaine d'années, l'étude des risques s'est imposée dans de nombreux domaines comme un cadre réducteur de l'incertitude et

de la complexité. Néanmoins, la société moderne vit aujourd'hui un curieux paradoxe où elle affirme sa volonté de se projeter dans l'avenir par une course accélérée à l'innovation tout en préservant une logique prudentielle. Il en découle une omniprésence de la maîtrise du risque devenue un phénomène sociétal tel que certains sociologues du début des années 1990 ont baptisé nos sociétés modernes de « *société du risque* » (M. Ulrich Beck).

Ce constat conduit à penser que **le numérique ne doit pas dominer la société mais doit rester simplement un nouveau produit du risque qu'il faut appréhender afin de revenir à une situation de maîtrise de la technologie**.

Pour répondre à cette double exigence avec efficacité, il a été imaginé de mettre en place une fonction de surveillance fondée sur une **cartographie des risques déterminée à partir d'une analyse des risques**. Cette approche est conforme aux nouveaux modèles de gouvernance proposés récemment au sein des normes *ISO/IEC* 31000 et *ISO/IEC* 27005.

Schéma n° 86 : Modèle de risque ISO / IEC 31000



Source *: OPECST*

B. ACTIVITÉS DE SÉCURITÉ POUR LA DÉTECTION, L'ÉVALUATION ET LA REMÉDIATION DES INCIDENTS

Les activités de la sécurité opérationnelle, d'un *Security Operations Center* (*SOC*), constituent un coût très voire trop onéreux pour les entreprises, en particulier du fait des compétences élevées et continues nécessaires aux experts. En outre, l'emploi de logiciels spécifiques, puissants et coûteux comme les systèmes de gestion des informations et événements de sécurité (*SIEM*) et les systèmes de détection d'intrusion (*IDS*) augmente cette difficulté.

Les activités de sécurité sont généralement l'œuvre d'experts du domaine, regroupés au sein d'une institution (ANSSI, DGA, etc.) ou d'entreprises privées. Pour l'investigation ou l'audit, ces activités sont occasionnelles et à forte compétence experte ce qui justifie pleinement l'usage de ces activités sous forme de services.

1. La sécurité opérationnelle

Schéma n° 87 : Site de supervision d'un système d'information



Source *: OPECST*

a) Centre pour la supervision de la sécurité

Un centre de sécurité opérationnelle (ou *SOC*) est la partie du système d'information de l'entreprise destinée à la mise en place de solutions pour la détection, la localisation et la qualification des événements de sécurité et la mise à disposition de plans de réaction.

Un centre de sécurité opérationnelle agit sur un site donné mais peut intervenir à distance à l'aide d'outils spécifiques et particulièrement sécurisés : cette supervision est dite centralisée et distribuée.

Les *SIEM* regroupent un ensemble d'outils en vue de l'analyse qui prend en compte un besoin de supervision de sécurité exprimé par un client.

b) Contrat de service de sécurité

La relation entre un centre de sécurité opérationnelle et son client s'établit au travers d'un contrat appelé *SLA (Service Level Agreement*) qui scelle au préalable le périmètre surveillé, les modes et délais d'intervention, le mécanisme d'escalade en cas d'incident.

c) Incident informatique

Un incident informatique est une menace de violation imminente des politiques de sécurité informatique, des politiques d'usage ou des pratiques. Ensuite, l'incident fait l'objet d'un ticket ; l'usager qui en a été victime le déclare à l'aide d'un outil spécialisé auquel il accède généralement à l'aide d'un navigateur *web*. L'usager doit décrire l'incident afin de bénéficier du service. Le *NIST* a défini des rapports d'incidents devant inclure une description de l'incident ou de l'événement, en utilisant la taxonomie proposée.

Un centre de sécurité opérationnelle intervient en majorité après des incidents liés à des **applications non testées ou modifiées**, à des **erreurs humaines** par ignorance ou manque de documentation. Les **problèmes matériels, électriques et de réseaux** ne représentent que 20 % des incidents.

d) Compétences multiples et compétence d'équipe

L'expert est responsable d'incident (*incident responder*) mais, en réalité, il s'agit d'une équipe d'experts plutôt que d'un individu, du fait du besoin de compétences multiples et hétérogènes allant de l'expertise réseau à l'expertise « *Java* » mais également en raison de **la durée de résolution d'un incident qui peut atteindre jusqu'à plusieurs jours en moyenne, plusieurs mois dans le cas d'attaques complexes et ciblées**.

e) Architecture de supervision d'un SOC

La partie de la supervision de la sécurité repose sur **l'analyse des traces** provenant des systèmes de détection d'intrusion placés aux divers endroits du système d'information pour en assurer la surveillance.

Le rôle d'un *SIEM* sera de gérer ces traces et de les interpréter. D'un point de vue de la gouvernance, la gestion de ces données requiert d'organiser les fonctions du *SIEM* sur le système gouverné. Il s'agit d'un cycle en quatre étapes : collecte, détection, analyse et traitement des incidents de sécurité. Chacune d'entre elles est également l'objet d'un processus de décision :

- collecter : décider de la pertinence d'un signal par l'observation ;

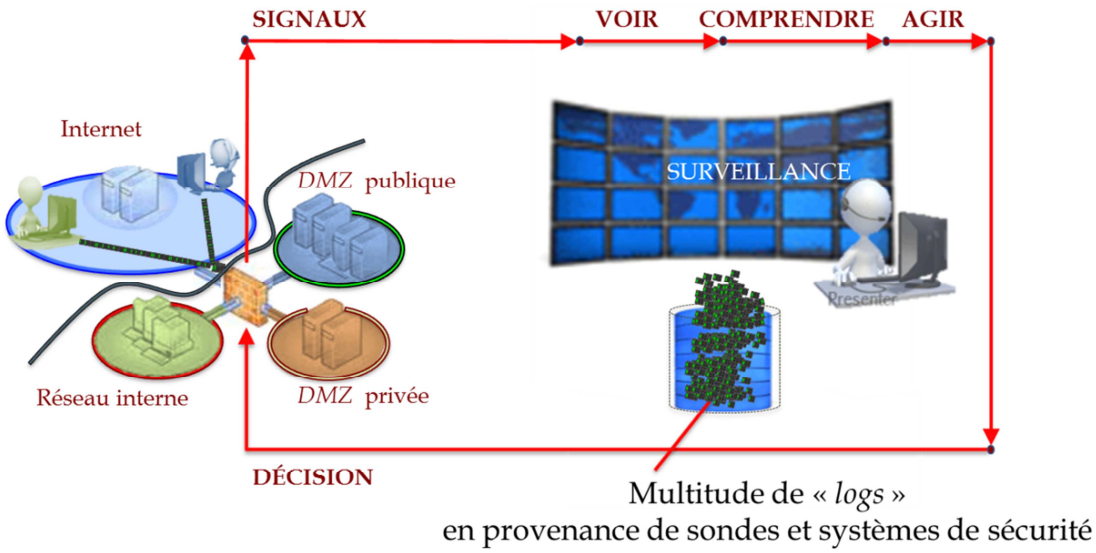
- voir : décider que ce signal constitue un incident de sécurité ;

- comprendre : analyser en localisant, identifiant et caractérisant l'incident ;

- décider des actions correctives.

La performance d'un tel système de surveillance repose entièrement sur la précision à chacune des étapes du cycle du processus de décision.

Schéma n° 88 : Architecture simplifiée du processus de surveillance de la sécurité numérique

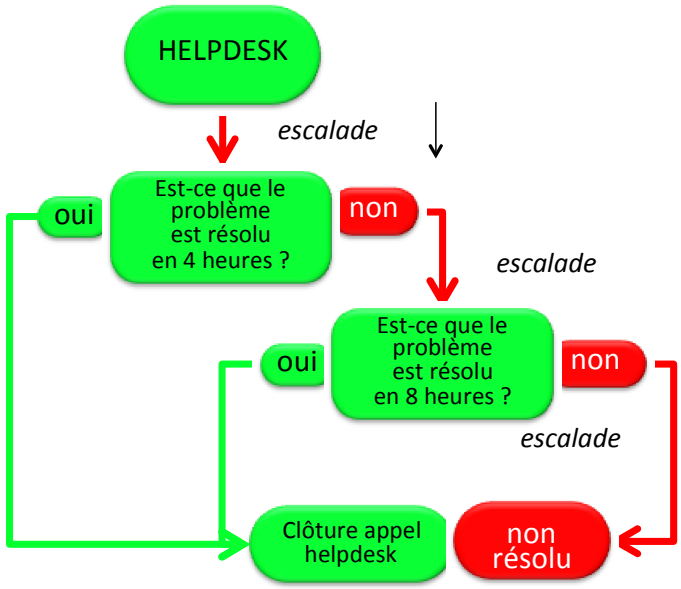


Source *: INSA thèse*

f) Le processus d'escalade jusqu'à la résolution de l'incident

À partir de l'apparition de l'incident jusqu'à sa résolution, une méthodologie d'intervention en forme d'escalade doit être mise en œuvre.

Schéma n° 89 : Circuit du traitement de l'incident de sécurité jusqu'à sa résolution



***Source** : INSA TC*

2. L'audit de sécurité

L'audit de sécurité d'un système d'information est **un instantané de ce système** dont le but est de détecter les vulnérabilités sur différents plans : organisationnel, technique, ressources humaines, conformité aux normes, aux règles de bonnes pratiques et aux contraintes juridiques.

L'audit peut être également conjoint à une analyse de risque selon le but poursuivi : réaction à une attaque, évaluation du niveau de sécurité du système d'information, évolution du système incorporant de nouveaux équipements ou processus, etc. **L'audit devrait même être pratiqué à chaque modification du système d'information**.

La démarche d'audit de sécurité est proche de celle de la démarche qualité : elle doit être méthodique et **ne pas omettre de tester un élément du système, à savoir le maillon faible**. L'audit repose sur plusieurs façons de faire : l'entretien, les tests d'intrusion, les relevés minutieux des configurations des systèmes (programmes, routeurs, postes de travail, serveurs, etc.). L'audit technique peut être mené seul ou s'inscrire dans un audit organisationnel. Il permet à l'expert de focaliser son attention sur les

rouages d'une nouvelle application *web* afin de s'assurer qu'il ne présentera pas de faille lors sa mise en ligne.

Une inspection méthodique et périodique du système d'information est un atout considérable pour la bonne santé de celui-ci, néanmoins, les ressources humaines afférentes à ces opérations sont longues et entraînent **des coûts non négligeables** pour une entreprise qui sont de l'ordre de 1 500 € à 2 000 € la journée, impliquant facilement plusieurs experts pendant plusieurs semaines.

Le « test d'intrusion » est une alternative intéressante puisqu'elle fait intervenir une équipe durant environ une semaine pour un coût de l'ordre de 10 000 € et permet de **détecter des vulnérabilités avant qu'elles ne soient exploitées** par de véritables pirates.

3. L'investigation liée aux incidents

L'investigation est une étape de recherche de cause d'un incident ; elle est dite pour cette raison « *post-mortem* », également appelée analyse forensique pour **détecter le mode opératoire d'un attaquant ou d'un robot** s'il s'agit d'une attaque par virus, ou de l'intrusion d'un logiciel malveillant.

Des équipes spécialisées interviennent pour déterminer et délimiter le périmètre ainsi que l'ampleur de l'attaque informatique. À cette occasion, **les preuves numériques sont collectées et analysées** afin d'établir l'origine de la malveillance ou de l'incident.

Les éléments de preuve collectés peuvent être un support à la démarche juridique ou d'assurance.

B. RÉACTION AUX ATTAQUES

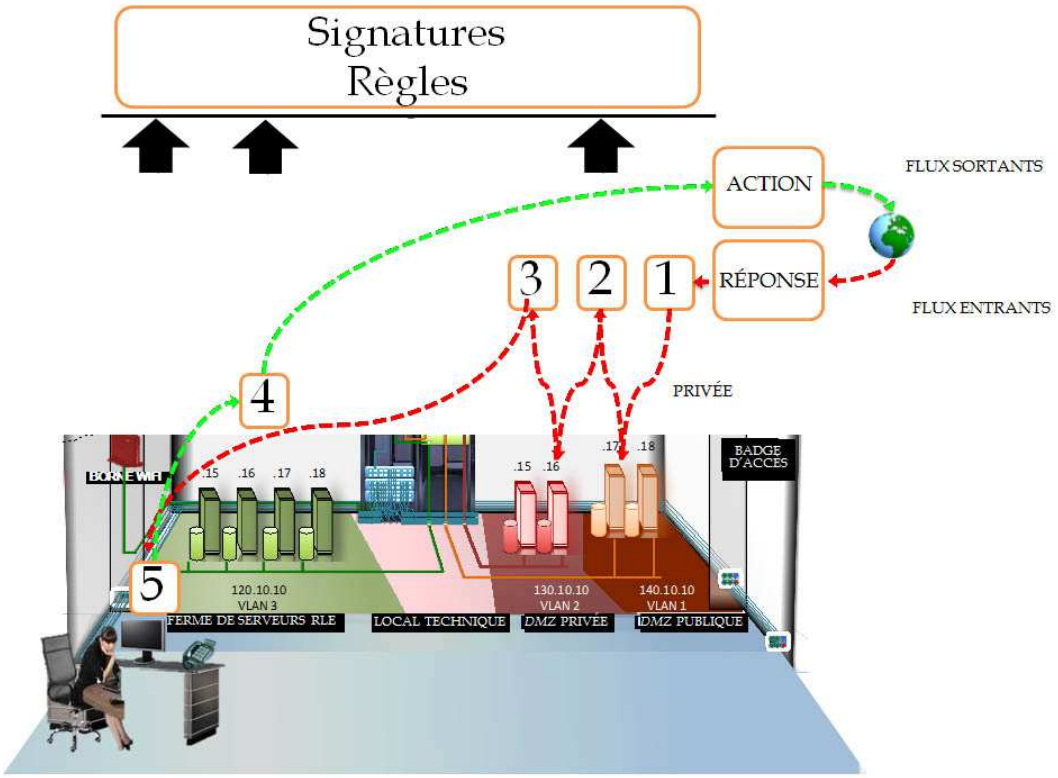
La difficulté de distinguer un individu ou même un système illégitime d'un système légitime a suggéré une fonction de détection d'anomalie qui tend à **considérer comme hostile toute activité ou flux se déroulant de l'autre côté d'une frontière appelée ligne de défense**. Cette même stratégie s'étant par ailleurs étendue aux activités internes.

1. L'analyse des flux

Le principe général consiste à soustraire tout bien exposé à la connaissance des attaquants. La zone de communication est le siège d'une multitude de filtres également appelés bastions. Leur rôle est d'affecter un laissez-passer à chaque flux légitime dont on sait identifier la source, la destination et le mode opératoire : ce sont **les flux maîtrisés**. Plusieurs mécanismes de filtrage de flux vont s'appliquer qui peuvent s'enchaîner et se compléter :

- le filtrage au moyen du pare-feu ;
- le filtrage des systèmes de détection d'intrusion (*IDS*) ;
- les antivirus.

Schéma n° 90 : Principe du filtrage de flux pour bloquer ou détecter les anomalies



***Source** : OPECST*

a) Filtrage au moyen du pare-feu

Ce type de filtrage concrétise les **règles** définies par les politiques de sécurité sous forme de : « ce que l'on peut faire et ce que l'on ne doit pas faire ». Une violation de ces règles provoque des alertes et entraîne un **blocage du flux**. On dit que **la sécurité est active**.

b) Filtrage (IDS)

La détection d'intrusion, grâce au système de détection d'intrusion, est une **sécurité passive**, dont l'objectif est d'informer l'analyste.

Le principe repose sur deux méthodes d'analyse différentes : **analyse sur signature** et **analyse sur comportement**. L'analyse fondée sur les signatures va tenter de déceler des intrusions en recherchant des codes, textes, *patterns* préalablement appris. L'analyse d'après le comportement

permet d'élaborer des profils de références de comportements – utilisateurs ou système. Ces profils de références sont étalonnés *via* des indicateurs qui permettent d'en **mesurer les déviances**. Cette méthode d'analyse, complémentaire de la première, offre **la possibilité de déceler des attaques encore inconnues**.

« **L'État va donner un label à des prestataires de confiance** chargés de détecter les vulnérabilités, les manquements des opérateurs critiques au cœur de leurs systèmes. Ils seront en relation avec l'État. Il y aura des prestataires de détection qualifiés par l'État, qui seront en contact avec l'ANSSI pour échanger sur les nouvelles menaces, **les nouvelles signatures techniques de comportement d'attaquant**. Ce sont ces critères techniques que l'on peut introduire dans les sondes automatiques **pour détecter que quelque chose d'anormal est en train de se passer** et que nous sommes *a priori* victimes d'une attaque. **Ces signatures sont désormais le bien le plus cher des agences de sécurité**. »

M. Pascal Chauve
Conseiller du Secrétaire général de la défense et de la sécurité nationale (SGDSN)
19 juin 2014
Auditions. Tome II du présent rapport

2. Le contrôle comme point fondamental, vers un contrôle multi-échelle

La question du déploiement d'un outil non contrôlé devient alors une question essentielle. **Comment peut-on demander à chacun d'être responsable de sa sécurité si aucun contrôle n'est possible** ? L'analogie avec l'automobile paraît appropriée : comment contrôler et répondre à des obligations légales et sécuritaires sans compteur de vitesse, tableau de bord, etc ?

C'est au travers des trois propriétés de la disponibilité, l'intégrité et la confidentialité que la sûreté de fonctionnement des systèmes est évaluée. Néanmoins d'autres propriétés de sécurité sont indispensables, par exemple l'« *accountability* » déjà mentionnée. Mais **on instrumente très peu les systèmes numériques dès leur conception au sein de leur écosystème**. Pourquoi ne pas mettre en place une normalisation imposant à tout système conçu des moyens de contrôle des trois propriétés de sécurité ?

CHAPITRE VII – LA CULTURE DU NUMÉRIQUE ET L'ÉDUCATION À SA SÉCURITÉ

À ce stade de la présente étude, vos rapporteurs entendent insister sur le décalage existant entre le recours permanent à l'outil numérique en perpétuel devenir et le manque de maîtrise de cet outil, doublé d'une absence de recul quant au recours plus ou moins opportun à son usage.

Comme les entreprises peuvent être désemparées face à cette situation dont les évolutions s'inscrivent dans des calendriers multiples et parfois contradictoires, l'ANSSI et des groupements d'entreprises ont élaboré des méthodes et conçu des guides pour aider les entreprises à bâtir leur sécurité numérique de manière rapide, cohérente et efficace.

Cela s'impose particulièrement face à l'extension de l'infogérance et à sa déclinaison dans l'informatique en nuage.

I. TEMPS ET CONTRETEMPS DE LA SÉCURITÉ NUMÉRIQUE

A. HYPERCONNEXION ET HYPORÉFLEXION

Le numérique a commencé par révéler qu'il permettait d'agir, le plus souvent de travailler, « ***en temps réel*** », ce qui voulait signifier immédiatement, ravalant les actions effectuées sans lui à une sorte d'irréalité singulière.

Puis les techniques ont permis non seulement une **accélération** des possibilités accompagnant ce « temps réel » mais également une **ubiquité permanente** accompagnée d'un **accès illimité à l'information et au savoir**.

Pour illustrer la véracité et la supériorité de ces nouveaux concepts et techniques, la création rapide de nouveaux empires économiques venait rendre très tangibles les promesses de ce monde supposé immatériel et sans limites.

Plongé très rapidement dans ce nouvel univers de la fin du XXe siècle, la meilleure preuve de l'adaptation de l'homme connecté a semblé être l'**hyperconnexion**.

Cependant, en suivant ce tempo soutenu, **le temps a manqué pour une observation, voire une réflexion, *a fortiori* pour une éducation et la construction d'une culture du numérique**.

La nécessité d'une telle construction se fait particulièrement sentir dans **les entreprises qui ont toutes non simplement besoin du numérique**

mais d'un numérique sûr. Sinon, c'est leur système nerveux qui risque d'être atteint jusqu'à compromettre leur existence.

Cette construction nécessite des matières fiables : matériels, logiciels, routeurs assortis de protocoles divers. Cela est rendu difficile par le caractère encore récent de l'usage du numérique et l'inadaptation plutôt prononcée des personnels quant à l'édification de la sécurité numérique. En effet, **utiliser quotidiennement toute la gamme des outils numériques, même avec brio, ne suffit pas à rendre les usagers responsables, c'est-à-dire conscients des impératifs rigoureux de la sécurité numérique**.

D'autant que cette sécurité ne pourra, souvent, être assurée qu'au prix de l'abandon de deux principes admis comme supérieurs à tous les autres sans avoir été discutés : la connexion immédiate et permanente, l'accélération de la rapidité.

Or, il ressort de nombre d'auditions que la sécurité implique d'abord, par exemple, une **analyse de la confidentialité des données** à protéger, de celles pouvant être stockées ou transmises de telle ou telle manière, sans oublier de se préoccuper des conditions de sécurité offertes par le ou les destinataires du message.

Toutes les données ne sont pas à protéger de la même manière. Il convient donc de les hiérarchiser par degré de confidentialité sans pour autant consacrer un temps excessif à ce classement.

Une fois classées, les catégories de données subiront **des traitements numériques différents**. Tout ne pourra être stocké dans les nuages informatiques ; la question du recours à des nuages souverains se posera aussi à cette occasion.

Le canal de transmission devra également être sélectionné après réflexion sur les garanties de sécurité qu'il offre.

Cela posera aussi la question de l'**homogénéité de la sécurité tout au long du canal de transmission du message**. Ainsi, le recours à un téléphone crypté n'offre de sécurité que si l'interlocuteur est équipé d'un appareil de même niveau technique.

Pour illustrer de manière très concrète les précautions élémentaires évoquées ci-dessus, il suffit de passer en revue des situations, très courantes, de la vie quotidienne des entreprises, d'en déduire des règles de prudence pratiques avant d'en tirer des principes généraux constituant l'hygiène informatique.

Le Réseau de Grandes Entreprises (CIGREF) – association regroupant cent trente grandes entreprises et organismes français ayant pour mission de « *promouvoir la culture numérique comme source d'innovation et de performance* » - a eu l'excellente idée de mettre en scène, de manière ludique, à travers un jeu sérieux appelé *Keep eye* ou « *Aie l'œil* », des situations affrontées par les personnels des entreprises, en transformant chaque joueur,

maillon faible supposé de la sécurité numérique, en « *ange gardien d'un salarié de l'entreprise* ».

Le scénario de ce jeu est consultable sur le site du CIGREF et **en annexe du présent rapport**.

Par exemple : que faire lorsque l'on trouve une clé *USB* ? Peut-on emporter un ordinateur à l'étranger, le recharger dans les aéroports, le laisser dans le coffre-fort de sa chambre d'hôtel ?

Certaines personnes entendues ont indiqué, par exemple, que pour se rendre dans certains pays, il était prudent d'emporter un ordinateur et un téléphone n'ayant jamais servi et de ne plus l'utiliser au retour.

Les plus prudents perfectionnent leur mot de passe, cryptent leurs messages, évitent de se connecter à tous les réseaux *Wi-Fi* proposés. Mais, souvent, les mots de passe choisis sont trop simples, le cryptage peu fiable et la confiance en des réseaux, des équipements autres ou en des interlocuteurs plus ou moins habituels conduit à adopter une attitude globalement imprudente alors même qu'elle revêt certaines apparences de la prudence.

Il peut s'agir aussi de simples règles de comportement à observer et dont le non-respect peut être constaté chaque jour dans tous les moyens de transports (trains, avions, etc.), dans les restaurants, les hôtels, au téléphone, etc.

Certains entreprises estiment utiles de recommander à leur personnel de veiller à ce que nul ne lise, en même temps qu'eux, les messages affichés sur l'écran de leur ordinateur.

Mais, là encore, souvent, la priorité accordée à la permanence de la connexion nuit à la sécurité de celle-ci.

La conscience de ces divers risques numériques progresse mais sans aller jusqu'à se traduire en actes réfléchis de prévention et de précaution érigés en règles de conduite permanentes… et à adapter en permanence. Ces contraintes sont mal vécues et ressenties comme antagonistes par rapport à la liberté qui semble caractériser le numérique.

Une anecdote, rapportée par plusieurs personnes entendues, illustre la difficulté de concilier efficacité et sécurité ainsi que le fait que l'efficacité immédiate risque de compromettre les buts qu'elle est censée viser.

« Un exemple bien connu, en matière de vente d'avions, dans la concurrence entre *Airbus* et *Boeing*, quand M. Édouard Balladur était Premier ministre : il a pris l'avion pour l'Arabie Saoudite et il n'y avait que deux personnes connaissant le prix qui allait être proposé pour cette vente qui allait être signée. Le Premier ministre a passé une communication téléphonique depuis l'avion avec une des deux personnes en charge de la négociation mentionnant ce prix et, à l'atterrissage, il été constaté qu'une offre financière juste un peu meilleure venait d'être effectuée par *Boeing*.

À l'époque les communications chiffrées n'existaient pas ou étaient très peu efficaces. Et la *NSA* avait déjà mis en place *Echelon*. **Maintenant elles existent mais ce n'est pas forcément pour autant que les hommes politiques les utilisent**. *Teorem* existe : ce téléphone sécurisé permet de chiffrer les données, de chiffrer la voix, de tout chiffrer. Mais il reste dans la boîte à gant des voitures des autorités. »

M. Jérôme Notin
Président, NOV'IT
19 février 2014
Auditions. Tome II du présent rapport

À partir de ces observations quotidiennes et de ses connaissances techniques, l'**ANSSI a élaboré des règles d'hygiène informatique** rassemblées dans un guide consultable sur le site de l'ANSSI. Le résumé de ces quarante règles figure en annexe du présent rapport.

Là encore, comme pour le jeu sérieux mis au point par le CIGREF, nombre de ces règles, ou leur utilité, ont été rappelées par les personnes entendues par vos rapporteurs.

Dans les propositions de recommandations, la plupart des règles d'hygiène informatique imaginées par l'ANSSI sont rappelées pour mieux mettre en perspective par rapport à elles les recommandations proposées.

B. DES PRIORITÉS QUI RALENTISSENT

Un exemple de contretemps dans l'évolution du numérique est fourni par la **coexistence, pour l'heure non convergente, de priorités mondiales, internationales, européennes et nationales** en partie déjà évoquées plus en détail dans le chapitre premier du présent rapport.

En France, un projet de loi sur le numérique est annoncé depuis le début de l'actuel quinquennat présidentiel.

Depuis 2012, un projet de règlement et un projet de directive sont en gestation dans les institutions de l'Union européenne.

À partir de 2013, la volonté de négocier à marche forcée puis de conclure aussi rapidement que possible un Traité économique de partenariat transatlantique (*TAFTA*) incluant le numérique, vient interférer avec les deux projets d'évolution des règles européennes mentionnées ci-dessus.

En outre, **la nécessité d'un texte international régissant la gouvernance mondiale de l'Internet est de plus en plus souvent évoquée**.

Ces quatre priorités risquent de mal se concilier.

Si le traité transatlantique est conclu en premier, la liberté de l'Union européenne est bridée d'autant. De même pour la France par rapport à

l'Union européenne, où ce qui relève de la subsidiarité risque d'être affecté par des règles dont la cohérence risque de ne pas s'embarrasser de la hiérarchie des normes juridiques.

Face aux quatre rythmes mondial, international, européen et national, influant finalement sur le sens des dispositions à adopter relatives au numérique, il n'est pas évident qu'une perception aiguë de l'enjeu dicte en permanence la politique gouvernementale française ou celle des autres États membres de l'Union européenne.

À cet égard, vos rapporteurs émettent l'idée nouvelle de prise en considération, de caractère vital, du numérique pour affirmer **l'exigence de l'affirmation d'une exception numérique dans les négociations internationales**.

Celle-ci ne viendrait pas se juxtaposer à l'exception culturelle mais l'engloberait.

II. LES ACTEURS DE LA SÉCURITÉ NUMÉRIQUE

Si l'ANSSI se situe à la pointe des avancées en faveur de la sécurité numérique des entreprises, d'autres initiatives viennent utilement compléter son action comme, par exemple, récemment, celle de la création du club des industriels de la cyberdéfense.

A. LES CONSEILS DE SÉCURITÉ DISPENSÉS AUX INDUSTRIELS PAR L'ANSSI

1. L'infogérance

L'apport et les limites des conseils donnés par l'ANSSI aux industriels ressortent de ses divers guides de bonnes pratiques, dont celui sur les règles d'hygiène informatique, dont les quarante préconisations sont rappelées dans les propositions des rapporteurs à la fin de la présente étude.

Un autre exemple est fourni par le guide de l'ANSSI intitulé « *Maîtriser les risques de l'infogérance* » relatif à l'externalisation des systèmes d'information.

Sans analyser l'ensemble de cet intéressant document, certains conseils dispensés par celui-ci situent bien l'équilibre à rechercher entre recours accru au numérique et sécurité, non seulement des systèmes d'information de l'entreprise mais encore de la sécurité de l'entreprise dans son ensemble, dans la mesure où, comme déjà souligné, un affaiblissement de son système nerveux numérique pourrait conduire à sa disparition.

Recourir à un tiers pour gérer son système d'information, telle pourrait être la définition de l'externalisation de l'infogérance.

Il peut s'agir de gérer des infrastructures, des applications ou encore de l'hébergement de service.

Pour vos rapporteurs, la question consiste à se demander si les risques inhérents à l'infogérance – du fait de la **sous-traitance** simple ou en cascade à laquelle le prestataire peut recourir, du fait de l'**incertitude sur la localisation des données**, notamment dans l'informatique en nuage, du fait, enfin, du **risque de divulgation de données sensibles**… – excèdent ou non les avantages à attendre de cette infogérance.

Ce risque est particulièrement sensible en ce qui concerne les données à caractère personnel dont le responsable de traitement est comptable ; des sanctions pénales venant même sanctionner ses manquements éventuels.

L'ensemble de ces éléments doit inciter le chef d'entreprise qui a recours à l'infogérance à mûrement peser les termes du contrat le liant au prestataire d'infogérance sécurisée.

Ce contrat devrait préciser que le client a un droit de contrôle sur :

- **le choix des sous-traitants** ;

- les **modalités de paiement** de ceux-ci ;

- la **sécurité des lieux d'hébergement de données** proposés ;

- l'existence d'un **contrat liant le prestataire à ses sous-traitants** (comprenant des clauses relatives à la sécurité et à la confidentialité offertes par les sous-traitants) ;

- la valorisation pour le client de **choix de nouvelles solutions matérielles ou logicielles** par le prestataire, notamment s'il s'agit de recourir à des **applications propriétaires peu répandues** car le client doit pouvoir **obtenir, à tout moment, la restitution de ses données dans un format standard et ouvert**.

L'énumération des clauses protectrices indispensables à prévoir dans le contrat conduit à s'interroger sur la possibilité pratique de mettre en œuvre un contrôle réel du client sur ces éléments multiples et très techniques si le rapport de force face au prestataire d'infogérance ne joue pas à son avantage.

Il convient de souligner également **un risque particulier, celui des interventions à distance**.

L'entreprise sera tentée de réclamer la possibilité de ce genre d'interventions dans l'espoir d'une réduction du coût et de la rapidité des délais d'intervention.

Mais il faut mettre en regard de ces deux gains espérés **les nombreux risques propres aux interventions à distance**.

Parmi ceux-ci, il est possible de citer : des **mots de passe pas assez sécurisés**, des **failles dans les interfaces d'accès**, des **systèmes d'exploitation non mis à jour**, l'**absence de traçabilité des actions**, sans parler de **l'insuffisante prise en compte de la sécurité informatique en général par les personnels des dispositifs de télémaintenance**.

Autant de **risques de nature à faciliter les intrusions**.

Il incombe alors au client de se prémunir contre ces risques en menant une véritable analyse de risques qui lui permettra d'exiger tout document de nature à le rassurer sur les mesures de sécurité techniques et organisationnelles proposées par le prestataire.

Pour l'ANSSI, les dispositifs de télémaintenance ne sauraient être considérés comme sûrs sans la mise en place d'une passerelle sécurisée, seule à même de garantir un niveau d'authentification, de prévention, de confidentialité et d'intégrité des données, de traçabilité des actions effectuées par le centre de support, etc.

Et **ce recours à une passerelle sécurisée doit passer par un audit de celle-ci**.

De plus, au risque lié à la **perte de maîtrise de son système d'information**, augmenté de celui résultant des interventions à distance, peut s'ajouter celui de **l'hébergement mutualisé**, c'est-à-dire de l'hébergement de plusieurs services sur un même serveur.

Dans ce cas, **le service ayant la vulnérabilité la plus importante risque d'accroître la vulnérabilité des autres services**.

Par exemple, une attaque par déni de service entraînant une perte de disponibilité d'un serveur peut compromettre du même coup d'autres services hébergés par le même serveur en les rendant également indisponibles.

En réalité, l'ANSSI estime que « *Le fait de voir les services partager le même environnement physique peut conduire à des croisements d'information (contenu de fichiers clients de plusieurs sites dans la même base de données, ou le même sous-répertoire, etc.). **Les risques auxquels s'expose un service cohébergé sont donc augmentés de façon significative dans un environnement non maîtrisé.*** »

De plus, l'**ANSSI estime que l'hébergement mutualisé compromet une analyse rapide et pertinente des incidents – l'hébergeur refusera de communiquer les journaux d'événements du serveur et de ses équipements périphériques** afin de ne pas nuire à la confidentialité des autres services hébergés.

Encore une fois, **il est primordial que le contrat conclu entre le client et l'hébergeur soit extrêmement précis** quant aux modalités de l'hébergement incluant sa **réversibilité** mais également la communication des **journaux des événements**, le **suivi attentif** du service hébergé (mises à

jour, maintenance, etc.), les **modalités de prévention des attaques** et les **réactions face aux incidents**.

2. Une forme particulière d'infogérance : l'informatique en nuage

Dans cette forme d'infogérance, ni l'emplacement ni les modalités de fonctionnement du nuage informatique (*cloud computing*) ne sont portés à la connaissance du client.

Le nuage informatique peut proposer la fourniture :

- de **machines virtuelles** permettant d'installer à distance le système d'exploitation et les applications de son choix (*Infrastructure as a Service*) ;

- de **plates-formes** permettant le développement à distance d'applications (*Platform as a Service*) ;

- d'**applications** directement utilisables à distance (*Software as a Service*).

Les risques de l'infogérance décrits ci-dessus sont également présents dans l'informatique en nuage.

Les réserves émises précédemment sont encore bien plus pertinentes dans le cadre de l'informatique en nuage car **il ne s'agit plus seulement de la difficulté de négocier un contrat mais de l'impossibilité d'y procéder puisqu'il s'agit généralement de souscrire à des offres par validation de contrats types** !

La localisation des données à tout moment est impossible dans le nuage numérique, d'où une **incertitude sur le droit applicable** ; en l'absence de certitude sur cette localisation, **le principe de territorialité est battu en brèche**.

Et cela est contraire aux recommandations du rapport du Conseil d'État de 2014, analysées précédemment.

Dès lors, **quelles sont les juridictions compétentes et le droit applicables** ?

À ces incertitudes vient s'ajouter la **perte de contrôle du client sur la gestion des incidents de sécurité**.

En outre, il deviendra **difficile de changer de prestataire car la portabilité des données n'est pas toujours garantie dans les contrats types**.

Comme déjà souligné à propos de l'infogérance en général, **l'intégrité et la confidentialité des données risquent d'être compromises** en raison d'une importante dégradation du stockage et de la mémoire.

Enfin, en supposant que le client se soit décidé à quitter un prestataire de nuage ne lui donnant pas satisfaction, **rien ne garantit l'effacement ou l'absence de duplication des données confiées**.

Il convient d'être particulièrement attentif à la nationalité des prestataires de nuages informatiques et à la localisation de leurs serveurs dans l'Union européenne ou en France si l'on souhaite ne pas abandonner tout contrôle sur ses données à caractère personnel.

À noter, toutefois, que **la localisation, en elle-même, ne constitue pas une garantie de sécurité mais seulement une présomption**.

À l'opposé de ce saut dans l'inconnu, une **analyse de risque** devrait permettre de mieux cerner les objectifs de sécurité à poursuivre face aux risques acceptés, refusés ou éventuellement transférés à une assurance.

Une telle analyse devrait permettre de conclure le contrat avec le prestataire en toute connaissance de cause et en gardant à l'esprit que, en ce domaine, loin de figer totalement une situation, le contrat doit prévoir la prise en compte d'évolutions inhérentes au domaine du numérique.

Cette évolution peut être observée grâce à la mise en place d'un comité de suivi de la sécurité numérique permettant de favoriser la **prise en compte de failles de sécurité nouvelles**, par exemple.

Des audits de sécurité complèteraient utilement l'action de ce comité.

Tous les risques soulignés ci-dessus peuvent-ils être gérés, même de manière calculée, par des opérateurs d'infrastructures vitales ? Non.

D'autant moins que, depuis la loi de programmation militaire de 2013, **face à des attaques, terroristes ou non, le Premier ministre a le pouvoir de décider de la mise en œuvre de mesures spécifiques tendant à protéger notamment les systèmes d'information et les réseaux de télécommunications des opérateurs d'infrastructures vitales**.

Il peut s'agir, par exemple, d'une **augmentation de la sauvegarde des traces**.

B. LES INITIATIVES DES INDUSTRIELS EN MATIÈRE DE SÉCURITÉ NUMÉRIQUE

Les industriels sont les premiers à avoir conscience des vulnérabilités du numérique et de la complémentarité des solutions à mettre en œuvre pour y remédier.

C'est pourquoi, outre les initiatives prises à l'intérieur même de leurs entreprises, ils ont mis en place nombre d'instances de réflexion et d'action.

Parmi celles-ci figurent le réseau de grandes entreprises (CIGREF), le Comité de la filière industrielle de sécurité (CoFIS).

Ces initiatives sont en phase avec celles prises en matière de cyberdéfense.

« Partout où il y a de l'informatique et des échanges de données, nous sommes en présence d'un espace attaquable, qu'il faut apprendre à défendre. **Si nous ne maîtrisons pas le cyberespace, nous ne maîtrisons aucune capacité opérationnelle.** »

Contre-amiral Arnaud Coustillière
Officier général cyberdéfense
État-major des armées - 2014

C'est pourquoi la cyberdéfense est l'une des deux priorités nationales fixées par le Livre blanc sur la défense et la sécurité nationale de 2013.

Six mois après le lancement du plan national de cyberdéfense, se concrétisant par le Pacte Défense cyber 2016, assorti de **cinquante mesures**, et par le Pacte défense PME – qui concernent aussi bien la formation et la recherche que les entreprises –, le ministre a souhaité accélérer la mise en œuvre du volet industriel de ce plan car il considère que l'espace numérique est un nouveau champ de bataille de ce que pourrait être une cyberguerre.

Récemment, le ministre de la défense a été à l'origine d'une initiative consistant à créer le club des industriels de la cyberdéfense.

Pour ce faire, le club des industriels de la cyberdéfense devrait réunir, notamment, *Airbus Defense and Space*, *Alcatel, Atos / Bull, Orange, Sony, Sagem, Thales*, auxquels viendraient s'ajouter des petites et moyennes entreprises ainsi que de grands clients, dont les opérateurs d'infrastructures vitales de secteurs stratégiques comme ceux de l'énergie, des transports et des banques.

Ce rassemblement permettrait de mieux définir les besoins en matière de protection des réseaux informatiques pour que l'offre des fournisseurs puisse s'y adapter.

À travers cette initiative serait saisie l'occasion **d'améliorer la formation de tous les collaborateurs de ces entreprises**, d'apporter un **savoir-faire mieux protégé, d'expérimenter des solutions** et de **qualifier des produits et des services**.

À noter que l'armée se livre déjà à des exercices de guerre électronique. C'est ainsi que, en septembre 2014, l'exercice *Defnet 2014* se fondait sur le scénario d'une **attaque des réseaux d'une base aérienne par des pirates informatiques** exploitant une vulnérabilité d'un des sous-traitants des installations militaires de cette base.

La détection de l'attaque, l'identification puis la neutralisation des assaillants ont constitué les phases de cet exercice.

Pour l'avenir, des plates-formes seront mises en place pour assurer la formation, l'entraînement à la gestion des cyberattaques et l'expérimentation de nouveaux produits de sécurité informatique.

Le Pacte Defense cyber, en son axe 6, prévoit de **favoriser l'émergence d'une communauté nationale de cyberdéfense** en s'appuyant sur un cercle de partenaires et les réseaux de la réserve.

À noter que la loi de programmation militaire 2014-2019 prévoit de **tripler les moyens alloués à la cyberdéfense** et d'augmenter les effectifs grâce à la **création de 550 postes, dont 200 postes d'ingénieurs à la DGA**, de 2014 à 2019.

Au-delà des capacités défensives, il est maintenant affirmé que **la nécessité de capacités offensives en cybersécurité s'impose**. C'est aussi sous ces angles qu'une très grande importance est accordée à la base industrielle de technologie et de défense.

III. FAIRE DE L'ÉCONOMIE AVEC DU DROIT ?

En dépit des règles régissant la protection des données individuelles au niveau national et européen, la protection des données individuelles et de l'entreprise dans l'entreprise ne paraît pas assurée.

Pour y remédier, des efforts d'éducation sont à entreprendre, des prises de conscience à accomplir mais aussi de disposer de matériels et d'outils fiables.

Quant aux matériels, ni la France ni les autres États de l'Union européenne ne sont à même, seuls, de garantir un usage souverain rentable de l'ensemble des composants, ordinateurs, logiciels, réseaux utilisés, qu'ils soient ou non conçus ou fabriqués dans d'autres parties du monde.

Quant aux outils, ces matériels étant reliés entre eux, à d'autres objets, à des logiciels et, enfin, à leurs utilisateurs, il convient de faire en sorte que la chaîne d'interaction qui les relie puisse être l'objet de recours juridiques, soit en tant que chaîne, soit en tant qu'élément individuel indispensable à la sécurité de l'ensemble.

Au cours de la centaine d'auditions menées par vos rapporteurs, il leur est en effet apparu que les éléments techniques de la sécurité du numérique dépendaient souvent de règles juridiques indépendantes les unes des autres. Il conviendrait de donner une cohérence d'ensemble reliant chaque élément de la chaîne numérique et garantissant l'usage de celles-ci. La France dispose en la matière de nombre d'atouts dans le domaine du droit numérique, qu'il serait souhaitable de mobiliser pour en faire des instruments de puissance économique à l'échelle internationale.

Un exemple : la cryptographie. À de nombreuses reprises, celle-ci a été citée comme un élément clé de la transmission sécurisée des messages numériques. Il se trouve que, grâce à l'école française de mathématiques, parmi les toutes premières dans le monde, grâce à la recherche menée dans ce domaine, notamment par l'armée au sein de la Délégation générale pour l'armement, **cet atout peut faire partie de ceux à développer en priorité** pour faire face à l'insécurité numérique de plus en plus évidente à laquelle se trouvent confrontées les entreprises et la société en général. Enfin, la France dispose encore d'une considérable capacité en matière de langues et de linguistique, capital qui pourrait être valorisé aussi au profit des outils du numérique.

Il semble alors prioritaire de former à la cryptographie, de favoriser la recherche dans ce domaine, d'aider les jeunes créateurs d'entreprise à se diriger vers cette activité, de les soutenir jusqu'à la consolidation de leur entreprise – ce qui suppose de les aider à passer le stade où ils risquent d'accepter que des sociétés nord-américaines rachètent leur entreprise.

Parallèlement, les lacunes observées dans la sécurité numérique des entreprises peuvent conduire à l'adoption de nouvelles règles de droit pérennes de manière à favoriser l'apparition de nouveaux marchés.

Quels sont les besoins non satisfaits ? Ils sont nombreux et vont des **sondes souveraines** à la **cartographie des risques** ; des **détecteurs d'intrusion** à la **réalisation d'audits** de sécurité numérique ; de la **formation au codage** dès la maternelle à la **réalisation de jeux de travail** (ou *serious games*) pour accélérer et ancrer les réflexes conditionnant la sécurité numérique.

La coopération déjà existante entre la CNIL et l'ANSSI peut aider à concevoir et à mettre en place les nouvelles règles de droit nécessaires et leur traduction pratique. Les préconisations de vos rapporteurs vont dans ce sens : simplifier l'accès au numérique en protégeant mieux le citoyen et les entreprises.

Au-delà, dans le cadre des trente-quatre plans de la Nouvelle France industrielle lancés le 12 septembre 2013, **pas moins d'une quinzaine d'entre eux concernent très directement le numérique** (logiciels et systèmes embarqués, textiles techniques et intelligents, réseaux électriques intelligents, santé numérique, *Big data, cloud computing,* e-Éducation, souveraineté télécoms, objets connectés, réalité augmentée, services sans contact, supercalculateurs, robotique, usine du futur) **et l'un d'eux la cybersécurité**. Ils doivent être suivis avec attention par le Gouvernement et par tous les acteurs de la filière.

Le plan cybersécurité vise à **construire « *la France de la sécurité et de la confiance numérique* »** au moyen d'une industrie performante en matière de cybersécurité pour **relever un défi de souveraineté et saisir une**

opportunité. Il a des objectifs ambitieux comme celui de la **sécurisation des infrastructures les plus vitales** pour assurer la défense comme la sécurité du pays et protéger la vie quotidienne des Français ; les objectifs de souveraineté reposant sur la **protection des secrets numériques**.

Ce plan représente une opportunité, car il est porteur de créations d'emplois puisque la France possède, en ce domaine, des acteurs industriels de rang mondial et un tissu de PME capables de relever ce défi.

Le plan ambitionne d'accroître significativement la demande en **solutions de cybersécurité de confiance** ; développer, pour les besoins nationaux, des **offres de confiance ;** organiser la **conquête de marchés étrangers** et **renforcer les entreprises nationales de cybersécurité** pour qu'une offre de confiance nationale existe et soit mieux prise en considération par les commanditaires publics et privés nationaux et davantage valorisée à l'export.

Cette offre de confiance repose sur un effort de gouvernance et de valorisation de la recherche et du développement pour tirer tout le bénéfice d'un tissu industriel national large, mais parfois trop dispersé (plus de six cents acteurs). Il reste à le consolider tout en évitant les risques de concurrence stérile ou de rachats inappropriés portés par l'éparpillement actuel. Sans omettre surtout de profiter des extraordinaires opportunités de conquête de parts de marché que les regroupements ou adossements peuvent offrir.

Les industriels n'ont d'ailleurs pas attendu le plan cybersécurité pour se mobiliser et manifester leur créativité. Tel est le cas, par exemple, du CoFIS, du CIGREF, du Club des directeurs de sécurité informatique, tous entendus par vos rapporteurs.

Et leurs efforts se conjuguent avec ceux des filières de formation, à en juger par l'audition des directeurs de grandes écoles.

Vos rapporteurs tiennent à insister sur la nécessité de clarifier les règles juridiques à imaginer dès le futur projet de loi sur le numérique annoncé pour le début de l'année 2015.

Le rôle de l'OPECST à cette date consistera à présenter à la commission des affaires économiques du Sénat, qui l'a saisi de la présente étude, ce rapport et ses recommandations.

Au-delà de cette première présentation, il serait opportun d'élargir cette démarche habituelle à d'autres commissions attentives au numérique et à sa sécurité, tant à l'Assemblée nationale qu'au Sénat et, évidemment, de remettre officiellement le présent rapport aux instances gouvernementales concernées dont, en premier lieu, la secrétaire d'État en charge du numérique, Mme Axelle Lemaire, entendue dans le cadre de la journée d'auditions publiques du 19 juin 2014.

À noter que, récemment, le 10 novembre 2014, Mme Axelle Lemaire a adressé une lettre au Président de l'OPECST lui indiquant que le numérique constituait, plus que jamais, une priorité du Gouvernement qui souhaite **construire une** « ***République numérique*** ».

C'est ainsi que : « ***Le Premier ministre a décidé de placer la transition numérique au premier rang des priorités de l'action du Gouvernement*** ».

Le présent rapport s'inscrit dans la grande concertation sur le numérique, devant s'achever au début du mois de février 2015, pour « *nourrir le projet de loi numérique* ».

Les règles à mettre en place doivent être mûrement réfléchies pour que le numérique soit un facteur de développement économique qui place la France au premier rang européen et international.

Vos rapporteurs ont montré dans ce rapport que des groupes de pression puissants sont à l'œuvre à Bruxelles pour retarder au maximum l'adoption du projet de règlement afin qu'il ne vienne pas interférer avec la négociation du traité commercial transatlantique.

Pendant ces divers temps, dont certains indispensables et d'autres parasitaires, la fabrication des matériels et des outils numériques en Asie s'affirme.

Faire de l'économie avec du droit ? Cela est possible et nécessaire pour s'inscrire dans la révolution numérique en cours. Elle s'y prête bien, étant présente partout et en tout.

Cela peut supposer de bouleverser quelque peu les rapports que les divers acteurs, plus ou moins conscients, de cette révolution ont l'habitude d'avoir entre eux.

Cela concerne aussi bien les chercheurs que les jeunes créateurs d'entreprise, les patrons de PME, les opérateurs d'importance vitale, les collectivités territoriales, les administrations et les gouvernements.

Enfin, comment ne pas avoir à l'esprit que, pendant la conception et la réalisation de cette révolution numérique aux enjeux essentiels et mondiaux, l'espionnage et les actions d'intelligence économique continuent ?

CONCLUSION

Après s'être interrogés, de manière prioritaire, pendant plusieurs mois sur le risque numérique avec l'aide de la centaine de personnes entendues, qui, toutes, ont tenu à faire partager avec patience le meilleur de leurs connaissances, vos rapporteurs reviennent devant l'OPECST, qui leur a fait l'honneur de les désigner, avec une moisson de recommandations.

« Trop », diront certains ? « Trop précises », selon d'autres ? « Utopiques » ou « Excessivement techniques », d'après des lecteurs aux avis opposés mais également critiques.

Face à ces appréciations, vos rapporteurs avouent qu'ils ignoraient totalement le type et le nombre de recommandations qu'ils formaliseraient au terme de leurs investigations. Tout comme, au début de leurs travaux, ils auraient également été bien en peine d'entrer dans la technicité de certaines de leurs actuelles propositions.

Mais, aujourd'hui, face à l'ampleur et la complexité du risque numérique, vos rapporteurs regrettent de mettre un terme à ce rapport alors que tant d'autres idées leur viennent.

Et d'abord celle-ci : **le risque numérique, une fois analysé, peut constituer une opportunité pour des démarches créatives aux retombées non négligeables**.

C'est à cette condition que le risque peut éviter de se muer en danger. Mais cette condition préalable de compréhension, seule à même de permettre de se saisir à bon escient de l'outil numérique, exige de nouvelles attitudes de la part de chacun, dans sa vie privée comme dans sa vie sociale, dont la vie professionnelle, au sein, éventuellement, d'entreprises, en particulier celles jugées d'importance vitale.

À la commission des affaires économiques du Sénat, auteur de la saisine à l'origine de ce rapport, vos rapporteurs répondent aujourd'hui, avec encore plus de certitudes qu'au moment de l'étude de faisabilité, que l'exploration du risque numérique est pleinement justifiée et que cette démarche trouve sa justification dans les actions vitales à en déduire.

L'humanité a cru, jusqu'à présent, mettre le numérique à son service. Aujourd'hui, les développements du numérique sont tels qu'un basculement a commencé à s'opérer : **le numérique façonne une humanité différente, hyperconnectée mais encore plus fragile**, s'en remettant à des protections dont l'apparente puissance risque de décevoir.

C'est pour cela que vos rapporteurs ont souhaité **tester le potentiel théorique de solidité, de résistance et de résilience de rouages particulièrement sensibles des sociétés modernes, à savoir les entreprises**

bien particulières que constituent les opérateurs d'importance vitale, et en se focalisant d'abord sur deux secteurs, celui des **télécommunications** et celui de l'**énergie**.

Cet examen a révélé l'extrême imbrication de ces opérateurs dans le tissu social, l'impossibilité de conforter la sécurité numérique seulement autour d'eux alors qu'ils innervent la société dont ils n'illustrent que la fragilité la plus évidente.

Il a été constaté aussi qu'une sécurité numérique n'est pas simplement à attendre de matériels, de logiciels, d'antivirus ou de pare-feu divers face à d'autres matériels, logiciels, etc., car **les vulnérabilités majeures résident en l'homme**.

Les attaques numériques les plus abouties sont fondées sur la faiblesse de ce maillon technologique.

Dès lors, **pour réduire le risque numérique, il s'agit d'éducation, de sensibilisation, d'acquisition de réflexes, d'un savoir se comporter face au numérique** plutôt que d'une science ou d'une technologie numérique imposant leur logique binaire.

Pour être maître de lui-même, **l'homme numérique, tout à la fois augmenté et diminué,** 1 puis 0 tour à tour, doit s'interroger sur son rapport au monde, sur la souveraineté numérique dont il peut attendre protection et initiatives à un rythme accéléré par rapport aux évolutions sociétales antérieures.

Ces questions doivent être pensées à partir d'analyses provenant d'horizons multiples et filtrées par des forums de discussion nouveaux, originaux, multidisciplinaires. Certains sont déjà en place.

Un tel dialogue a été modestement esquissé lors des trois auditions publiques organisées par vos rapporteurs tant à l'Assemblée nationale qu'au Sénat. Il doit maintenant se poursuivre activement dans les mondes de l'éducation ou de l'entreprise notamment.

Puissent les recommandations adoptées par l'OPECST favoriser et nourrir ces mutations.

RECOMMANDATIONS

Au début de leur travail d'investigation, vos rapporteurs ont proposé au président de la commission des affaires économiques du Sénat, à l'origine de la saisine de l'OPECST, de limiter le champ du rapport aux opérateurs d'importance vitale, les OIV et, parmi eux, aux secteurs des télécommunications et de l'énergie, stratégiques pour l'économie française et l'indépendance nationale.

Il leur est apparu aussi que **les failles de sécurité, liées aux matériels, aux attaques mais aussi aux comportements au sein des OIV ne pouvaient être totalement dissociées de leur environnement et ne faisaient qu'attirer l'attention sur les failles identiques mais encore plus béantes, existant chez les filiales, les sous-traitants, les clients des OIV, sans parler des utilisateurs quotidiens du numérique qui sont les personnels des entreprises.**

Au terme de la centaine d'auditions réalisées par les rapporteurs, il leur semble évident que **l'omniprésence du numérique dans la vie sociale et individuelle actuelle fait de sa sécurité un enjeu majeur**.

L'imbrication des réseaux numériques, leur impact et leurs vulnérabilités rendent nécessaire une appréhension globale des exigences de la sécurité numérique.

C'est pourquoi les recommandations ci-dessous présentent une architecture *a priori* complexe, seule à même de se situer à la hauteur des défis mouvants à relever dans un temps record.

Ces recommandations proviennent de l'analyse des informations recueillies lors des auditions et s'ordonnent autour de plusieurs éléments du socle de base des travaux de l'ANSSI intitulé « *Guide d'hygiène informatique* » – utiles à rappeler car ces règles ne sont pas toujours connues et encore moins suivies par les personnes concernées.

Les rapporteurs ont souhaité émettre des recommandations en cohérence avec les préconisations de l'ANSSI tout en allant au-delà et approfondir les idées recueillies lors des auditions.

Chacune de ces sources est identifiée dans les propositions de recommandations adoptées par l'OPECST.

Vos rapporteurs ont la conviction que cette construction permettra d'appréhender différemment le concept de sécurité numérique, d'en cerner les limites, d'y introduire de la confiance et de proposer des pistes pour donner des prolongements économiques aux idées novatrices indispensables à mettre en œuvre.

En outre, après une première série de **recommandations d'ordre général** et plutôt politiques, un ***vade-mecum*** **de recommandations de sécurité numérique à l'usage des entreprises** est proposé.

RECOMMANDATIONS D'ORDRE GÉNÉRAL

I. DÉVELOPPER UNE CULTURE DU NUMÉRIQUE : FORMER ET INFORMER MASSIVEMENT TOUTES LES CLASSES D'ÂGE À L'INFORMATIQUE, DANS TOUS LES MILIEUX SOCIAUX

- **Éduquer au numérique au sein du système éducatif, dès l'école maternelle et jusque dans l'enseignement supérieur, tout au long de la vie –** notamment au moyen de la formation continue, particulièrement dans les branches professionnelles :
  - ✓ former à c**omprendre ce qu'est le numérique** plutôt que de se contenter d'apprendre à utiliser les outils du numérique ;
  - ✓ enseigner les **symboles du numérique**, les **bases du codage et de la programmation**, les principes du **cryptage**.

- **Éduquer à la sécurité** :
  - ✓ enseignement de l'informatique à l'école : **y inclure la sécurité informatique** à travers les règles d'hygiène informatique et former au risque numérique ;
  - ✓ programmes de l'enseignement supérieur : **renforcer les moyens de la formation universitaire en matière de cybersécurité** et y introduire des modules de **formation à la sécurité informatique** incluant l'hygiène informatique en allant jusqu'à la validation de formations diplômantes dans cette discipline ;
  - ✓ **favoriser également d'autres types de formation, y compris expérimentales** ;
  - ✓ créer un pôle de recherche à ambition européenne dans le domaine de la cybersécurité civile, en plus du pôle militaire de l'ouest de la France ; celui-ci pourrait s'appuyer sur l'INRIA et avoir vocation à développer la coopération européenne ;
  - ✓ formation initiale et continue des fonctionnaires et magistrats de la justice et de la sécurité civile : y inclure une **sensibilisation au risque numérique et à la sécurisation du numérique**.

- Instaurer dans les entreprises un permis d'aptitude à utiliser le numérique en toute sécurité **– sorte de permis de conduire numérique**, en assurant la

mise à niveau régulière de ses détenteurs pour faire face aux évolutions très rapides dans ce secteur (*retombées économiques possibles*).

- Mener des **campagnes de prévention sur le thème de la sécurité informatique** en direction du grand public comme des professionnels :
  - ✓ diffuser des programmes de sensibilisation à la sécurité numérique à la **radio**, à la **télévision**, aux heures de grande écoute et en assurer l'a présence sur l'**Internet**.

- Sensibiliser les utilisateurs, les responsables, à l'aide de **plates-formes de démonstration d'attaques informatiques et de tests de résistance** (*retombées économiques possibles*).

II. ASSURER LES CONDITIONS D'UNE AUTONOMIE NUMÉRIQUE POUR PRÉSERVER LA SOUVERAINETÉ

- **Développer des équipements de détection d'attaques informatiques français** (bénéficiant du financement du Programme d'investissements d'avenir) et des laboratoires de haute sécurité (*retombées économiques possibles*).
- Définir des cercles de confiance appropriés à la sécurité numérique.
- Élaborer une **doctrine française de la cybersécurité à l'usage des entreprises** – voir ci-après le *vade-mecum* de recommandations de sécurité numérique à l'usage des entreprises – **des citoyens et des administrations**.
- Mettre en place un cadre européen unifié favorable à la **sécurisation des données des citoyens européens**.
- **Créer l'équivalent d'un *Google* souverain français ou européen** – après l'Aérospatiale ou l'Ariane européennes – tout comme la Chine, l'Inde et la Russie développent actuellement des Internets en propre (pour des questions de langages et d'alphabets, etc.). *L'Europe bénéficierait de retombées économiques possibles*.
- **Soumettre au droit français les sociétés gérant des serveurs sur le territoire national et les clients français des sociétés gérant des serveurs hors du territoire national.**
- Dans la mesure où le droit ne permet pas, aujourd'hui, de trouver des solutions aux problèmes rencontrés, par exemple, dans l'affaire d'espionnage généralisé de la diplomatie et des industriels français, **autoriser les laboratoires spécialisés, civils comme militaires, à mener**

des recherches à visées offensives dans le domine dual de la cybersécurité.

- **Renforcer les équipes qui travaillent sur la cryptologie et la virologie informatiques** et leur donner, sous le contrôle de l'ANSSI, y compris dans les laboratoires universitaires, la possibilité de débrider les systèmes d'exploitation, de déverrouiller, de désassembler des logiciels, de vérifier les flux informatiques, de faire de la rétro-ingénierie pour **mieux comprendre la nature des menaces afin de se donner les moyens de tracer les flux véhiculant des logiciels malveillants.**

III. SE DONNER LES MOYENS DE LA SÉCURITÉ NUMÉRIQUE PAR UNE MEILLEURE COOPÉRATION ENTRE LES ACTEURS

- Créer un lieu d'échange sur le numérique réunissant **ingénieurs**, **politiques** et **administratifs pour développer une culture du numérique** au sein de la sphère politique et administrative.
- Instituer une coopération entre les industriels et entre les industriels, la communauté de défense et le monde académique pour élaborer et appliquer une **stratégie nationale de cybersécurité à moyen et long termes** pour faire face aux attaques.
- Élargir les pouvoirs de l'ANSSI en lui donnant un **pouvoir de régulation et d'injonction**.
- Encourager, sur tout le territoire national, le **développement d'acteurs de confiance spécialistes de la sécurité informatique** *(retombées économiques possibles)*.

IV. À PARTIR DE DISPOSITIONS ET DE PRATIQUES NATIONALES VERTUEUSES, CONSTRUIRE UN DROIT EUROPÉEN

- Modifier le code des marchés publics pour **que les réponses des appels d'offres ne dévoilent pas l'intégralité du système d'information d'une entreprise** (*retombées économiques possibles*).
- **Mieux organiser la conservation des preuves d'un délit numérique.**
- Réformer la législation française et européenne de manière à **imposer le niveau de protection, le référentiel de sécurité des OIV aux PME** qui leur sont liées (filiales, fournisseurs, sous-traitants) **–** *retombées économiques possibles*.
- **Imaginer un droit de la donnée,** après une large consultation citoyenne, pour :

- ✓ **imposer sur Internet le respect de la <u>présomption d'innocence</u>, du <u>contradictoire</u>** ;
- ✓ **encadrer le droit au déréférencement, à l'oubli pour les données personnelles** ;
- ✓ **étendre la <u>durée des prescriptions liées à des délits informatiques</u>** où les préjudices perdurent ;
- ✓ fixer la **<u>date de départ du délai de prescription des délits informatiques</u>** à celle de la **date de la découverte du délit** par la victime.

V. ASSEMBLÉES PARLEMENTAIRES, COLLECTIVITÉS TERRITORIALES ET ADMINISTRATIONS

- **Sensibiliser <u>les collectivités territoriales et les administrations</u> à la sécurité informatique** :
- **Faire du <u>Parlement</u> un lieu exemplaire de la prise de conscience des vulnérabilités du numérique.**

VADE-MECUM
DE RECOMMANDATIONS DE SÉCURITÉ NUMÉRIQUE À L'USAGE DES ENTREPRISES

Liste incluant (en italique) les préconisations du « Guide des règles d'hygiène informatique » élaboré par l'ANSSI.

Les recommandations prioritaires de l'OPECST figurent dans un encadré et les recommandations très importantes sur une trame grisée.

La sécurité numérique d'une entreprise ne dépend que d'elle-même : elle résulte d'une construction réfléchie et évolutive et ne saurait résulter automatiquement de prestataires extérieurs, de l'achat ou de l'installation de matériels.

Cette construction peut être ordonnée autour des dix aspects suivants :

1) Les **préalables** à la sécurité numérique de l'entreprise ;
2) Les **principes généraux** à respecter pour assurer la sécurité numérique de l'entreprise ;
3) La **construction** de la sécurité numérique de l'entreprise ;
4) L'**appréciation critique continue** de la structure de sécurité numérique ;
5) Le **parc informatique** de l'entreprise ;
6) Les **distinctions** entre :

- le numérique à usage **personnel** et le numérique à usage **professionnel** ;

- les **personnels permanents** de l'entreprise et les **autres usagers** du numérique ;

- la distinction entre l'usage du numérique **dans l'entreprise ou à l'extérieur**.

7) Les principes propres à l'utilisation de chaque réseau ou matériel numérique dont **l'informatique en nuage** ;
8) Les **réflexes** de sécurité numérique à acquérir ;
9) L'**évaluation** de la sécurité numérique de l'entreprise ;
10) La construction d'une **résilience** de l'entreprise après une attaque numérique.

Certains des dix aspects ci-dessus doivent être renforcés pour les opérateurs d'importance vitale et leurs partenaires.

1. Les préalables à la sécurité numérique de l'entreprise :

- **1 Classer les données en fonction de leur confidentialité** pour leur appliquer un régime de sécurité approprié ;
- *(ANSSI 19)* ***Chiffrer les données sensibles****, particulièrement sur les postes nomades ou les équipements qui risquent d'être perdus.*

Les produits de chiffrement de l'ensemble du système (chiffrement intégral ou de disque) ou d'un sous-ensemble (chiffrement de partitions) ont été qualifiés par l'ANSSI. Les mécanismes de chiffrement intégral de disques sont les plus efficaces et ne nécessitent pas d'identifier les fichiers à chiffrer.

- **2** Fonder la sécurité informatique sur **une approche globale et dans la profondeur** (plutôt qu'une protection à la périphérie), **grâce à un empilement de briques de sécurité**, et sur **l'ingénierie sociale**.
- **3 Réfléchir, au cas par cas, au meilleur moyen technique à employer** pour la transmission d'une information en fonction de son degré de confidentialité et de son urgence (nouveau métier).
- **4 Faire primer la sécurité numérique** sur la connexion continue ou la recharge immédiate.
- **5 Adopter des comportements adaptés** au niveau de sécurité des matériels et des réseaux.

2. La construction de la sécurité numérique de l'entreprise

- **6** Revoir les organigrammes des entreprises de manière à **assurer aux responsables de la sécurité du numérique un accès direct aux dirigeants de l'entreprise et donc le pouvoir d'imposer les normes ou habitudes de sécurité nécessaires** :
  - ✓ Identifier la fonction de responsable de la sécurité des systèmes informatiques (RSSI) comme **élevée** dans un parcours professionnel.
- **7 Sensibiliser les décideurs à la sécurité informatique**, notamment à la nécessité d'utiliser exclusivement des **téléphones portables sécurisés** voire celle d'aménager des **salles de réunion opaques aux ondes** (principe de la cage de Faraday).
- *(ANSSI 37)* ***Mettre en place une chaîne permanente d'alerte et de réaction*** *connue de tous les intervenants comprenant un ou plusieurs interlocuteurs référents formés à la réaction.*

- **OIV.1 Former à la sécurité informatique**, les dirigeants et les personnels, les sous-traitants, les fournisseurs, les clients.
- **OIV.2 Communiquer avec d'autres OIV** sur le risque numérique.

……..

- **8 Établir un plan global de sécurité** (de l'informatique de gestion, industrielle et des applications utilisées) et en étendre le respect aux **filiales** et aux **sous-traitants.**
- ***(ANSSI 21)*** *Mettre en place, dès leur conception, un* ***cloisonnement maîtrisé des réseaux informatique intérieurs****. Créer un sous-réseau protégé par une passerelle de connexion spécifique pour les postes ou les serveurs contenant des informations importantes pour la vie de l'entreprise.*
- ***(ANSSI 28) Interdire tout accès à l'Internet depuis les comptes d'administration*** *en équipant les administrateurs de deux postes distincts.*
- **OIV.3** Vérifier **l'étanchéité** des réseaux prétendus fermés.
  - ***(ANSSI 23) Utiliser systématiquement des applications et des protocoles sécurisés et donc proscrire les protocoles non sécurisés (telnet, FTP, POP, SMTP, HTTP) et n'utiliser que leurs équivalents sécurisés (SSH, SFTP, POPS, SMTPS, HTTPS, etc.).***
- **9 Multiplier les sites de stockage des données.**

……...

- **10** Avoir une gestion des droits des profils utilisateurs et administrateurs sur les postes et, surtout, sur les services de l'entreprise qui soit décrite dans la politique de sécurité de l'entreprise.
- **11** Réserver des droits administrateurs **uniquement à des personnes habilitées**, y compris sur les téléphones mobiles, les périphériques comme les imprimantes 3D et les objets connectés.
- ***(ANSSI 30) Ne jamais donner aux utilisateurs de privilège d'administration*** *– quelle que soit leur position hiérarchique dans l'entreprise.*
- ***(ANSSI 8) Identifier nommément chaque personne ayant accès au système*** *et* ***supprimer les comptes et accès génériques et anonymes****.*
- ***(ANSSI 2) Établir un inventaire exhaustif des comptes privilégiés et des comptes génériques et le tenir à jour.***
- ***(ANSSI 29) Cloisonner le réseau d'administration vis-à-vis du réseau de travail des utilisateurs*** *(cloisonnement physique des réseaux ou, à défaut, cloisonnement logique cryptographique ou, à tout le moins, cloisonnement logique par VLAN) et* ***maintenir à jour les postes d'administration****.*

……..

- ***(ANSSI 4) Centraliser en un point unique d'accès contrôlable les accès Internet de l'entreprise et les interconnexions avec des réseaux partenaires***

en nombre minimal, le recours au Wi-Fi et au téléphone *(contrôle, surveillance et analyse des* logs*).*

……

- **12** Instaurer la **cartographie obligatoire des *Supervisory Control And Data Acquisition* (*SCADA*).**

- **13** **Déconnecter les *SCADA* de l'Internet**, ce qui suppose de renoncer à la mise à jour directe des systèmes par Internet pour l'effectuer, grâce à un serveur isolé et contrôlé après le téléchargement de la mise à jour.

……

- **14** **Recourir à des antivirus divers de manière à assurer une sorte de biodiversité de la protection.**
- **15** **Proposer aux PME** des solutions de **sécurité numérique « Tout-En-Un ».**

- **OIV.4** Étudier la possibilité d'**assurer au mieux le risque numérique**.

3. L'appréciation critique continue de la structure numérique mise en place

- **OIV.5** Mettre en place un **centre de sécurité opérationnel** procédant à une **surveillance permanente et** incluant des **systèmes de détection dans les réseaux**, des **cellules de crise** et des **équipes d'interventions propres** ;
- **OIV.6** Disposer, aux côtés des responsables des systèmes d'information, d'**une filière opérationnelle rattachée aux équipes de production informatique** ;

- ***(ANSSI 1) Dresser la cartographie (adresses IP, noms de domaine, noms des machines, logiciels, interfaces réseaux, etc.) de l'installation informatique, la tenir à jour*** *dans le cadre d'une politique de déploiement des systèmes et* ***ne pas la stocker sur le réseau****.*

- **16** Établir la **cartographie des risques de ses systèmes d'information, du maillage** de ses sous-traitants, de ses fournisseurs, de ses clients, de ses personnels afin d'**apprécier le degré de vulnérabilité informatique** de ses activités ;

- ***(ANSSI 20) Auditer ou faire auditer fréquemment la configuration de l'annuaire central*** *(Active Directory, Windows ou LDAP) notamment pour vérifier si les droits d'accès aux données des personnes clés de l'entreprise sont correctement positionnés.*

- **17** **Installer des sondes sur le réseau** de manière à apprécier, en temps réel, ce qui se passe et faire gérer les sondes de détection d'attaque par des **prestataires qualifiés**.

- ***(ANSSI 26)*** *Dans le cadre de la* ***supervision des systèmes et des réseaux, définir concrètement les événements déclencheurs d'une alerte à traiter dans les vingt-quatre heures*** *(connexion d'un utilisateur hors de ses horaires habituels ou de ses présences déclarées transfert massif de données vers l'extérieur de l'entreprise, etc.).*
- ***(ANSSI 27) Définir la fréquence, les modalités d'analyse et les conséquences (alertes…) des événements figurant dans les journaux de l'entreprise.***

4. Le parc informatique de l'entreprise

- **18 Investir dans la sécurité des systèmes d'information** *(retombées économiques possibles)***.**
- ***(ANSSI 14) Mettre en place un niveau de sécurité homogène pour l'ensemble du parc informatique (désactiver les services inutiles, …).***
- ***(ANSSI R16) Utiliser un outil de gestion du parc informatique*** *pour le* ***déploiement des politiques de sécurité*** *et les* ***mises à jour*** *des équipements.*
- **19** N'acheter que des matériels et ne recourir qu'à des fournisseurs **référencés par l'ANSSI** *(retombées économiques possibles).*
- ***(ANSSI 35)*** *Mettre en place des* ***procédures de destruction ou de recyclage*** *des* ***supports informatiques en fin de vie.***

Matériels informatiques

- **20 Intégrer la sécurité numérique dès la conception d'un matériel ou d'une application et procéder à des évaluations de risque des matériels informatiques** *(retombées économiques possibles).*
- **21** Toujours **assortir la sécurité technique à la sécurité d'usage**.
- **22** Soumettre les **équipementiers** à des **obligations de sécurité spécifiques**.
- **23 Certifier rapidement les logiciels et les équipements critiques diffusés dans l'Union européenne** *(retombées économiques possibles)***.**
- **24** Corriger les **logiciels** présentant des failles.
- **25** Interdire la **captation des données à distance**.
- **26 Objets connectés** : **définir des protocoles** pour leur fabrication et leur usage incluant l'information de leurs utilisateurs sur la possibilité de les déconnecter et **favoriser la recherche en matière de sécurisation de ces objets.**

5. Les trois séries de distinctions à opérer

entre le numérique à usage personnel et le numérique à usage professionnel :

- ***(ANSSI R5) Ne pas utiliser ses outils numériques personnels pour un usage professionnel*** *– même pas les clés USB… mais plutôt* ***donner des téléphones professionnels*** *pour des usages personnels accessoires.*
- **27 Interdire tout chargement de logiciels non professionnels sur les postes de travail** (clés *USB*, disques externes, *DVD*, etc.).
- **28** En cas d'utilisation de postes de travail à domicile, leur garantir un **niveau de sécurité** ne compromettant pas la sécurité de l'entreprise.

entre les personnels permanents de l'entreprise et les autres usagers du numérique :

- *(ANSSI 32) Utiliser impérativement des* ***mécanismes robustes d'accès aux locaux de l'entreprise.***
- *(ANSSI 3) Élaborer et appliquer des* ***procédures d'arrivée et de départ des utilisateurs du système d'information (personnels, stagiaires, fournisseurs, clients, etc.).***
- *(ANSSI 34)* ***Ne laisser aucune prise d'accès au réseau interne ou aucun chemin de câble accessible dans les endroits ouverts au public*** *(salles d'attente, couloirs, placards où sont connectés des imprimantes, des écrans d'affichage, des caméras de surveillance, des téléphone, des prises réseau, etc.).*
- *(ANSSI 33)* ***Protéger rigoureusement les clés et badges permettant l'accès aux locaux et les codes d'alarme*** *(clés et* badges *à récupérer, codes d'alarme à changer, clés et codes à ne jamais donner à des prestataires extérieurs).*

entre l'usage du numérique dans l'entreprise ou à l'extérieur :

- ***(ANSSI 25) Vérifier qu'aucun équipement du réseau*** *(équipements industriels ou de supervision, commutateurs réseaux, routeurs, serveurs, imprimantes, etc.)* ***ne comporte d'interface d'administration accessible depuis Internet.***
- ***(ANSSI 24) Sécuriser les passerelles d'interconnexion avec Internet de manière à assurer un cloisonnement entre l'accès à l'Internet, la zone de service (DMZ) et le réseau interne.***
- ***(ANSSI R18) Interdire, dans tous les cas où cela est possible, les connexions à distance sur les postes clients*** *et, sinon, appliquer les recommandations de sécurité relative à la téléassistance disponibles sur le site de l'ANSSI.*
- **29** En cas d'utilisation de l'Intranet de l'entreprise depuis l'extérieur, mettre en œuvre un accès sécurisé *via* des *Virtual Private Networks* (*VPN*).

- ***(ANSSI 31)*** *N'autoriser* ***l'accès à distance au réseau de l'entreprise****, y compris pour l'administrateur du réseau,* ***que depuis des postes de l'entreprise dotés de mécanismes d'authentification forte*** *protégeant l'intégrité et la confidentialité des échanges.*

6. Les principes propres à l'utilisation de chaque réseau ou matériel numérique

- ***(ANSSI 22) Éviter l'usage d'infrastructures sans fil (Wi-Fi).*** *À tout le moins,* ***cloisonner le réseau d'accès Wi-Fi*** *du reste du système d'information (une passerelle maîtrisée assurant l'interconnexion avec le réseau principal) et* ***chiffrer le réseau Wi-Fi****.*
- **30 Chiffrer les réseaux *Wi-Fi*** au moyen de *WPA Entreprise* (Wi-Fi sécurisé).
- **31 Proscrire les mécanismes de protection fondés sur une clé partagée.**
- **32 Éviter le recours aux technologies des courants porteurs en ligne (CPL).**
- ***(ANSSI 7) Définir une politique de sécurité pour la mise à jour des composants logiciels et des postes et l'appliquer strictement sur l'ensemble du parc.***
- ***(ANSSI 6) Mettre à jour les logiciels*** *de manière sécurisée pour résister aux virus* ***à partir du site de leur éditeur ;*** *se tenir informer des vulnérabilités et des mises à jour ; si un composant ne peut être mis à jour, il ne doit pas être utilisé.*
- **33** Définir des **règles de gestion et d'usage** des messageries personnelles.
- ***(ANSSI 15) Interdire techniquement la connexion des supports amovibles.***
- ***(ANSSI 17) Gérer les terminaux nomades selon une politique de sécurité au moins aussi stricte que celle applicable aux postes fixes.*** *Ce qui suppose, souvent, le* ***renforcement de certaines fonctions de sécurité*** *(chiffrement de disque, authentification renforcée, etc.).*
- **34 Laisser les téléphones portables à l'extérieur des salles où se tiennent des réunions confidentielles** dans les entreprises qui n'ont pas de politique de sécurité pour les mobiles en mode invité – ce que tous les logiciels d'administration ne peuvent faire aujourd'hui – **bannir toute connexion Internet dans ces salles** et envisager la **création de salles sécurisées** (cages de Faraday).
- ***(ANSSI 35) Définir des règles d'utilisation des imprimantes et des photocopieuses*** *: présence physique du demandeur pour démarrer une*

impression, destruction des documents oubliés sur les imprimantes ou les photocopieuses, broyage des documents plutôt que mise à la corbeille.

7. Les réflexes de sécurité numérique à acquérir

- ***(ANSSI 39) Rappeler, au moins chaque année, aux utilisateurs les règles d'hygiène informatique élémentaires : les informations, sensibles par nature, imposent des comportements exemplaires*** *(respect de la politique de sécurité, verrouillage systématique des sessions hors usage immédiat, non connexion des équipements personnels, non divulgation et non réutilisation et des mots de passe à des tiers, signalement des événements suspects, aménagement des visites* (*retombées économiques possibles*).
- ***(ANSSI R39) Signature d'une charte d'usage des moyens informatiques par chaque utilisateur.***

Identité numérique

- **35** Réaliser un projet d'**identité numérique fondée sur la carte *SIM***.
- **36** Favoriser le développement des puces *RFID*, des codes barre et autres dispositifs d'identification, de référencement, de classement, pour **provoquer l'émergence d'un marché ouvert et foisonnant de dispositifs de reconnaissance et de sécurisation des objets**, des transactions, des usages *(retombées économiques possibles)*.
- **37** Effectuer immédiatement l'intégralité des **mises à jour** des antivirus, des pare-feu, etc.
- ***Mots de passe*** *:*
  - ✓ ***(ANSSI 9) Définir des règles de choix et de dimensionnement des mots de passe*** *en fonction du degré de sensibilité des accès à protéger.*
  - ✓ ***(ANSSI 11) Ne pas conserver les mots de passe en clair*** *dans les systèmes informatiques* ***ni utiliser de mécanismes automatiques de sauvegarde des mots de passe****.*
  - ✓ ***(ANSSI 10) Changer les mots de passe tous les six mois et bloquer les comptes jusqu'au respect effectif de cette règle.***
  - ✓ ***(ANSSI 12) Renouveler systématiquement les éléments d'authentification par défaut sur les équipements****.*
  - ✓ ***(ANSSI 13) Privilégier l'authentification par carte à puce nécessitant un code PIN.***

Nuages numériques

- **38** Préférer ses **propres centres de stockage de données** (*retombées économiques possibles*)**.**
- **39** **Ne stocker dans les nuages numériques que des données peu confidentielles**.
- **40** **Diversifier les lieux de stockage de données** *(retombées économiques possibles)***.**

……

- **41** Passer de la notion de **coffre-fort numérique**, qui n'offre pas des garanties de sécurité suffisantes pour y confier tous ses biens, à une gestion active du risque en conservant les procédures actuelles de sauvegarde car la maîtrise de l'outil est devenue impossible.
- **42** Évaluer la fiabilité d'un nuage au vu de trois critères : **disponibilité**, **intégrité** et **confidentialité**.
- **43** Ne stocker que dans des nuages permettant une **authentification** et un **cryptage des données**.
- **44** Créer et promouvoir **un label européen de stockage des données** *(retombées économiques possibles)*.
- **45** **Développer des nuages maîtrisés avec des fournisseurs français** *(retombées économiques possibles).*
- **46** Créer des offres de ***messagerie nationales*** **sécurisées, chiffrées** et traitées au niveau national *(retombées économiques possibles)*.
- **47** La **localisation en France** peut permettre un contrôle sur place du régulateur *(retombées économiques possibles).*
- **48** Réduire la dépendance aux nuages grâce à des **outils français ou européens** s'appuyant sur la dynamique de **l'*open source*** *(retombées économiques possibles)*.
- **49** Privilégier les nuages utilisant des routeurs européens – et envisager la fabrication de processeurs européens *(retombées économiques possibles)*.
- **50** La souveraineté numérique peut-être facilitée par des équipements, des services qualifiés et des redondances nationales *(retombées économiques possibles)*.
- **51** Contracter une police d'assurance en cas de recours au nuage numérique *(retombées économiques possibles)*.

8. L'évaluation de la sécurité numérique de l'entreprise

- **52 Effectuer des tests d'intrusion incluant de l'ingénierie locale.** En conséquence, mettre à jour la politique de sécurité informatique *(retombées économiques possibles)*.

- **OIV.7** Effectuer des **exercices réguliers de crise informatique**.

- **53 Procéder à des audits réguliers de sécurité des règles informatiques** *(retombées économiques possibles)*.

- ***(ANSSI R40) L'audit annuel de sécurité du système d'information doit être assorti d'un plan d'action,*** *de* ***réunions fréquentes de suivi*** *de ce plan et d'un* ***tableau de bord de l'avancement des actions*** *de ce plan pris en compte au plus haut niveau.*

- **54** Avoir la possibilité de **faire évaluer le risque pris en recourant aux équipements du commerce** – ainsi que le recommande l'ANSSI.

- **55 Former au *hacking***.

9. La construction d'une résilience de l'entreprise après une attaque numérique

- **OIV.8** En cas d'attaque du site de l'entreprise, **toujours avoir à disposition le nom de son développeur, ses clés d'accès, ses mots de passe et la manière d'obtenir les journaux.**

- **OIV.9** Mettre en place un réseau de transmission des incidents pour **informer sans délai l'ANSSI, la CNIL** et des interlocuteurs de même niveau des attaques subies.

- **56 Enregistrer tous les *logs* et les placer sur une sauvegarde distincte** afin de les rendre disponibles en cas d'attaque y compris pour les téléphones mobiles et les objets connectés *(retombées économiques possibles)*.

- **57 Anticiper la perte des archives en les classant par hiérarchie de sauvegarde** (archives courantes, intermédiaires, définitives, en distinguant les archives sensibles dans chaque catégorie) **et en assurant leur lisibilité dans le temps par les appareils de lecture** *(retombées économiques possibles)*.

  L'usage du nuage numérique pour stocker les archives n'exonère pas de cette précaution.

- **58** Compléter cette démarche par des **simulations de perte d'archives** et des **exercices de restauration desdites archives** *(retombées économiques possibles)*.

- *(ANSSI 36)* ***Disposer d'un plan de reprise et de continuité d'activité informatique tenu à jour*** *pour sauvegarder les données essentielles de l'entreprise.*
- *(ANSSI 32)* ***Sauvegarder périodiquement et automatiquement les données sensibles de l'entreprise*** *dans un lieu distinct de celui des serveurs en fonctionnement.*
- *(ANSSI 38)* ***Traiter intégralement l'infection d'une machine*** *(comment le code malveillant s'est-il installé ? Combien de postes sont-ils compromis ? Quelles informations ont-elles été divulguées ?) incluant un* ***retour d'expérience*** *et une* ***capitalisation****.*
- *(ANSSI 38) Prendre les mesures immédiates suivantes* ***: isoler les machines infectées*** *du réseau,* ***ne pas les éteindre*** *électriquement,* ***copier les mémoires et les disques durs****,* ***réinstaller intégralement la machine*** *après copie des disques.*

Incidents informatiques

- **59** Doter le système d'information d'une structure d'administration à même de le **préserver d'une réaction en chaîne en cas d'attaque**.
- **60** Définir une **marche à suivre à l'intention des petites et moyennes entreprises, des collectivités territoriales et des particuliers** pour leur indiquer vers quels acteurs de proximité se tourner en cas d'incident *(retombées économiques possibles)*.
- **61** Former les utilisateurs à l'analyse des **incidents dus aux antivirus** et aux **réactions** à adopter face à ceux-ci.
- **62** **Réagir à un virus en moins de vingt-quatre heures –** (l'entreprise *Saoudi Aramco* a réagi en quelques heures).
- **63** Fabriquer des **outils français d'analyse des incidents informatiques** *(retombées économiques possibles)*. Inciter au développement de ces outils au niveau national par des jeunes entreprises innovantes et des entreprises de taille intermédiaire. Le marché de la sécurité informatique est en plein développement, la France dispose d'un tissu d'entreprises tout à fait à même d'y devenir des acteurs majeurs et les écoles françaises de mathématiques et d'informatique comptent parmi les meilleures du monde.
- **64** Favoriser une prise en compte des expériences **des services de police et de justice** au niveau européen.

ANNEXES

LETTRE DE SAISINE DE L'OPECST

RÉPUBLIQUE FRANÇAISE

SÉNAT

COMMISSION
DES AFFAIRES
ÉCONOMIQUES

LE PRÉSIDENT

Monsieur Bruno SIDO
Président
Office parlementaire d'évaluation des
choix scientifiques et technologiques
Casier de La Poste
Palais du Luxembourg

Paris, le 26 juin 2013

Réf : 491 (MLB)

Monsieur le Président,

Par courrier en date du 5 juin dernier, vous me faites part de votre intérêt pour la question des risques connexes à la numérisation de la société et de l'économie.

Vous évoquez en particulier les enseignements préoccupants que vous retirez de l'audition publique organisée le 21 février dernier par l'Office parlementaire d'évaluation des choix scientifiques et technologiques et je mesure moi-même les enjeux liés à cette question notamment pour la compétitivité des entreprises et leur environnement économique.

Après en avoir consulté les membres, j'ai l'honneur de vous indiquer que la commission des affaires économiques a décidé de saisir l'Office, en application de l'article 6 *ter* de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires, d'une étude sur le thème du risque numérique et plus précisément la sécurité des réseaux informatiques ainsi que le stockage des données personnelles ou industrielles et leur exploitation.

J'attire néanmoins votre attention sur la nomination envisagée de deux parlementaires en mission sur un sujet d'études assez proche, ce qui vous conduira éventuellement à préciser le champ de votre étude afin d'éviter des redondances inutiles.

Je vous prie d'agréer, Monsieur le Président, l'expression de ma haute considération.

Daniel RAOUL

15 rue de Vaugirard – 75291 PARIS CEDEX 06 - TÉLÉPHONE : 01 42 34 30 89 - TÉLÉCOPIE : 01 42 34 20 76

EXTRAITS DES RÉUNIONS DE L'OPECST DU 17 DÉCEMBRE 2014 ET DU 28 JANVIER 2015 : ADOPTION DU RAPPORT

EXTRAIT DE LA RÉUNION DE L'OPECST DU 17 DÉCEMBRE 2014

M. Jean-Yves Le Déaut, député, président de l'OPECST. – Nous allons entendre la présentation du projet de rapport de Mme Anne-Yvonne Le Dain, députée, et de M. Bruno Sido, sénateur, premier vice-président de l'OPECST, sur le risque numérique. Selon une méthode maintenant éprouvée, nous avons mis le projet de rapport en consultation. Cette consultation est organisée sur place dans chaque assemblée. Il est simplement demandé aux membres de l'Office de prévenir de leur arrivée pour éviter de mobiliser le secrétariat pendant des journées entières.

Je vous rappelle que la saisine relative au risque numérique a été effectuée par la commission des affaires économiques du Sénat le 26 juin 2013 et que nous avions organisé quelques mois auparavant, le 21 février 2013, une audition publique en lien avec les deux commissions de la défense de l'Assemblée nationale et du Sénat. Le sous-titre de cette audition se présentait déjà comme une piste de solution : « *Le risque numérique : en prendre conscience pour mieux le maîtriser* » et était déjà apparue la nécessité d'observer les règles d'hygiène informatique pour utiliser les outils numériques. En effet, la sécurité n'est pas seulement une affaire de technique ou de protection mais appelle aussi à la vigilance permanente à tous les niveaux.

Le présent projet de rapport entre dans le détail de la technologie pour mieux faire ressortir les pratiques possibles. Parmi celles-ci, je mentionnerai notamment le chiffrage par clé publique/clé privée qui consiste à conserver par devers soi la clé privée, indispensable au décodage, tandis que l'on donne à toute personne qui envoie un message une clé publique permettant de chiffrer son message.

Le projet de rapport contient des recommandations très nombreuses, près de cent cinquante. Nous reviendrons sur leur contenu après leur présentation. Il me semble, après en avoir parlé avec les rapporteurs, qu'un travail de synthèse et de regroupement de certaines de ces recommandations pourrait être réalisé. Certaines appellent des modifications de nature législative ou règlementaire ; d'autres sont plus techniques. On gagnerait à faire ressortir des recommandations principales, qui s'attachent à essayer de redéfinir les principes de la société numérique. Vous avez vous-même prévu une hiérarchisation pour mettre en valeur certaines recommandations. J'y ai moi-même travaillé ce matin.

Après la projection du petit film prévue en introduction et la présentation par les rapporteurs, je souhaiterais qu'on puisse voir comment on pourrait arriver, sur un certain nombre de points, à modifier un peu le projet de rapport.

La présentation du jeu « Keep On Eye » élaboré par le CIGREF est projetée.

M. Bruno Sido, sénateur, premier vice-président, rapporteur. – Mme Anne-Yvonne Le Dain et moi-même avons aujourd'hui le plaisir de vous présenter le projet de rapport sur le risque numérique dont vous nous avez confié l'élaboration.

C'est à partir d'une **saisine de la commission des Affaires économiques du Sénat** que nous avons entrepris **une étude de faisabilité** adoptée le 16 avril 2014.

Cette saisine faisait elle-même suite à une **journée d'auditions publiques** organisées conjointement par l'OPECST et la commission des Affaires étrangères et de la Défense du Sénat au mois de février 2013. Ce jour-là, l'audition publique avait été scindée en deux parties, l'une relative au risque numérique militaire et l'autre au risque numérique civil.

Nous comptions donc réaliser notre rapport en approfondissant la question du risque numérique civil mais il nous est rapidement apparu que, en matière de risque numérique, **la distinction entre le civil et le militaire était artificielle** compte tenu justement de la nature du numérique qui est présent partout.

Au terme d'**une centaine d'auditions** comprenant trois journées d'auditions publiques et des déplacements à Bruxelles et en province, notamment pour visiter le centre de haute sécurité de la Direction générale pour l'armement et le laboratoire de haute sécurité de l'INRIA, vos rapporteurs ont établi **une douzaine de constats** sur la situation de la sécurité numérique et procédé à des choix pour mener à bien leur étude.

Au début de celle-ci, nous avons pris soin de rencontrer le président de la commission des Affaires économiques du Sénat, M. Daniel Raoul, aujourd'hui de retour à l'OPECST ce dont nous nous réjouissons.

Nous lui avons indiqué que nous centrerions notre réflexion sur **les opérateurs d'importance vitale**, c'est-à-dire les entreprises dont le fonctionnement ne doit en aucun cas être interrompu, notamment du fait d'une défaillance de leur système d'information numérique.

Ces entreprises sont d'ailleurs soumises à des **directives nationales de sécurité (DNS)** qui leur imposent des obligations extrêmement précises. La loi de programmation militaire de 2013 les a renforcées.

L'angle d'attaque pour aborder l'étude à partir des opérateurs d'importance vitale s'est révélé intéressant pour le raisonnement mais conduisait aussitôt à replacer l'ensemble des activités desdits opérateurs

dans la chaîne de sécurité qu'ils constituent avec leurs fournisseurs, leurs sous-traitants, leurs clients et leurs personnels.

En outre, pour être tout à fait complet, au moment où le Gouvernement annonçait un ambitieux projet de loi sur le numérique, il n'a cependant pas attendu le dépôt de celui-ci pour prendre, d'une part, comme déjà indiqué, dans la loi de programmation militaire, en 2013, des initiatives relatives justement aux opérateurs d'importance vitale et, d'autre part, pour élaborer, au cours de l'été 2014, des mesures relatives à la sécurité numérique concernant les administrations.

Ce qui montre que le Gouvernement comme nous-mêmes avons été conduits à effectuer des analyses rigoureuses sur les différents secteurs pour finalement constater que tout se recoupe et que la sécurité numérique, voire la sécurité tout court, ne peuvent être assurées qu'à partir de mesures reliées entre elles.

Par quelque bout que l'on considère la question, il est impossible de ne pas voir dans les ramifications du numérique **le système nerveux de la société et des individus qui la composent**, d'où l'impossibilité de scinder artificiellement les préoccupations de sécurité en divers segments d'études.

C'est bien ce qu'ont vu, en premier, les attaquants des systèmes numériques. À l'heure où notre pays se trouve placé sous les dispositions du plan vigipirate à un très haut degré – dit « écarlate » –, le thème d'étude de l'OPECST ne peut qu'être au cœur des préoccupations de tous les parlementaires.

Pour relancer ce défi, depuis quelques années, des dispositifs ingénieux ont été imaginés et des moyens réels en hommes et en moyens ont été accordés. Par exemple, en 2009, l'Agence nationale de sécurité des systèmes d'informations (ANSSI) a été créée.

Mais je dois préciser, dès l'abord, que des dispositifs étaient déjà en place et que, maintenant, ce n'est pas en accordant toujours davantage de compétences à l'ANSSI ni en portant ses effectifs de trois cents à mille ou à trois mille – seuils qui ne sont d'ailleurs nullement envisagés –, qu'on résoudrait les questions posées par les failles de la sécurité numérique et qu'on parerait aux attaques dont elle est l'objet.

En effet, cette question transversale suppose l'acquisition, par l'ensemble de la société, d'une **culture du numérique** et d'une **éducation initiale et continue** à la hauteur des services rendus par cette technique, en dépit des fragilités qu'elle recèle.

Depuis le début de mon propos et surtout à la suite de la vidéo que vous venez de regarder, vous vous demandez peut-être si vos rapporteurs n'ont pas cédé à quelque alarmisme. Je vous rassurerai en disant que nous avons d'abord souhaité démontrer, dans une analyse que l'on a voulu extrêmement fouillée, le mécanisme de transmission des messages et les

fragilités, souvent de conception, des matériels, des réseaux, des services et des diverses applications numériques.

À un moment donné, il nous est apparu que **les imperfections constatées peuvent constituer également des chances** et c'est cet aspect que Mme Anne-Yvonne Le Dain va maintenant développer pour vous montrer la face optimiste de l'analyse de vos rapporteurs.

Mme Anne-Yvonne Le Dain, députée, rapporteur. – Au fur et à mesure des auditions, une idée m'a de plus en plus préoccupée : comment tirer parti d'une difficulté, d'une inquiétude, d'un mal éventuel et, en l'occurrence, **en matière d'insécurité numérique, comment faire de l'économie avec du droit** ? À partir du droit national, du droit européen et même du droit international.

Il se trouve que **la France possède de nombreux atouts** en ce domaine, tant en matière de logiciels et de matériels qu'en matière de connaissances, notamment grâce à l'École française de mathématiques qui a été à l'origine d'une grande tradition en matière de cryptologie et de cryptographie. S'y ajoutent les ressources des universités, des centres de recherche de la Direction générale de l'armement, du CNRS ou de l'INRIA, pour ne citer qu'eux. Elles devraient permettre de conforter les entreprises œuvrant en ces domaines et, surtout, de faire en sorte que de nouvelles initiatives puissent naître sans être récupérées aussitôt par nos concurrents principaux, à savoir les États-Unis d'Amérique au moment où l'Union européenne est en train de négocier un accord commercial transatlantique.

Dans le monde du numérique beaucoup de dispositifs sont en autorégulation alors que, au niveau national comme au niveau international les enjeux économiques sont considérables. Les entreprises nord-américaines, les *GAFA (Google, Apple, Facebook et Amazon*) agissent à ce niveau et sont extrêmement présentes, y compris à Bruxelles où se bâtit le cadre de l'économie numérique du XXIème siècle. L'enjeu est colossal. Le numérique touche tout, dans la vie personnelle comme dans la vie professionnelle de chacun, les personnes physiques comme les personnes morales.

Pour mettre en valeur les atouts français, il faut se débarrasser de préjugés et d'attitudes routinières. Par exemple, les préjugés associés à l'image des *hackers* qui peuvent également être employés fort utilement pour devenir, non pas des pirates, mais des corsaires au service des institutions qui les emploient.

On voit bien qu'il s'agit actuellement d'un enjeu absolument stratégique et c'est ce qui a motivé la rédaction de ce rapport.

À ce stade de notre travail, nous avons auditionné beaucoup de monde et accompli beaucoup de travail avec le président Bruno Sido, et je pense que les cent quarante recommandations qui vous sont proposées sont tout à fait importantes, mais qu'il serait pertinent, sur la base du document,

qui représente un énorme travail, dont je remercie les administrateurs, de consacrer encore un peu de temps pour réécrire, reformuler, revoir la manière dont les choses sont dites ;pour communiquer de manière plus efficace dans un contexte où, en ce moment, entre l'Union européenne et les États-Unis d'Amérique, et dans les relations internationales en général, les enjeux dans ce domaine sont considérables.

Il serait souhaitable de prendre encore deux à trois semaines après les vacances pour revoir un certain nombre de finalités, pour reformuler, reclasser et donner des priorités en ce domaine. L'enjeu est essentiel ; on a pu le mesurer en entendant énormément de monde, en se posant la question de la protection des données individuelles et personnelles dont les volumes ont explosé.

Au moment de la décision de lancer la présente étude, l'affaire Snowden n'était pas encore sur la table et le piratage du portable de la chancelière allemande n'était pas encore connu. Nous avions anticipé. Maintenant, l'environnement national et international a encore évolué et il serait essentiel de prendre un peu de temps pour reformuler un certain nombre de choses. Je vous remercie.

M. Jean-Yves Le Déaut, député. – Je souhaiterais d'abord dire que, y compris les schémas que je trouve très, très bien, il y a là un matériau de fond qui est bon. Vous demandez un peu de temps car j'ai cru comprendre que vous aviez été « charrette » sur la fin. Je voudrais remercier l'administrateur et l'expert qui l'a assisté, du travail qui a été fait.

J'ai vu le rapport ce matin et n'ai eu qu'un peu de temps pour y travailler. Je pense d'abord, à propos du projet de recommandations, que l'on peut arriver à une très bonne étude de l'Office en ordonnant les cent quarante ou cent cinquante recommandations qui sont là pour mettre en valeur des schémas que vous avez élaborés et qui expliquent parfaitement la problématique.

Le premier point que je voudrais signaler c'est que la partie introductive du projet de recommandations intègre un rappel du guide de l'ANSSI. Or, notre but, à l'Assemblée nationale comme au Sénat, n'est pas de reprendre des dispositions qui existent déjà mais de sélectionner, dans les recommandations de l'ANSSI, les points sur lesquels il y aurait moyen de faire évoluer les choses.

J'ai donc pris la responsabilité de faire une proposition de rédaction pour les recommandations que je vous transmettrai tout à l'heure. J'ai ordonné autour de six chapitres les propositions : le premier chapitre s'intitulerait « *Développer une culture du numérique autour de la sphère politique et administrative* ». Le deuxième point, que vous avez très bien traité à mon avis, concernerait le risque numérique ; cela est plutôt bien et je reprends vos recommandations. Le troisième point consisterait à faire du risque numérique une grande cause nationale dans l'éducation et la formation et

tout ce que vous proposez apparaît sous ce chapitre. Le quatrième chapitre serait « *Renforcer les moyens de la formation universitaire et de la recherche en matière de cybersécurité* » ; c'est le point le moins abordé dans les recommandations, mais c'est un débat dans lequel je suis déjà intervenu pour dire que, à côté du pôle militaire de défense situé dans l'ouest de la France, il existe un autre pôle de cybersécurité civile, dans une autre région, consacré à des thèmes de recherche qui pourraient le situer à un niveau européen. Cinquièmement, il s'agit de mieux protéger les entreprises et c'est là l'essentiel du rapport. Il serait plus efficace pour aider les entreprises d'indiquer quatre ou cinq grands points d'évolution possible de la loi.

Toutes les autres propositions seraient alors placées en annexe sous la forme d'une ébauche d'un guide de cybersécurité à destination des entreprises. Toutes les dispositions pratiques pourraient également être hiérarchisées. Enfin, il faudrait insérer la stratégie nationale dans une stratégie européenne et, sur certains points, j'aimerais que les rapporteurs nous indiquent comment ils voient le débat citoyen dans le domaine du risque informatique ; comment ils appréhendent la possibilité d'imposer le respect sur Internet de la présomption d'innocence, celle du contradictoire et des prescriptions. Il serait souhaitable aussi d'interdire la captation des données à distance et, pour cela, de déterminer ce qui est législatif dans ces recommandations.

Il faudrait également encourager le développement d'acteurs de confiance, ce qui pourrait entraîner des retombées économiques. Très souvent, dans vos conclusions finales, vous attirez l'attention sur ces retombées économiques possibles et cela mériterait des précisions. Enfin, il y a d'autres points qui devraient sans doute être déplacés d'un chapitre à un autre si ma proposition en six points était adoptée.

Ce matin, je me suis livré à un exercice de nouvel ordonnancement des recommandations. Vous avez mes notes et il est possible d'agencer cela autrement tout en améliorant la formulation des idées sachant que le fond de ce texte est excellent et qu'une amélioration formelle serait, à mon avis, de nature à faire passer les bons messages qui sont dans ce rapport.

Et, ce, d'autant plus que les rapporteurs, même s'ils ne l'ont pas dit, n'ont pas eu suffisamment de temps pour étudier ce projet de rapport en dépit de l'existence d'un pré-rapport. Cela a été trop « charrette » de finaliser complètement ce projet pour la fin de l'année. Donc, si les deux rapporteurs le demandent, cette réunion de l'Office parlementaire pourrait constituer une réunion de travail en vue de l'élaboration d'un nouveau texte à valider et à examiner rapidement par la suite puisque les rapporteurs ont déjà en partie commencé leur présentation.

Il n'y a aucun problème à procéder de la sorte car les thèmes que vous avez abordés sont des thèmes majeurs.

Peut-être serait-il souhaitable d'insister sur la partie recherche et enseignement supérieur et j'aimerais que, dans le corps du texte, vous rajoutiez un point – qui figure dans mon avis budgétaire sur la cyberdéfense –, pour souligner qu'il risque de manquer de personnes formées à la cyberdéfense dans les prochaines années ; si vous en étiez d'accord, peut-être serait-il souhaitable de mettre ce point en exergue de manière plus évidente ?

M. Bruno Sido. – On est toujours pressé par le temps et il est toujours possible de revisiter et de réordonner ce projet de rapport, sans changer le fond puisque c'est le résultat de nos investigations. Mais, sur la forme, il est toujours possible de placer des éléments en annexe. La version définitive vous sera soumise avant l'examen par l'Office pour vous donner le temps de bien apprécier la forme définitive.

Mme Anne-Yvonne Le Dain. – C'est un travail colossal. Le président Bruno Sido, moi-même et l'administrateur avons consacré un temps colossal aux auditions dont trois auditions publiques incluant des table rondes plus confidentielles et cela a permis d'embrasser tout le champ de ce sujet stratégique ; il était temps de le faire. Cela représente un joli travail sous réserve d'une remise en forme finale pour améliorer la visibilité de ce rapport pour le rendre plus efficace aux yeux du grand public comme des média ; c'est aussi simple que cela.

Mme Marie-Christine Blandin, sénatrice. – Je n'ai pas grand-chose à dire à part mon admiration pour la densité de ce qu'on trouve dans ce rapport : c'est une bible. Peut-être y a-t-il une ergonomie à développer pour mieux accéder au contenu, mais c'est vraiment très riche et très bien.

Pour ma part, je n'étais pas sur le champ exclusif de l'entreprise car la commission de la culture du Sénat avait travaillé sur des thèmes qui sont aux frontières du sujet de ce rapport. Par exemple, à la page 41, vous parlez de la régulation de l'échange entre les personnes physiques, puis après, on passe au virtuel. Nous avions travaillé sur le virtuel pour lequel il apparaît que, si les gens ne s'adressent pas des signes préalables, un sourire préalable, rapidement un propos peut être à l'origine de polémiques. C'est pourquoi, les discussions sur Internet, par exemple de syndicats ou de partis politiques, s'enveniment avec méchanceté et des modérateurs ont donc été mis en place. Le numérique fait apparaître de nouveaux acteurs et de nouveaux pouvoirs car les modérateurs sont des gens de pouvoir. Cela a également de l'importance dans l'entreprise parce que le modérateur prend le pouvoir alors que personne ne s'en aperçoit. Il filtre les débats avec ses convictions.

Ensuite, tout acte public pris par le passé a donné lieu à des archives papiers ; elles se trouvent à la Bibliothèque nationale et sont consultables dans les archives départementales, etc. Maintenant, le numérique donne le pouvoir à celui qui émet des documents de les détruire. J'en donnerai quelques exemples : une des académies – je ne sais plus si c'est celle des sciences, celle de médecine ou celle des technologies – a fait disparaître un

rapport sur l'amiante datant d'une époque où elle estimait que cette matière n'était pas dangereuse, ce qui est tout de même gênant [*Des signataires issus de l'INSERM se sont désolidarisés* a posteriori *du rapport de l'Académie de Médecine : « Amiante et protection de la population exposée à l'inhalation de fibres d'amiante dans les bâtiments publics et privés », Bulletin de l'Académie Nationale de Médecine ; Tome 180 n°4 – séances des 16, 23, 30 avril 1996, page 887*]. Le numérique permet très facilement ce genre d'opérations de disparition.

Quant à l'AFSSAPS – on avait travaillé là-dessus avec M. Jean-Pierre Door –, au moment de la pandémie grippale, il a fallu vacciner tout le monde donc, en catastrophe. Sanofi, GSK et Roche ont mis au point des vaccins comprenant des sels d'aluminium. Moi, je me souvenais qu'une page de l'AFSSAPS disait que les sels d'aluminium posaient problème, qu'il fallait les interdire aux enfants de moins de deux ans et que, à terme, il n'y aurait plus de vaccins de ce type. J'ai donc recherché cette page mais ne l'ai pas trouvée. Je pouvais avoir rêvé sauf qu'une étudiante en médecine qui avait fait sa thèse sur les vaccinations avait pris une copie d'écran de cette page et c'est donc ainsi que je l'ai retrouvée.

Je ne parle pas du fond, mais le numérique donne le pouvoir de détruire des archives publiques et une réflexion démocratique doit être conduite là-dessus, car cela pose tout de même un problème.

Je continue, toujours un peu en marge de votre rapport, à propos de préoccupations relatives aux libertés individuelles. Je ne suis pas sur *Facebook*. J'ai reçu de nombreuses invitations d'amis qui y sont et, la dernière fois, j'ai reçu une invitation de personnes souhaitant m'inviter avec la liste de tous mes amis, de mon beau-fils, de mon ancienne collaboratrice etc. Cela fait froid dans le dos car, si l'on repense aux réseaux de résistance, on se dit que si, aujourd'hui, nous nous trouvions dans la même situation, n'importe quelle police fasciste, en appuyant sur un bouton, pourrait obtenir tous les lieux où vous pouvez vous cacher, toutes vos relations... Je ne suis pas sur le réseau, et, pourtant, les gens qui me mentionnent sur le réseau y développent en creux l'imagerie de mes amis et, cela, c'est un problème de liberté.

Certaines de vos recommandations sont relatives à l'éducation et à l'enseignement supérieur. Je souhaiterais alerter sur la mauvaise formation des étudiants au numérique et sur le plagiat. En effet, de plus en plus de thèses sont plagiées dans les universités ; cela constitue un vrai problème au point que, lors de son audition au Sénat, M. André Syrota, de l'Institut national de la santé et de la recherche médicale (Inserm) et de l'Alliance pour les sciences de la vie et de la santé (Aviesan), nous a alertés sur le fait que 40 % des publications, dans *Nature*, de découvertes, d'innovations etc. n'étaient pas reproductibles parce que le travail n'est pas fait de première main. Cela pose problème.

Vous parlez de la compétitivité des entreprises. La commission de la culture du Sénat a travaillé sur les entreprises de presse, qui gagnent leur

argent sur la publicité, mais, depuis que *Google* les référence et se place entre les publicitaires et les agences de presse, c'est *Google* qui ramasse l'argent.

La Belgique a souhaité élaborer un texte pour empêcher cela, mais *Google* a débranché toutes les entreprises de presse belges du référencement. Tout récemment, *Google plus* vient de débrancher l'Espagne qui préparait un nouveau texte de loi dans ce domaine. Ce qui donne une idée du pouvoir de ces monopoles. Dans votre rapport, vous parlez beaucoup du risque des monopoles.

Ensuite, dans un passage, vous évoquez la mentalité des *hackers*. Avec *Le Monde diplomatique*, nous avions réuni les *Anonymous*. C'était impressionnant, car ils nous ont expliqué comment ils avaient aidé la démocratie en Égypte pendant la répression ; de même en Tunisie. Tous les journalistes du *Monde* souriaient et trouvaient ces jeunes gens formidables mais, par derrière, ceux-ci nous ont précisé qu'ils n'avaient qu'une ligne, celle de la circulation de l'information : si un chef d'État fasciste voulait susciter l'adhésion de jeunes, et au moyen d'un message à la jeunesse, et qu'un autre État souhaite l'empêcher, les *Anonymous* feraient en sorte que ce message parvienne jusqu'à elle. Ils entendent être inodores et incolores ; leur philosophie, c'est la sacralisation du message.

Merci donc pour votre rapport.

À propos du coût éventuel de la sécurité numérique sur la compétitivité des entreprises, je souhaiterais peut-être un petit ajout pour évoquer l'engrenage de l'obsolescence et des coûts induits parce que je vois que, au sein de l'éducation nationale, dans les établissements scolaires, certains commencent à « se faire des cheveux blancs » à cause des achats de logiciels, du renouvellement de matériel etc. Pour cette raison là aussi, nous sommes incités de nous trouver face à des monopoles, pour faire jouer la concurrence et obtenir des prix raisonnables ; sinon cela va nous coûter toujours plus cher.

Par ailleurs, mais c'est peut-être évoqué dans le projet de rapport que je n'ai pu lire intégralement, qu'en est-il de la vulnérabilité physique des centres de stockage de données ?

J'ai conscience que mes commentaires sont parfois un peu aux limites du thème de la sécurité numérique des entreprises.

M. Bruno Sido. – Nous nous sommes aperçus, quasiment dès le départ, que le champ d'investigation était tellement vaste que, au-delà des généralités, nous nous sommes dit qu'il serait intéressant de traiter plus particulièrement, à titre d'exemple, du secteur de l'énergie et du secteur des télécommunications, deux secteurs parmi tant d'autres. Et nous ne pouvons même pas dire si les problèmes soulevés dans ces deux secteurs sont les mêmes que ceux d'autres secteurs – bancaire, administratif, universitaire… –, cela reste à examiner.

Les remarques faites par Mme Marie-Christine Blandin sont tout à fait pertinentes et intéressantes. Heureusement pour les thèses, le plagiat était devenu tellement répandu qu'il y a maintenant des logiciels pour le détecter.

Mme Anne-Yvonne Le Dain. – Je vous remercie pour cet élargissement des perspectives. Le champ du numérique est gigantesque, car le numérique est vraiment partout. Il est impossible de le traiter dans son ensemble. Nous avons souhaité indiquer la manière dont on pourrait se protéger des risques grâce à des guides de bonnes pratiques, même si cela apparaît très difficile du fait, notamment, de l'existence de portes dérobées dans les matériels.

Nous n'avons pas seulement à subir le numérique, mais aussi à nous en saisir pour en faire une opportunité économique, de manière à se protéger tout en se développant, d'autant qu'il s'agit d'un enjeu mondial.

M. Bruno Sido. – Nous nous sommes aperçus, sans entrer forcément dans la technique, que l'application de quelques principes de bon sens permettait de se prémunir pour l'essentiel de l'insécurité numérique. La première chose, c'est déjà d'en avoir conscience. Quand on pense que des patrons se rendent en Chine avec leur ordinateur et leurs tableaux de calcul, travaillent avec ces outils sur place et s'aperçoivent à leur tour que, finalement, s'ils n'ont pas remporté le marché, c'est parce qu'au passage de la frontière, on avait capturé toutes leurs données, y compris celles de leurs téléphones. Il vaut mieux se rendre en Chine avec un petit téléphone neuf que l'on jette au retour.

La deuxième chose c'est l'hygiène informatique : il faut savoir qu'il vaut mieux ne pas ramasser de clés *USB*, puis s'en servir ; en fait, c'est comme pour sa brosse à dents, il vaut mieux ne jamais la prêter.

Enfin, l'administration s'est bien adaptée depuis un certain temps, et c'était d'ailleurs extrêmement important. De leur côté, les opérateurs d'importance vitale (OIV) donnent l'exemple.

On nous a dit, à propos des feux de signalisation informatisés aux carrefours, ce que tous les responsables de la préfecture de police de Paris savent : en cas de panne du système informatique de ces feux, il y aurait des blessés, voire des morts ; car, en moins de deux heures, les gens en viendraient aux mains si tout s'arrêtait.

L'ANSSI a déjà été reformatée, mais elle a du mal à embaucher, quoiqu'elle n'hésite pas à faire appel aussi à des *hackers* repentis. D'ailleurs, certains sont-ils peut-être devenus *hackers* pour se faire remarquer à cette fin ? La direction générale pour l'armement travaille également à la sécurité numérique vingt-quatre heures sur vingt-quatre et, ce matin, j'assistais à une réunion de la Commission supérieure du service public des postes et des communications électroniques au cours de laquelle le Premier ministre a dit que le numérique et sa sécurité constituaient une priorité, qu'il ne fallait pas

que le numérique flanche sinon plus rien ne se passerait aujourd'hui. Tout le monde a bien pris conscience de cela, bien plus qu'il y a quelques années, et les principes d'hygiène informatique commencent à se répandre.

On pourra toujours se poser la question de savoir pourquoi il existe des *hackers*, mais il faut aussi se souvenir de l'attaque de la *CIA*, donc des États-Unis d'Amérique contre les centrifugeuses iraniennes. Cela constitue bien une attaque d'État à État et cela aurait pu aller plus loin. On pointe souvent la Chine d'un doigt accusateur, sans trop de preuves d'ailleurs, et c'est vrai que toute attaque informatique peut retarder un pays tandis que sa sécurité active lui permet de rattraper son retard et, éventuellement, d'aller de l'avant. Cette question ne peut absolument pas être négligée par les gouvernements.

Le rapport peut paraître touffu mais le sujet lui-même est touffu ; il est très compliqué. L'informatique, c'est un peu la loi de la maille et des nœuds en électricité, on ne sait pas où passe l'électricité mais elle arrive au bout. Il en va un peu de même pour l'informatique, sujet très compliqué, car les attaques peuvent venir de partout et même du fabricant qui utilise une porte de derrière prévue pour son seul usage.

On peut avoir des soupçons sur tout, même sur les téléphones ou les tablettes sécurisés de la présidence de la République et du Gouvernement – d'ailleurs plus ou moins utilisés. Finalement, c'est François Mitterrand qui avait raison en estimant que, si quelqu'un a quelque chose d'important à dire à une autre personne, cela doit se faire directement, sans l'écrire, ni téléphoner.

M. Jean-Yves Le Déaut. – Cela fait penser à cette plaisanterie soviétique : « Si tu penses quelque chose, ne le dis pas ; si tu le dis, ne l'écris pas ; si tu l'écris, ne le signe pas ; et si tu le signes, ne t'étonne plus de rien ».

Juste deux petits points de forme encore. Tout d'abord, je trouve que le schéma de la page 48 montrant l'intérieur de la boîte noire du numérique est excellent ; cela représente très bien la complexité du système numérique qui vient d'être évoquée.

Deuxièmement, excusez-moi, c'est un réflexe de professeur qui a assisté à de nombreuses soutenances de thèses, je note que l'acronyme *SCADA,* sa définition, ne figurent pas dans le glossaire. Si j'ai bien compris, il s'agit de données du système de production des entreprises collectées à partir de capteurs que, quelquefois, l'on va chercher sur Internet. Or, si tous les capteurs de machines sensibles sont en lien avec Internet, il peut y avoir, à un moment donné, moyen de capter les données qu'ils transmettent et même d'introduire un espion à l'intérieur du système.

M. Bruno Sido : Renseignement pris, *SCADA* signifie « *Supervisory Control and Data Acquisition* », et désigne un logiciel de supervision industrielle tel que vous l'avez parfaitement bien compris. Cette précision figurera dans le glossaire.

M. Jean-Yves Le Déaut. – Au terme de cette réunion de travail, nous prenons date pour la présentation d'une version améliorée suivant les indications retenues, en notant qu'il y a déjà eu unanimité pour dire qu'il s'agissait d'un bon travail.

EXTRAIT DE LA RÉUNION DE L'OPECST DU 28 JANVIER 2015 : ADOPTION DU RAPPORT

M. Jean-Yves Le Déaut, député, président. – Nous avons déjà eu une discussion sur ce sujet le 17 décembre dernier et nos collègues rapporteurs ont souhaité disposer d'un peu plus de temps pour arriver à une version qui intègre la réorganisation des recommandations et qu'ils ont aussi pu améliorer. Ce projet a été mis en consultation, comme c'est la règle, quarante-huit heures avant la réunion de ce jour.

Cette version n'a pas tout intégré. J'ai moi-même retravaillé encore ces deux derniers jours sur quelques améliorations de forme, et on dispose maintenant d'un document qui contient des recommandations très importantes. Il me semble nécessaire que, conformément aux options prises dans le cadre de l'étude de faisabilité, vous proposiez de modifier l'intitulé puisque vous avez opportunément choisi de cibler votre étude.

Je voudrais tout de suite vous féliciter, en englobant dans ces félicitations le conseil technique que vous avez reçu. Car ce document, avec ses recommandations, pose bien le problème.

(Une brève vidéo sur la sécurité numérique, très récemment élaborée par le CIGREF à destination des entreprises, est alors projetée dont le message consiste à attirer l'attention sur le fait que : « *100 % des entreprises protègent leurs données ; logiquement très peu d'entre elles ont dû connaître une faille de sécurité lors des douze derniers mois… mais en fait, oups ! 73 % ! Comme quoi, on n'est jamais trop prudent. Chaque seconde, notre environnement déborde d'activités, des gens comme vous et moi qui, chaque jour, génèrent des millions de données sensibles en envoient et en reçoivent, les partagent aux quatre coins du monde. Mais qui veille sur tout ça ? Qui peut agir pour éliminer les risques ? Et si c'était vous ?* »*)*

M. Bruno Sido, sénateur, premier vice-président, rapporteur. – Mme Anne-Yvonne Le Dain et moi-même avons aujourd'hui le plaisir de vous présenter le projet de rapport sur le risque numérique dont vous nous avez confié l'élaboration et dont la vidéo qui vient d'être projetée illustre en quelques minutes la problématique en ce qui concerne les entreprises.

C'est à partir d'une **saisine de la commission des Affaires économiques du Sénat** que nous avons entrepris **une étude de faisabilité** adoptée par l'Office le 16 avril 2014.

Cette saisine faisait elle-même suite à une **journée d'auditions publiques** organisée conjointement par l'OPECST et la commission des Affaires étrangères et de la Défense du Sénat au mois de février 2013. Ce jour-là, l'audition publique avait été scindée en deux parties, l'une relative au risque numérique militaire et l'autre au risque numérique civil.

Au début de nos investigations, nous comptions donc réaliser notre rapport en approfondissant la seule question du risque numérique civil. Mais il nous est rapidement apparu que, en matière de risque numérique, **la**

distinction entre le civil et le militaire était artificielle, compte tenu justement de la nature du numérique qui est présent partout.

Au terme d'**une centaine d'auditions** comprenant trois journées d'auditions publiques et des déplacements à Bruxelles et en province, notamment pour visiter le centre de haute sécurité de la Direction générale pour l'armement et le laboratoire de haute sécurité de l'INRIA, vos rapporteurs ont établi **une douzaine de constats** sur la situation de la sécurité numérique et procédé à **trois choix** pour mener à bien leur étude.

Au début de celle-ci, nous avons pris soin de rencontrer le président de la commission des Affaires économiques du Sénat, M. Daniel Raoul, aujourd'hui de retour à l'OPECST ce dont nous nous réjouissons.

Nous lui avons indiqué que nous centrerions notre réflexion sur **les opérateurs d'importance vitale (OIV)**, c'est-à-dire les entreprises dont le fonctionnement ne doit en aucun cas être interrompu, notamment du fait d'une défaillance de leur système d'information numérique.

Ces entreprises sont d'ailleurs soumises à des **directives nationales de sécurité (DNS)** qui leur imposent des obligations extrêmement précises que la loi de programmation militaire de 2013 a renforcées.

Après quelques mois de nos travaux, l'angle d'attaque pour aborder l'étude à partir des opérateurs d'importance vitale s'est révélé avoir été intéressant pour le raisonnement mais nous a conduit bientôt à replacer l'ensemble des activités desdits opérateurs dans **la chaîne de sécurité numérique** qu'ils constituent avec leurs fournisseurs, leurs sous-traitants, leurs clients et leurs personnels.

En outre, pour être tout à fait complet, au moment où le Gouvernement annonçait un ambitieux projet de loi sur le numérique, il n'a cependant pas attendu le dépôt de celui-ci pour prendre, comme déjà indiqué, dans la loi de programmation militaire, en 2013, des initiatives relatives justement aux opérateurs d'importance vitale et, d'autre part, pour élaborer, au cours de l'été 2014, des mesures relatives à la sécurité numérique concernant les administrations.

Ce qui montre que le Gouvernement, comme nous-mêmes, avons été conduits à effectuer en parallèle des analyses rigoureuses sur les différents secteurs pour finalement constater que tout se recoupe et que la sécurité numérique, voire la sécurité tout court, ne peuvent être assurées qu'à partir de mesures reliées entre elles.

Par quelque bout que l'on considère la question, il est impossible de ne pas voir dans les ramifications du numérique **le système nerveux de la société et même des individus** qui la composent d'où l'impossibilité de scinder artificiellement les préoccupations de sécurité en divers segments d'études.

C'est bien ce qu'ont vu, les premiers, les attaquants des systèmes numériques. À l'heure où notre pays se trouve placé sous les dispositions du plan vigipirate à son plus haut degré – soit l'alerte attentat –, le thème d'étude de l'OPECST ne peut qu'être au cœur des préoccupations de tous les parlementaires.

Pour relever ce défi, depuis quelques années, des dispositifs ingénieux ont été imaginés et des moyens réels en hommes et en moyens ont été accordés. Par exemple, en 2009, l'Agence nationale de sécurité des systèmes d'informations (ANSSI) a été créée.

Mais, dès l'abord, je dois préciser que des dispositifs étaient déjà en place antérieurement et que, maintenant, ce n'est pas en accordant toujours davantage de compétences à l'ANSSI ni en portant, par exemple, ses effectifs de 300 à 1 000 ou à 3 000 – seuils qui ne sont d'ailleurs nullement envisagés – , qu'on résoudrait toutes les questions posées par les failles de la sécurité numérique, ni qu'on parerait à toutes les attaques dont cette sécurité est l'objet.

En effet, cette question transversale suppose l'acquisition par l'ensemble de la société d'une **culture du numérique** et d'une **éducation initiale et continue** à la hauteur des services rendus par cette technique, à la fois en dépit et en raison des fragilités qu'elle recèle.

Depuis le début de mon propos, et surtout à la suite du visionnage de la vidéo que vous venez de regarder, vous vous demandez peut-être si vos rapporteurs n'ont pas cédé à quelque alarmisme. Je vous rassurerai en disant que nous avons d'abord souhaité démontrer dans une analyse, que l'on a voulu extrêmement fouillée, le mécanisme de transmission d'un message au sein du système d'information de l'entreprise et les fragilités, souvent de conception, des matériels, des réseaux, des services et des diverses applications numériques.

Mais avant cela, nous devons lever une ambiguïté. En dépit de l'actualité sur les aspects les plus médiatisés du risque numérique et ses liens avec le terrorisme, **le présent projet de rapport n'a rien d'une fresque générale ou journalistique sur le numérique** où, par exemple, seraient développées des considérations sur la gouvernance mondiale de l'Internet, car il s'agit d'un rapport technique. L'OPECST produit de tels rapports directement liés aux préoccupations des entreprises que, malheureusement, le Sénat a parfois tendance à négliger. C'est pourquoi je rappelle que la commission des affaires économiques, à l'origine de la saisine, s'inquiétait de l'éventuelle fragilité des entreprises liée aux vulnérabilités des réseaux matériels, logiciels, numériques. Cela est particulièrement technique.

En qualité de membre de cette commission, j'insiste sur l'importance de cette dimension du sujet.

La question sous-jacente posée à l'Office était notamment celle du pillage organisé des informations des entreprises. Il serait déraisonnable de

continuer à ignorer le fait que l'on puisse puiser dans ces informations comme dans un libre-service. **La situation de l'économie française s'accommode-t-elle de tels pillages ou bien résulte-t-elle en partie de ceux-ci, alors justement qu'ils durent depuis des années ?**

À un moment donné, il nous est apparu que **les imperfections constatées peuvent constituer également des chances** et c'est cet aspect que Mme Anne-Yvonne Le Dain va maintenant développer pour vous montrer que l'analyse de vos rapporteurs comporte aussi une face réactive, voire optimiste.

Mme Anne-Yvonne Le Dain, députée, rapporteur. – Je ne crois pas que l'indispensable prise de conscience qu'a évoquée Bruno Sido relève d'une approche pessimiste du numérique, mais l'idée que la sécurité numérique puisse devenir un atout de développement économique me tient à cœur, et c'est là un axe majeur de notre analyse. Il s'agit de faire d'une crainte une opportunité.

Au fur et à mesure des auditions, une idée nous a de plus en plus préoccupée : comment tirer parti d'une situation un peu compromise et, en l'occurrence, en matière d'insécurité numérique, **comment faire de l'économie avec du droit** ? Un développement dans le rapport illustre ce que cette idée sous-tend.

Il se trouve que **la France possède de nombreux atouts** en ce domaine car, sans même parler des fabricants d'antivirus, les connaissances de l'École française de mathématiques alliées à une grande tradition en matière de cryptologie, de cryptographie et de linguistique, les ressources des centres de recherche de la Direction générale de l'armement ou de l'INRIA, pour ne citer qu'eux, devraient permettre de conforter les entreprises œuvrant dans le domaine de la sécurité numérique et, surtout, permettre de nouvelles initiatives qui ne seraient pas récupérées aussitôt par nos concurrents principaux, à savoir les États-Unis d'Amérique – qui écrivent l'informatique à l'aide du même alphabet que nous, contrairement aux Russes, aux Indiens ou aux Chinois.

Pour mettre en valeur les atouts français, il faut se débarrasser de préjugés et d'attitudes routinières. Par exemple, les préjugés associés à l'image des *hackers* alors que certains d'entre eux pourraient être employés fort utilement pour élaborer des solutions de prévention et de riposte aux attaques numériques éventuelles – un certain nombre d'entreprises le fait déjà. Les personnes entendues ont cité des exemples de *hackers* peu diplômés que l'administration française n'avait pu recruter à un niveau de salaire décent. En effet, leur diplôme ne donnait accès qu'à un niveau indiciaire de traitement dans la fonction publique peu propre à rémunérer équitablement les hautes compétences dont ils faisaient preuve.

Une autre personne entendue nous a cité les exemples de jeunes entreprises extrêmement innovantes dans le numérique aussitôt rachetées

par des financiers d'outre-Atlantique venus faire, en quelque sorte, leur marché en France.

Face à une telle situation, il ne suffit pas de demander aux autres de faire preuve d'initiative, de créativité, de réactivité, si nous-mêmes, parlementaires, ne montrons pas l'exemple d'abord par notre engagement personnel, puis à travers les décisions des assemblées et collectivités territoriales au sein desquelles nous pouvons avoir une influence. Certaines de nos propositions de recommandations vont dans ce sens.

Libre au Gouvernement d'agir de même face aux administrations.

Venons-en maintenant à l'observation de nos comportements face aux exigences de la sécurité numérique souvent négligées dans la vie courante.

Par exemple, qui d'entre nous hésite avant de s'abonner à une messagerie électronique alors que celle-ci est peut-être contrôlée par une firme étrangère ? Qui prend le temps minimal de réflexion avant de choisir la voie la plus sécurisée pour transmettre un message urgent ? Les services des assemblées sont-ils eux-mêmes à la pointe quant à la sécurité informatique ? Les collectivités territoriales ne pourraient-elles s'intéresser davantage à cette question ? Qu'en est-il enfin des entreprises que l'on suppose à la pointe en matière de technologie de sécurité numérique ? Et, quand on parle de sécurité numérique, les ordinateurs ne sont pas les seuls objets à prendre en considération, les téléphones portables sont égalementsources de risques, ainsi que tous les « objets dits connectés ».

Tout naturellement, à ce stade de l'analyse, chacun pense au rôle de l'éducation nationale. Or, vos rapporteurs proposent, dans la vingtaine de recommandations prioritaires qu'ils vous soumettent, d'**enseigner le codage** de manière ludique dès l'école maternelle et de **créer une véritable filière d'enseignement de l'informatique incluant systématiquement des modules significatifs sur sa sécurité** jusque dans l'enseignement supérieur. Et, ce, sur tout le territoire national.

Cela peut paraître évident mais la situation actuelle n'est pas à la hauteur des exigences, loin s'en faut.

Qu'observe-t-on aujourd'hui ? L'absence de l'informatique dans les programmes ou, quand elle y figure, c'est avec un nombre d'heures extrêmement restreint et malheureusement sans enseignement sur la sécurité du numérique, ou si peu, y compris dans les écoles spécialisées.

En outre, quels sont **les enseignants** censés faire face à cette nouvelle demande ? D'où proviennent-ils aujourd'hui ? D'où proviendront les effectifs accrus nécessaires demain ? Il serait bien imprudent de croire qu'on peut facilement reconvertir un professeur de mathématiques, de sciences physiques ou de technologie en professeur d'informatique. Chacun sait que l'informatique n'est pas vraiment une branche des mathématiques ni une section de l'électronique.

Quand je parle de filière de l'enseignement de l'éducation au numérique, il s'agit aussi de **diplômes** reconnus et d'un **corps d'inspection**. Et où placer cet enseignement dans l'emploi du temps des élèves ?

Mais, me direz-vous, cette construction n'aurait-elle pas bientôt pour effet de figer les connaissances des enseignants alors que ce secteur évolue si vite ?

C'est un risque réel qui doit être d'emblée pris en compte pour anticiper la sclérose éventuelle desdits enseignants dont la réactivité devra demeurer la qualité première.

Mais, sans entrer davantage dans cette partie de nos propositions, je crois que le Premier vice-président souhaiterait vous en détailler un peu davantage la philosophie.

M. Bruno Sido. – Pour bien situer notre propos par rapport aux contextes international, européen et national actuels, je souhaiterais insister sur la totale symbiose existant entre le numérique et la société.

En général, chacun admet ce phénomène fusionnel mais sans accepter d'en tirer vraiment les conséquences. Ainsi, il ne sert à rien d'élever des digues juridiques ou technologiques si, dans le même temps, des accords internationaux ou la réalité d'un rapport de force non encadré viennent ruiner nos efforts.

Autant une partie de notre projet de rapport entre dans le détail des systèmes informatiques, autant il nous a paru indispensable de faire précéder cette analyse par **une vision d'ensemble**.

Tel fut le cas pour expliquer pourquoi la négociation actuelle du Traité de partenariat transatlantique et le rythme d'avancée de l'élaboration de la directive et du projet de règlement européens, ainsi que la maturation du projet de loi sur le numérique en France sont en réalité étroitement liés.

Vous avez pu trouver, dans les deux premiers chapitres du rapport, les raisons pour lesquelles il est très important, à la fois, que **les droits et libertés soient respectés** dans l'univers numérique, tout en veillant à **protéger la souveraineté numérique de la France comme de l'Union européenne**.

Il s'agit là d'objectifs vitaux qui doivent primer sur la libre circulation des marchandises, l'abaissement des droits de douane ou l'instauration d'une concurrence libre et parfaite.

Vos rapporteurs se sont d'ailleurs demandé s'il ne serait pas primordial de concevoir une exception numérique d'après le modèle de l'exception culturelle et pour les mêmes raisons.

En effet, l'exception culturelle a permis de conserver une industrie cinématographique française dynamique alors qu'elle aurait pu être laminée par des principes commerciaux qui prétendaient la dominer. Les cinémas d'autres pays d'Europe en ont été victimes.

De même, dans le numérique, **toutes les chances doivent être mises de notre côté pour que des industries françaises et européennes puissent concevoir, fabriquer, voire seulement contrôler pour les labelliser, les matériels, logiciels, systèmes d'exploitation, cœurs de réseaux qui forment la longue chaîne de la sécurité numérique**.

Cette idée n'a pu être qu'esquissée dans ce rapport mais elle mériterait d'être développée dans d'autres enceintes et, prioritairement, se concrétiser avant qu'il ne soit définitivement trop tard.

Je voudrais aussi attirer votre attention sur les schémas qui sont projetés depuis le début de notre présentation – et qui figurent tous dans le rapport. Beaucoup de ces schémas ont d'ailleurs été **élaborés par l'OPECST**, ce qui n'est pas si fréquent. Ils nous ont semblé utiles pour expliciter **une réalité numérique multiple difficile à appréhender** autrement.

C'est ainsi que, devant la difficulté d'expliquer une réalité technologique plus que complexe, le schéma de l'éléphant vous permet soudain de voir que, par exemple, la perception du numérique n'est que parcellaire, ce qu'a d'ailleurs illustré aussi la **multitude de rapports parlementaires** traitant de ce thème. Beaucoup de ces études n'ont porté que sur un aspect bien particulier du numérique. Et **très peu ont approfondi la question de la sécurité du recours croissant au numérique par les entreprises**.

C'est ainsi qu'un rapport parlementaire analyse l'ouverture des données ou « *open data* », un autre le traitement des données massives ou « *big data* », le troisième la gouvernance mondiale de l'Internet, un autre enfin le modèle proposé par les États-Unis d'Amérique, et ainsi de suite.

Le présent rapport n'a pas pour ambition de constituer une anthologie du numérique mais de montrer que, même si cela ne saute pas aux yeux, toutes ces questions sont interdépendantes.

La sécurité numérique est présente derrière chacune d'entre elles et permet, peut-être, de reconstituer le puzzle des Internets et de tous les aspects du numérique en général, pour en faire ce que vous voyez sur l'écran sous la forme imagée de cet éléphant.

Mme Anne-Yvonne Le Dain. – En ma qualité de scientifique, je souhaiterais vous montrer quelques schémas qui rendent compte de la réelle complexité de ce numérique que nous croyons pouvoir appréhender avec ce que nous avons sous les yeux. Ce schéma-ci représente le réseau global de l'Internet en Île-de France et vous pouvez noter le nœud dense de ramifications se trouvant sous La Défense. Un spécialiste nous a indiqué que, à cet endroit, une frontière numérique séparait l'Inde de l'Europe du point de vue de la gestion des réseaux numériques, ce qui ne tombe pas sous le sens. La dématérialisation a des conséquences absolument sidérantes.

Cet autre schéma représente les ramifications numériques d'une entreprise avec son centre de gestion, ses activités de production, ses

contacts avec l'extérieur, avec ses sous-traitants et leurs propres sous-traitants et, se superposant à tout cela, les multiples connexions, par nature très imprévisibles, réalisées à l'initiative de ses employés.

Il est évident que des liens entre tous ces éléments, de leur continuité, de leur intégrité, dépendent, dans un premier temps, la sécurité numérique, et, bien sûr, ensuite, la protection contre de mauvaises surprises. À cet égard, une des recommandations de vos rapporteurs consiste à **couper totalement les *SCADA* – c'est à dire les systèmes numériques commandant la production – de l'Internet**. Cette préconisation peut, à première vue, sembler très exagérée pour beaucoup d'organisations croyant fonctionner parfaitement.

Cependant, pour vous convaincre en un instant de l'utilité de cette recommandation, j'évoquerai simplement l'anecdote rapportée par une personne entendue, à savoir la pénétration du système des *SCADA* d'un hôpital nord-américain par un adolescent de seize ans qui avait réussi à bloquer la climatisation de cet établissement et exigeait une rançon pour la rétablir. Cela va au-delà de la simple constatation de l'habileté avérée d'un adolescent face à l'inconscience de l'administration d'un hôpital. La prise en considération du facteur humain est primordiale pour opposer une défense idoine.

Par ailleurs, quand on sait que des **logiciels d'attaques informatiques** sont maintenant disponibles dans le commerce, donc éventuellement à la disposition d'individus particulièrement malfaisants, le rapprochement de ce fait avec le fait précédent peut conduire à réfléchir.

D'autant que, même si notre rapport a souhaité disséquer, pour ainsi dire, la complexité de la sécurité numérique d'une entreprise, un des constats auxquels vos rapporteurs sont parvenus, mentionné dans le préambule du rapport, est le suivant : **au-delà des failles technologiques, les failles humaines entraînent des vulnérabilités plus grandes**.

D'où l'effort d'éducation que nous avons déjà évoqué et, plus généralement, une action de sensibilisation massive à mener dont la petite projection du début de notre réunion a montré la nécessité.

En effet, ce **film réalisé par le CIGREF** à la demande d'une **quarantaine d'entreprises internationales** est **destiné à être diffusé**, accompagné d'un test ludique, **à destination de tous les employés** desdites sociétés avec, évidemment, l'espoir que cette sensibilisation gagne **leurs familles et d'autres entreprises**, ainsi que les administrations, voire les politiques eux-mêmes.

Trop souvent, les dirigeants des entreprises ne prennent pas assez au sérieux les exigences de la sécurité numérique. Ainsi, l'usage systématique d'un téléphone portable sécurisé est difficile à accepter.

Pour illustrer cette prégnance tous azimuts du risque numérique, nous avons prévu d'insérer en annexe du tome premier du rapport, un petit

questionnaire, imaginé par le même CIGREF, recensant certaines situations quotidiennes liées au numérique et proposant plusieurs réactions possibles.

Il a été remis à chacun d'entre vous les quelques pages de ce jeu-questionnaire et, tout en écoutant avec attention notre présentation à deux voix, vous avez peut-être déjà tenté de déterminer ce qu'aurait été votre attitude numériquement responsable dans tel ou tel cas.

Quand on parcourt l'ensemble de ce questionnaire, chacun ne peut que s'étonner de ses erreurs de réflexe ou des hésitations à opter pour la bonne option qui auraient constitué autant des failles de sécurité dans la vie quotidienne.

Cela illustre qu'il ne faudrait plus **jamais concevoir quelque avancée du numérique que ce soit sans qu'une analyse approfondie ait pu proposer, dans le même temps, des instruments de sécurité**. Cet enjeu pourrait, d'ailleurs, constituer une opportunité pour notre économie.

Cela suppose de faire preuve de davantage de cohérence dans la prise au sérieux du concept même de sécurité numérique. Et cela commence dès la conception des **organigrammes des entreprises** où l'« empêcheur de tourner en rond » que représente souvent le responsable de la sécurité n'est pas situé au bon niveau pour que ses conseils puissent être entendus et acceptés à temps par les dirigeants.

Ces affirmations ne sont pas excessives car des exemples quotidiens montrent que **les entreprises n'ont pas encore tiré les conséquences des impératifs que devraient leur dicter la sécurisation numérique de leurs activités**.

Dans de nombreuses entreprises, les employés utilisent indifféremment leurs matériels numériques personnels ou professionnels, d'autant que les usages sont de plus en plus nomades. Les accès Internet sont multiples, les personnes séjournant temporairement dans l'entreprise pas assez contrôlées, l'usage des clés USB s'est banalisé et les comportements inconséquents vis-à-vis de l'utilisation des objets connectés sont aussi variés qu'innombrables.

Et des exemples récents montrent que des pirates ou attaquants ont bien compris que **les failles du numérique peuvent être d'autant mieux exploités qu'elles sont élargies par les défaillances humaines**.

C'est ce que les spécialistes du numérique appellent l'ingénierie sociale associée aux attaques techniques. Tel a été encore le cas, à la fin de l'année 2014, à propos de l'attaque connue sous le nom d'« arnaque au président » où, après une étude poussée des habitudes numériques et des caractéristiques de chacun des protagonistes, un appel téléphonique du supposé président d'une société est adressé, le vendredi soir, à un comptable de cette entreprise pour lui demander d'adresser d'urgence, de la part du président, une somme importante qui permettra d'assurer *in extremis*, au

cours de la fin de semaine, la conclusion d'une négociation déjà bien avancée.

Ce procédé peut vous paraître enfantin voire grossier, mais, à la fin de l'année 2014, **l'entreprise Michelin** a déboursé **1,6 million d'euros**, piégée par cette arnaque.

De nombreux présidents, dirigeants d'opérateurs d'importance vitale ont été sollicités de la même manière et tous n'ont pas eu la chance d'avoir des personnels assez sensibilisés au risque numérique pour ne pas tomber dans de tels traquenards.

Parfois, même si l'attaque n'est pas identifiée immédiatement, il est encore possible d'interrompre les rebonds successifs de pays en pays de l'argent ainsi naïvement remis mais à condition d'opérer extrêmement rapidement.

M. Bruno Sido. – Je voudrais, avant de terminer notre présentation, et avant d'en venir à vos questions, évoquer les objets connectés dont chacun s'amuse et s'émerveille et qui ont constitué des cadeaux de Noël recherchés : il faut savoir que ces objets sont conçus d'abord pour séduire, **sans que la question de leur sécurité soit incluse** dès l'origine.

Or, d'après certaines personnes auditionnées, le nombre de ces objets par individu pourrait dépasser la cinquantaine dans quelques années et la plupart de ces objets communiqueront entre eux sans intervention ni contrôle humains.

D'où la recommandation de vos rapporteurs de **prévoir des protocoles de conception d'objets connectés incluant obligatoirement à tout coup des préconisations de sécurité** et, à tout le moins, une information sur l'absence de sécurité.

Pour résumer l'esprit des propositions de recommandations essentielles faites par vos rapporteurs en faveur d'une amélioration de la sécurité numérique des entreprises, nous vous les présentons en distinguant les trois temps d'une attaque : avant, pendant et après.

Avant une attaque numérique, il serait infiniment souhaitable pour les entreprises de :

- **classer les données** et **simuler des pertes d'archives** ;
- **chiffrer les données sensibles** ;
- **chiffrer les réseaux *Wi-Fi*** ;
- construire une **sécurité numérique dans la profondeur** ;
- établir un **plan global de sécurité** prévoyant l'homogénéité de celle-ci ;
- installer des **sondes sur le réseau,** dont des **sondes de détection d'attaque** ;

- n'acheter que des **matériels** et ne recourir qu'à des **fournisseurs référencés par l'ANSSI** ;
- **déconnecter les *SCADA* de l'Internet** ;
- **sécuriser les passerelles d'interconnexion** avec l'Internet ;
- **éviter l'usage d'infrastructures sans fil** (*Wi-Fi*) ;
- effectuer des **tests d'intrusion** et des **exercices réguliers de crises informatiques**, des **audits de sécurité** des règles informatiques ;
- **former à la sécurité informatique** ;
- mettre en place un **centre de sécurité opérationnel** ;
- **assurer le risque numérique.**

Mme Anne-Yvonne Le Dain. – **Pendant une attaque numérique**, il est urgent **:**

- **d'activer** les **cellules de crise** et les **équipes d'intervention** ;
- **d'informer sans délai l'ANSSI et la CNIL** ;
- **de communiquer avec d'autres opérateurs d'importance vitale (OIV)** ;
- **d'avoir à disposition le nom du développeur du site de l'entreprise**, ses clés d'accès, ses mots de passe et la manière d'obtenir les journaux informatiques ;
- **de réagir à un virus en moins de vingt-quatre heures** ;
- **d'analyser l'attaque** informatique subie.

M. Bruno Sido. – **Après une attaque numérique**, si une prévention avait été mise en place et utilisée lors de l'attaque, il faudrait **:**

- mettre en œuvre les enseignements des exercices de **restauration des archives** ;
- **changer les mots de passe**.

Si certaines entreprises concernées s'apercevaient qu'elles ont, malheureusement pour elles, négligé plusieurs de ces précautions, il ne leur resterait plus qu'à adopter d'urgence toutes les préconisations de vos rapporteurs.

Dans leurs préconisations, vos rapporteurs ont souhaité distinguer deux grandes catégories. D'abord **une vingtaine de recommandations générales**, classées en cinq sous-ensembles, puis, pour ceux qui souhaitent aller plus loin, **une centaine de recommandations placées sous un intitulé « *Vade-mecum pour la sécurité numérique des entreprises* »** où sont détaillées environ la moitié des prescriptions que la centaine d'auditions a inspirée à vos rapporteurs.

Il est donc possible d'avoir deux niveaux de lecture des recommandations du rapport, l'une, traditionnelle, avec les vingt premières

recommandations et l'autre, plus technique, et qui se veut opérationnelle, avec le *vade-mecum* destiné aux entreprises.

Faut-il rappeler que toutes les recommandations pouvant émaner de l'OPECST ne se traduisent pas obligatoirement ou uniquement dans un texte législatif mais peuvent prendre des formes plus directes à destination soit du Gouvernement, soit encore des entreprises, soit, enfin, des individus eux-mêmes puisque, vous le verrez à la lecture de ce rapport, chacun d'entre nous peut en tirer des leçons pour son comportement quotidien personnel.

Pour terminer, vos rapporteurs ont constaté qu'il existait peut-être, à ce stade de leurs travaux, comme cela est souvent le cas, une insuffisante adéquation entre l'objet du rapport et son intitulé initial. D'où la proposition de **modifier cet intitulé** pour mieux marquer que, au-delà des risques du numérique, il s'agit de **favoriser les conditions de la confiance** à mettre en lui et de mieux indiquer que ce rapport est très largement **tourné vers les entreprises**.

Le nouvel intitulé pourrait être, par exemple, « *La sécurité numérique des entreprises* » ou « *Les conditions de la confiance pour une sécurité numérique des entreprises* » ou bien d'autres encore que nous évoquerons ensemble lors de la discussion.

Nous vous remercions de votre attention et vous proposons de répondre maintenant à vos questions.

M. Jean-Yves Le Déaut. – Je voudrais tout d'abord vous remercier pour le travail qui a été accompli. La parole est à M. Daniel Raoul.

M. Daniel Raoul. – Je dois vous dire que j'ai eu un peu de difficulté à suivre compte tenu de la vitesse du débit avec lequel les orateurs ont exposé les conclusions de leurs travaux. Je relirai donc cela à tête reposée.

Avez-vous fait une distinction, quant au risque numérique, entre les voies hertziennes et les réseaux fibres ? Cela me paraît relativement important car l'on voit se développer le réseau *Wi-Fi* avec tout ce qu'on appelle la domotique, mais c'est également vrai dans une entreprise ; or, n'importe qui, avec un scanner de fréquences, peut attaquer ce système qui est d'une grande fragilité et ne procure aucune sécurité.

Je me souviens avoir préconisé, à l'occasion du versement de la subvention que j'accordais à une école d'ingénieurs, d'éviter le *Wi-Fi* dans les laboratoires et de préférer les réseaux câblés. Cette école d'ingénieurs, qui avait des contrats avec des entreprises privées, s'exposait inutilement.

Ma deuxième observation concerne l'impossibilité pour des compagnies d'assurance d'accepter d'assurer le risque numérique des entreprises.

En tout cas, dans les entreprises comme chez les particuliers, des précautions simples pourraient être prises comme l'arrêt de tous les

appareils en cas de non utilisation, au moins en fin de semaine, au lieu d'une simple mise en veille.

Par exemple, en ce moment, n'importe qui peut écouter ce qui se passe ici grâce à nos téléphones alors qu'ils sont en veille.

M. Bruno Sido. – Je serais tenté de répondre qu'effectivement, ce problème existe avec tout ce qui est hertzien, mais la sécurité n'est pas meilleure avec la fibre lorsque les fabricants ont prévu des « portes dérobées » aux bouts de celle-ci. Pour ceux qui ont des informations vraiment confidentielles à transmettre, cela n'est pas plus sûr.

D'ailleurs l'exemple de l'homme d'affaires qui se rend en Chine avec ses ordinateurs et ses téléphones personnels ou professionnels montre combien on est exposé à l'erreur. Il devrait partir avec des ordinateurs vides et des téléphones simples achetés pour la circonstance et non utilisés ensuite. Dans le cas contraire, il est susceptible de se faire piller les informations disponibles sur ses appareils, et, de ce fait, risque de ne pas pouvoir conclure de très importantes affaires.

Mme Catherine Procaccia, sénatrice. – Je trouve que vous avez été très ambitieux en pensant qu'un rapport de l'OPECST pouvait apporter des solutions au risque numérique.

En outre, depuis quelques années, il y a, comme vous le citez, l'ANSSI et d'autres organismes qui interviennent sans arrêt, ce qui n'empêche pas tous les risques. Alors les précautions que vous évoquez seraient importantes aussi bien pour les entreprises que pour les hommes politiques qui nous dirigent. Quant à ce que font les assemblées parlementaires, cela est plutôt public.

Je rapproche de ce que vous venez de dire de ce qui a été exposé précédemment aujourd'hui à propos des vaccins. Pour le risque numérique, c'est la même chose ; il y a des virus qui nous atteignent et des gens qui essayent d'attaquer les données des entreprises et des gouvernements.

Il pourrait y avoir des sortes de vaccins consistant à crypter les données et à éteindre tous les appareils systématiquement lors de leur non utilisation, même si on ne le fait pas.

Je ne sais pas si le rapport va pouvoir apporter grand-chose mais, en tout cas, je puis vous affirmer que, en matière d'assurance, il est actuellement impossible d'assurer le risque numérique puisque le principe de l'assurance repose sur l'analyse des risques qui se sont produits. Alors, quand vous dites que 73 % des entreprises se sont fait piller des données, comment voulez-vous que des assureurs puissent proposer quoi que ce soit puisque le coût de l'assurance risquerait d'être supérieur à celui de la sécurisation du système informatique de l'entreprise ?

J'ai la connaissance d'un certain nombre d'entreprises où les salariés se plaignent parce que, tous les mois, si ce n'est pas toutes les semaines, ils

ne peuvent plus accéder à leur messagerie parce qu'on leur demande de changer leurs mots de passe.

Il me semble que les entreprises qui exportent ont conscience de l'ampleur du risque numérique mais il reste difficile de trouver les moyens d'une sécurité totale, sans parler des moyens financiers et des moyens intellectuels qui risquent d'être inférieurs à ceux mis en œuvre par les pirates.

M. Daniel Raoul, sénateur. – En ce qui concerne la comparaison avec les virus, cela n'est pas tout à fait équivalent puisque, dans le domaine du numérique, outre les virus, il existe la volonté des pirates qui se livrent à l'attaque sans qu'il y ait forcément de virus injecté.

Mme Anne-Yvonne Le Dain. – Nous avons reçu en audition plus de cent personnes, de l'écrivain à des responsables industriels. En débutant cette étude, nous savions que le sujet était très riche, mais nous n'avions pas imaginé qu'il l'était à ce point. En fait, on entre dans un nouveau monde où l'on ne peut pénétrer avec les réflexes de l'ancien monde, plus rationnel.

Le nouveau monde est complètement multiforme, multi-ouvert et ne pas se protéger est une bêtise. Par exemple, après l'attaque contre les *Twin Towers*, les Américains ont pris le *Patriot Act* et s'en servent pour tout, y compris à des fins économiques. Ils ont condamné récemment une très belle entreprise française au motif qu'elle avait une sous- filiale dans un endroit célèbre où elle avait payé un contrat en dollars ; j'en suis resté abasourdie.

Donc les Américains se servent de la sécurité numérique comme d'un enjeu doctrinal, économique. Actuellement, les *GAFA (Google, Apple, Facebook et Amazon)* continuent à faire en sorte que la police de l'Internet soit assurée par une entreprise privée située en Californie, l'*ICANN,* grâce à laquelle la *NSA* américaine s'est procurée les adresses Internet du monde entier. Or, aujourd'hui, les entreprises américaines ont bien conscience que l'Europe est un espace pertinent économiquement. Elles sont donc présentes à Bruxelles où se négocie actuellement le traité transatlantique. Autour de la table de négociation sont présents des dizaines et des dizaines d'Américains qui expliquent à quel point ce traité est une évidence et qu'il faut lui soumettre l'ensemble du numérique.

Comme il y a davantage d'utilisateurs d'Internet en Europe qu'aux États-Unis d'Amérique, l'Europe est leur meilleur client. Il importe donc de se protéger des Américains, par exemple en créant un *Google* européen. Même si les Américains sont des alliés et des amis, économiquement nous sommes leur meilleur marché.

Sur la question de la sécurité numérique, nous disposons de tout ce qui convient en France et en Europe pour enclencher une dynamique sectorielle s'appuyant sur de nouveaux concepts, et permettant d'aller vers un autre monde que celui que l'on a connu jusque-là. Il n'y a plus de barrières économiques ou techniques comme autrefois ; aujourd'hui, tout est

réversible. Il faut de la vitesse, de la réactivité, de l'intelligence et de l'initiative locale, car l'échelon national ne fonctionne plus. Il faut multiplier les nouvelles procédures et les nouveaux procédés autour des concepts de multi-acteur et de multi-action, et construire de l'opacité au moyen de nuages de points. Il faut jouer sur le fait que le numérique est nanométrique et nanoseconde.

M. Jean-Yves Le Déaut. – Nous avons maintenant à conclure. Un certain nombre de corrections tardives ont été proposées, notamment sur le préambule et l'introduction. Avec l'accord des deux rapporteurs, j'ai comparé les versions et constaté que beaucoup de modifications souhaitées étaient relativement mineures. Si vous en êtes d'accord, je transmettrai le document annoté par mes soins aux rapporteurs afin qu'ils intègrent mes remarques au document final.

Le président Bruno Sido a indiqué votre intention de ne pas en rester aux aspects d'ordre général du sujet, comme la gouvernance mondiale de l'Internet, mais vous avez tout de même traitée celle-ci, et même bien traitée, et c'est réellement l'un des gros problèmes de la sécurité des systèmes informatiques que cette mauvaise gouvernance internationale de l'Internet. Je pense donc que des questions comme la démocratisation de l'*ICANN*, ou l'idée d'un affichage d'icônes renseignant mieux les usagers pourraient figurer dans la conclusion.

Finalement, tant qu'on n'aura pas fait évoluer le système de gouvernance, notamment au niveau des langues, car la domination linguistique de l'anglais conforte la mainmise non-américaine sur l'Internet, nous rencontrerons toujours de grandes difficultés à traiter les problèmes de sécurité numérique et de chaîne de sécurité.

À la fin du rapport, le *vade-mecum* à destination des entreprises est très bien. Il faudrait que la partie de la conclusion intitulée « *Faire de l'économie avec du droit* » figure avant les recommandations. Enfin, je suggérerais de développer les intitulés des principales recommandations.

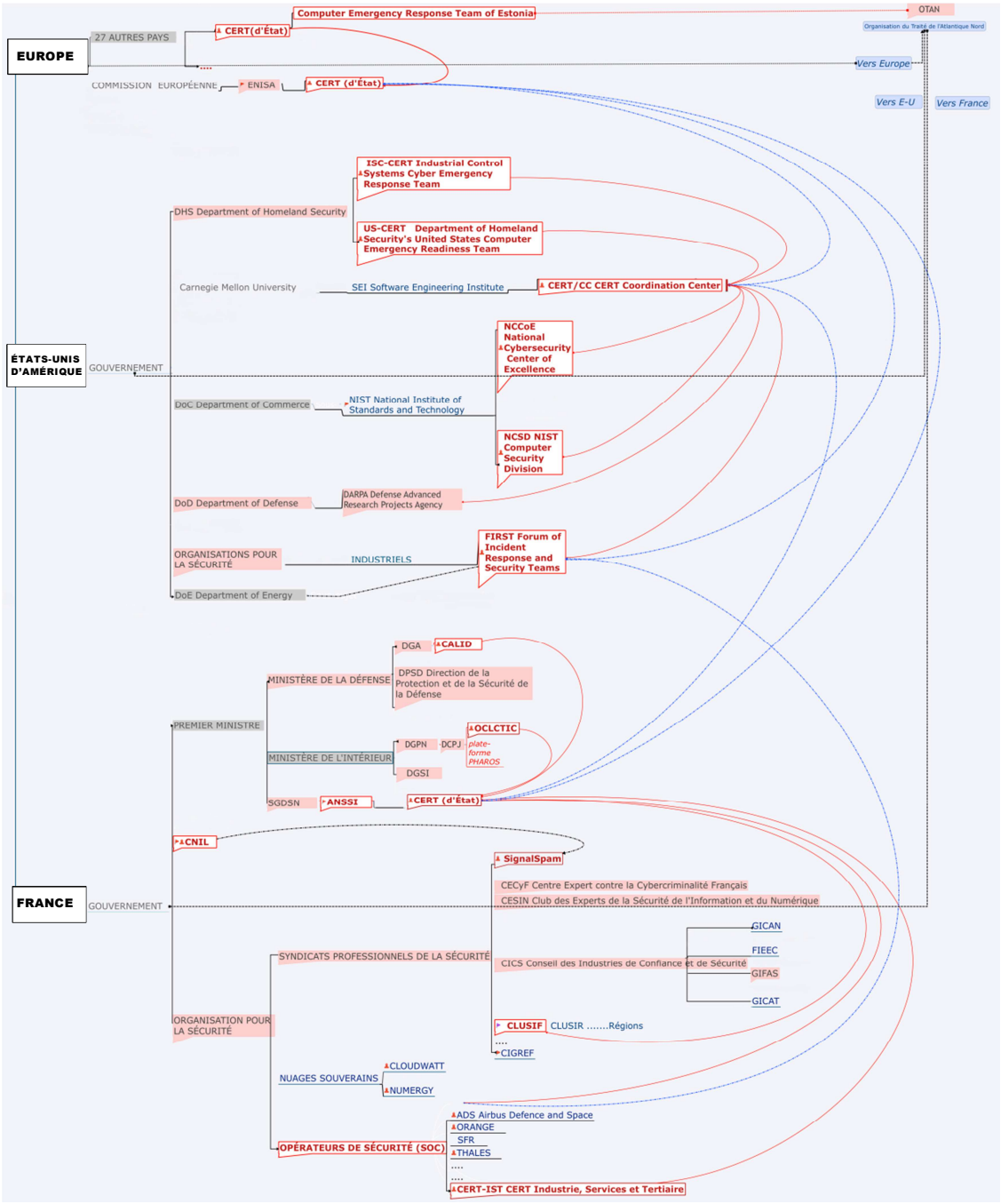
Nous sommes ainsi arrivés, d'après moi, à un très bon rapport. Je voudrais encore vous remercier car il s'agissait là d'une étude compliquée. Je voudrais encore remercier l'expert pour son apport technique.

Il reste maintenant à choisir un intitulé. Les rapporteurs ont carte blanche pour en décider.

Je vous propose d'adopter ce rapport et ses conclusions. Qui vote contre ? Qui s'abstient ? **Le rapport est adopté à l'unanimité** et je vous en remercie.

À la suite de ce débat, l'Office a autorisé la publication de ce rapport.

SCHÉMA DE LA SÉCURITÉ NUMÉRIQUE : INSTANCES PUBLIQUES OU PRIVÉES EN CHARGE DE LA SÉCURITÉ NUMÉRIQUE POUVANT CONCERNER LA FRANCE



	États ou unions d'États	En bleu	Entreprises ou groupements d'entreprises spécifiquement impliqués dans le numérique
	Entité ayant la sécurité comme objet	→	relation nationale
	Acteurs dont le cœur d'activité est la sécurité numérique opérationnelle (par exemple les centres d'opérations de sécurité (*SOC*) grâce à des ressources humaines spéciales ou à des guides pour les déployer.)	→	relation internationale
	Entité n'ayant pas la sécurité numérique comme seul objet		

***Source** : OPECST*

EXEMPLE DE BULLETIN DE L'ANSSI (26 JANVIER 2015)

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S.G.D.S.N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 26 janvier 2015
N° CERTFR-2015-ACT-004

Affaire suivie par:
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-004

1 - Vague de rançongiciels

Le CERT-FR est informé d'une recrudescence de messages électroniques malveillants incitant l'utilisateur à installer un rançongiciel sur son poste. Cet article s'inscrit dans la continuité de notre article précédent sur ce sujet (Bulletin d'actualité CERTFR-2014-ACT-048).

Un rançongiciel (ou ransomware) est un programme qui rend inaccessibles les fichiers de l'utilisateur, en général les documents bureautiques présents sur le profil de l'utilisateur (« Mes documents », « Mes Images », « Mes vidéos ») mais aussi (et surtout) dans tous les partages réseau ouverts en écriture à l'utilisateur compromis. Alors que les fichiers sont chiffrés par le rançongiciel, les fichiers originaux sont eux supprimés. A l'issue, un message de chantage est placé sur le bureau de l'utilisateur afin d'exiger le paiement d'une somme d'argent ou de bitcoins en échange de la clé de déchiffrement.

Les messages d'hameçonnage connus utilisent des techniques d'ingénierie sociale classiques indiquant par exemple « Votre fichier scanné est dans ce mail » pour inciter la victime à ouvrir l'archive en pièce jointe et à exécuter le maliciel.

La technique observée dans cette campagne est un message copiant la réception d'un fax dont la pièce jointe est une archive ZIP. Celle-ci contient le maliciel connu sous le nom de *CTB-Locker*. Ce rançongiciel figure parmi les plus avancés notamment au niveau de son cryptosystème et de ses communications à travers le réseau Tor, dont il embarque la librairie.

Recommandations

Le CERT-FR recommande les actions de prévention suivantes :

- la sensibilisation des utilisateurs : la plupart de ces messages sont non sollicités, d'un émetteur inconnu et contiennent des fautes d'orthographe ;
- l'utilisation des restrictions logicielles notamment pour interdire l'exécution de code depuis les répertoires temporaires ;
- la sauvegarde régulière des fichiers des utilisateurs sur des supports hors ligne ;
- la mise à jour des bases de signatures d'anti-virus et de passerelles de messagerie ;
- la protection appropriée des partages de fichiers, notamment en positionnant les permissions en lecture seule lorsque c'est possible ;
- l'application des correctifs de sécurité (système d'exploitation et applications).

Si un utilisateur est victime de ce type de maliciel, le CERT-FR recommande la conduite suivante :

- isoler au plus vite le poste compromis du réseau ;
- identifier le message malveillant et rechercher d'éventuelles copies envoyées à d'autres destinataires afin de les supprimer ;
- bloquer sur le serveur mandataire l'accès aux domaines ou URLs identifiés dans le message malveillant ;
- reformater le poste client et réinstaller un système sain ;

Secrétariat général de la défense et de la sécurité nationale – ANSSI – COSSI – CERT-FR
51, bd de La Tour-Maubourg **Tél.**: 01 71 75 84 50 **Web**: http://cert.ssi.gouv.fr
75700 Paris 07 SP **Fax**: 01 71 75 84 70 **Mél** : contact@cert.ssi.gouv.fr

– restaurer les copies de sauvegarde des fichiers perdus.

Le versement de la rançon à l'attaquant ne garantit ni le déchiffrement des fichiers ni la sécurité des moyens de paiement utilisés. Il peut notamment entraîner l'installation de maliciels supplémentaires sur le poste utilisé.

Documentation

– Bulletin d'Actualités CERTFR-2014-ACT-048 :
http://cert.ssi.gouv.fr/site/CERTFR-2014-ACT-048/
– Recommandation pour la mise en oeuvre d'une politique de restrictions logicielles sous Windows :
http://www.ssi.gouv.fr/IMG/pdf/NP_Applocker_NoteTech-v1.pdf
– Informations techniques sur CTB-Locker :
http://securelist.com/analysis/publications/64608/a-new-generation-of-ransomware/
https://blogs.mcafee.com/mcafee-labs/rise-backdoor-fckq-ctb-locker
– Méthodologie de suppression de mails malveillants :
http://blogs.technet.com/b/exchange/archive/2010/10/27/removing-specific-messages-from-your-exchange-server.aspx
– Site stop ransomware :
http://stopransomware.fr

2 - Le « certificate pinning »

Cet article présente une solution permettant de pallier des problèmes inhérents à la gestion des certificats sur Internet pour la sécurisation des échanges via le protocole HTTPS.

Concepts préalables

Un certificat X.509 contient trois informations importantes :

– un nom identifiant une entité ;
– une clé publique ;
– une signature cryptographique.

Le but d'un certificat est de prouver que la clé publique appartient à l'entité grâce à une signature cryptographique. La signature cryptographique est délivrée par une autorité de certification (AC) après un ensemble de vérifications.

Lorsqu'un navigateur se connecte à un site Internet via le protocole HTTPS (HTTP encapsulé par le protocole TLS), le site présente son certificat. Le navigateur est alors en mesure de s'assurer qu'il communique directement avec le site authentique en vérifiant la validité du certificat. Cette étape comprend, entres autres, la vérification de la signature cryptographique inclue dans le certificat.

Afin de vérifier la signature cryptographique, un client doit utiliser la clé publique de l'AC ayant effectué la signature. Pour l'obtenir de façon fiable, il peut l'extraire du certificat de l'AC, en prenant soin de vérifier la validité de ce certificat également. L'opération doit être réitérée jusqu'à arriver à un certificat dit "racine", connu à l'avance et jugé de confiance implicitement. La chaîne de certificats partant du certificat de départ jusqu'au certificat racine est aussi appelée chemin de certification.

Risques associés

Les navigateurs Internet utilisent une liste prédéfinie de certificats racines dont la confiance est reconnue publiquement. Cependant, plus cette liste est grande, plus la surface d'attaque est grande. En effet, la mauvaise pratique, simple erreur ou compromission d'une seule AC parmi celles se rattachant à un certificat racine peut mettre en péril toute l'infrastructure de confiance.

À titre d'exemple, en décembre 2012, des certificats émis frauduleusement ont été détectés. Ils permettaient à leur détenteur de se faire passer pour des sites dont le nom de domaine se termine par google.com. Cet incident est dû à une erreur de la part de l'autorité de certification Turque TURKTRUST [2] qui aurait délivré des certificats de AC intermédiaires au lieu de certificats finaux à des organisations.

Une mesure de contournement, le *certificate pinning*

En reprenant l'incident impliquant TURKTRUST, il est intéressant de noter qu'une simple observation du chemin de certification permet de repérer un élément inhabituel : le chemin remonte à une autorité racine Turque, ce qui semble étrange pour un domaine google.com et dont le certificat se rattache habituellement à l'AC racine GeoTrust Global. De manière sommaire, c'est sur ce raisonnement que repose le *certificate pinning*. Il permet, pour un site donné, d'« épingler » un point de son chemin de certification et d'émettre une alerte si cette contrainte supplémentaire n'est pas respectée. C'est d'ailleurs grâce à cette méthode, utilisée dans son navigateur Chrome, que Google avait détecté les certificats frauduleux liés à TURKTRUST.

Le *certificate pinning* peut être appliqué à plusieurs niveaux. Du moins au plus restrictif, il est par exemple possible :

- d'exiger que le certificat d'une AC particulière se trouve sur le chemin de certification d'un site Internet ;
- d'exiger une clé publique précise pour le certificat d'un site Internet (plus justement appelé *public key pinning*) ;
- d'exiger un certificat précis pour un site Internet.

Les principaux navigateurs, Internet Explorer, Chrome [4] et Firefox [5], supportent le *certificate pinning* et incluent des règles pour quelques sites Internet très connus. Dans le cas d'Internet Explorer, le support n'est pas natif avant la version 11 mais peut être apporté grâce à l'outil Microsoft EMET [6]. Ce dernier permet également de rajouter ses propres règles pour les sites Internet de son choix. A partir de la version 11 d'Internet Explorer, la fonctionnalité *SmartScreen* a été étendue [7], permettant à Microsoft de détecter des anomalies grâce à une supervision proche du *certificate pinning*.

Pour conclure, bien que le *certificate pinning* ne soit pas une solution idéale, notamment à cause de la complexité induite par la création ou mise à jour des règles, il reste un moyen simple et efficace pour remédier à des faiblesses de l'infrastructure de gestions de certificats basée sur les autorités de certification. D'autres méthodes de gestion sont actuellement à l'étude. Nous pouvons notamment citer DANE (DNS-Based Authentication of Named Entities) reposant sur des informations enregistrées dans l'infrastructure DNS, protégées par DNSSEC, pour associer un certificat ou une clé publique à un nom de domaine. L'adoption d'une méthode alternative telle que DANE nécessiterait cependant des modifications plus importantes des programmes l'utilisant, notamment les navigateurs.

Documentation

1 Article de Google annonçant la détection de certificats pour ses domaines remontant à l'IGC/A : http://googleonlinesecurity.blogspot.fr/2013/12/further-improving-digital-certificate.html
2 Article de Google annonçant la détection de certificats frauduleux remontant à l'autorité de certification TURKTRUST : http://googleonlinesecurity.blogspot.fr/2013/01/enhancing-digital-certificate-security.html
3 Recommandations de sécurité concernant l'analyse des flux HTTPS : http://www.ssi.gouv.fr/IMG/pdf/NP_TLS_NoteTech.pdf
4 Annonce du support du *public key pinning* dans Chrome : https://www.imperialviolet.org/2011/05/04/pinning.html
5 Annonce du support du *public key pinning* dans Firefox : https://blog.mozilla.org/security/2014/09/02/public-key-pinning/
6 Annonce du support du *certificate pinning* dans EMET permettant à Internet Explorer d'en bénéficier : http://blogs.technet.com/b/srd/archive/2013/05/08/emet-4-0-s-certificate-trust-feature.aspx
7 Mise à jour de la fonctionnalité *SmartScreen* pour Internet Explorer 11 : http://blogs.technet.com/b/pki/archive/2014/02/22/a-novel-method-in-ie11-for-dealing-with-fraudulent-digital-certificates.aspx

3 - Bulletin de sécurité Oracle

Lors de la publication de son bulletin de sécurité du 19 janvier 2015, Oracle a annoncé des vulnérabilités concernant 13 de ses produits, notamment :

- Oracle Database ;
- Oracle Java SE ;
- la suite de produits Oracle Sun Systems ;

– Oracle Linux et les produits de virtualisation ;
– Oracle MySQL ;

Les vulnérabilités touchant Oracle Database sont considérées majoritairement par l'éditeur comme mineures ou importantes. La vulnérabilité CVE-2015-6567 sur le composant *Core RDBMS* est considérée comme critique. Celle-ci permet à un attaquant distant d'effectuer une exécution de code arbitraire distante.

Les vulnérabilités touchant Oracle Java SE sont considérées majoritairement par l'éditeur comme importantes ou critiques. Les vulnérabilités critiques affectent les composants *Hotspot*, *JAX-WS*, *RMI* et *Libraries*. Oracle signale notamment que les vulnérabilités très critiques (ayant un score de criticité de 10/10) CVE-2015-0408, CVE-2014-6601, CVE-2015-0412 et CVE-2014-6549 permettent toutes une exécution de code arbitraire distante relativement aisée.

Les vulnérabilités impactant les produits Oracle Sun Systems sont considérées majoritairement par l'éditeur comme mineures ou importantes. Cependant, deux vulnérabilités sur les composants *Solaris Cluster* et les serveurs Fujitsu *M10-1*, *M10-4* et *M10-4S* sont considérées respectivement comme critique et très critique. Cette dernière (CVE-2013-4784) permet une exécution de code arbitraire distante relativement aisée et ne nécessite pas d'authentification préalable à l'exploitation.

Les vulnérabilités concernant Oracle Linux et les produits de virtualisation sont considérées majoritairement par l'éditeur comme mineures ou importantes. Cinq vulnérabilités sur un total de dix permettent une atteinte à l'intégrité, à la confidentialité des données et/ou un déni de service, le tout de façon distante et majoritairement sans nécessiter d'authentification préalable. Les vulnérabilités les moins critiques sont exploitables localement et nécessitent donc très majoritairement une authentification afin de les exploiter.

Les vulnérabilités touchant Oracle MySQL sont considérées majoritairement par l'éditeur comme importantes. Elles induisent dans une grande majorité un déni de service partiel sur le service, à l'exception de :

– la vulnérabilité CVE-2015-0411 (importante), permettant une atteinte partielle à l'intégrité et à la confidentialité des données de façon distante et non authentifiée ;
– la vulnérabilité CVE-2015-0374 (mineure), permettant une atteinte à la confidentialité des données nécessitant une authentification. Selon l'éditeur cette dernière vulnérabilité serait complexe à exploiter.

Documentation

– Bulletin de sécurité Oracle CPUJan2015 du 20 janvier 2015 :
http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
– CERTFR-2015-AVI-030 : Multiples vulnérabilités dans Oracle Sun Systems Products Suite :
http://www.cert.ssi.gouv.fr/site/CERTFR-2015-AVI-030/index.html
– CERTFR-2015-AVI-031 : Multiples vulnérabilités dans Oracle Virtualization :
http://www.cert.ssi.gouv.fr/site/CERTFR-2015-AVI-031/index.html
– CERTFR-2015-AVI-032 : Multiples vulnérabilités dans Oracle MySQL :
http://www.cert.ssi.gouv.fr/site/CERTFR-2015-AVI-032/index.html
– CERTFR-2015-AVI-033 : Multiples vulnérabilités dans Oracle Database Server :
http://www.cert.ssi.gouv.fr/site/CERTFR-2015-AVI-033/index.html
– CERTFR-2015-AVI-034 : Multiples vulnérabilités dans Oracle Java SE :
http://www.cert.ssi.gouv.fr/site/CERTFR-2015-AVI-034/index.html

4 - Rappel des avis émis

Dans la période du 19 au 25 janvier 2015, le CERT-FR a émis les publications suivantes :

– CERTFR-2015-ALE-001 : Vulnérabilité dans Adobe Flash Player
– CERTFR-2015-AVI-028 : Multiples vulnérabilités dans Moodle
– CERTFR-2015-AVI-029 : Vulnérabilité dans PolarSSL
– CERTFR-2015-AVI-030 : Multiples vulnérabilités dans Oracle Sun Systems Products Suite
– CERTFR-2015-AVI-031 : Multiples vulnérabilités dans Oracle Virtualization
– CERTFR-2015-AVI-032 : Multiples vulnérabilités dans Oracle MySQL
– CERTFR-2015-AVI-033 : Multiples vulnérabilités dans Oracle Database Server
– CERTFR-2015-AVI-034 : Multiples vulnérabilités dans Oracle Java SE
– CERTFR-2015-AVI-035 : Vulnérabilité dans Huawei Quidway

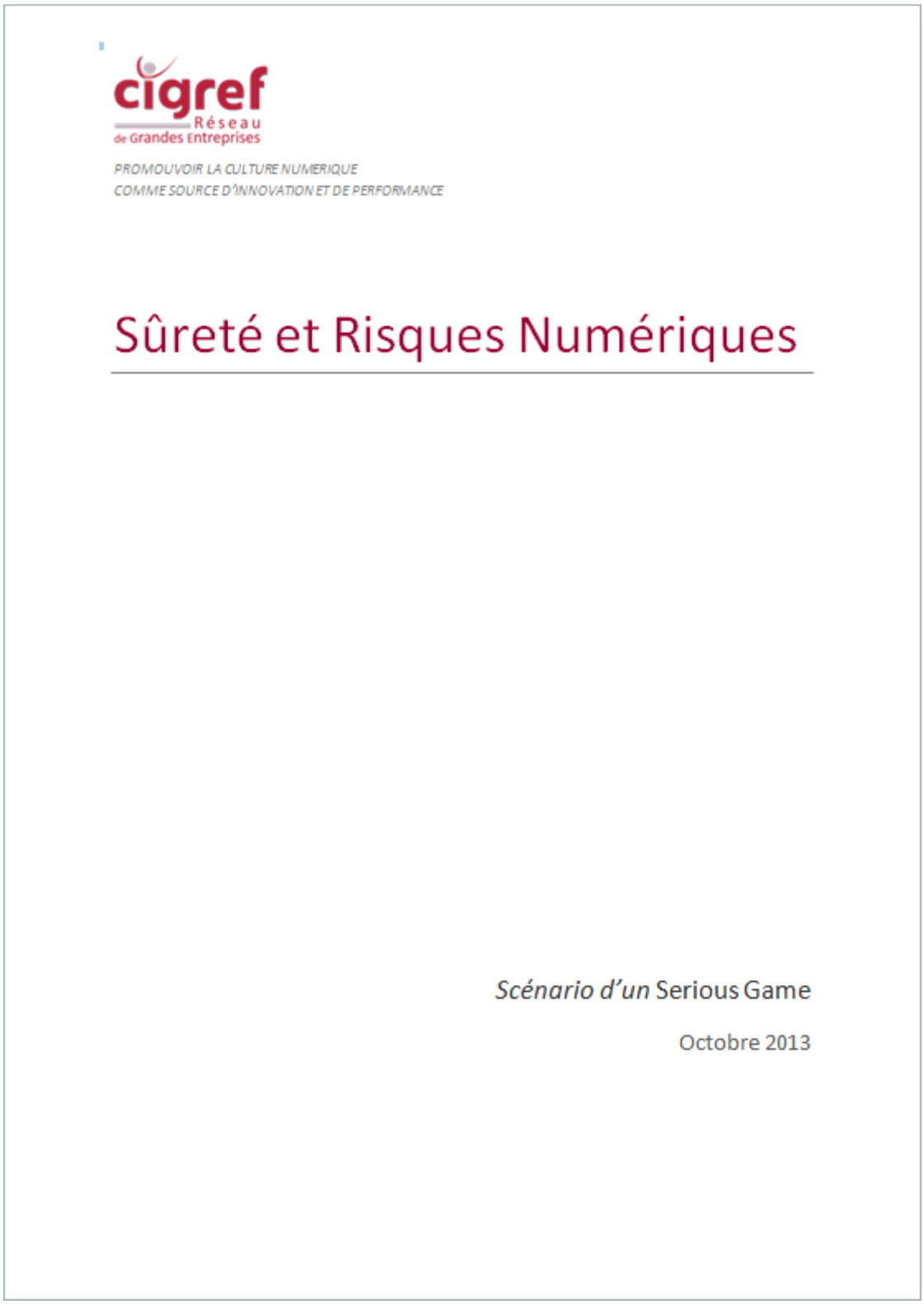
- CERTFR-2015-AVI-036 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2015-AVI-037 : Vulnérabilité dans Adobe Flash Player

Gestion détaillée du document

26 janvier 2015 version initiale.

Conditions d'utilisation de ce document : http://cert.ssi.gouv.fr/cert-fr/apropos.html
Dernière version de ce document : http://cert.ssi.gouv.fr/site/CERTFR-2015-ACT-004

LA SÉCURITÉ NUMÉRIQUE PAR LE JEU : SCÉNARIO D'UN *SERIOUS GAME* – OCTOBRE 2013 RAPPORT DU CIGREF - RÉSEAU DE GRANDES ENTREPRISES



cigref Réseau de Grandes Entreprises

SYNTHÈSE

La sécurité numérique est un sujet particulièrement sensible pour les entreprises aujourd'hui, à l'heure où les attaques se font de plus en plus fréquentes et de plus en plus violentes.

Face à cela, dans une grande majorité des cas, l'utilisateur est une des lignes de défense les plus importantes, au-delà de l'ensemble des solutions techniques et juridiques que l'entreprise peut déployer. Pourtant, ce sujet reste difficile à aborder, considéré souvent comme technique, contraignant et inintéressant par les collaborateurs.

Il est donc primordial de trouver une manière de faire passer les messages clés en matière de sécurité auprès de l'ensemble des employés, par un moyen remportant l'adhésion de tous.

Dans ce contexte, la solution du *Serious Game* convient parfaitement à la situation. Ce nouveau vecteur de formation permet de faire aisément passer les messages clés, tout en faisant adhérer les utilisateurs à un outil ludique innovant, qui adopte une démarque pédagogique attractive et stimulante et qui s'adapte à la disponibilité des utilisateurs.

Le groupe de travail CIGREF et les auditeurs de la promotion 2012/2013 du cycle CIGREF-INHESJ « Sécurité Numérique » ont donc cherché à faire un premier pas en ce sens en élaborant un scénario de *Serious Game*.

Il comprend un ensemble de situations de la vie courante des collaborateurs de l'entreprise, qui peuvent amener à des risques de sécurité importants pour le patrimoine informationnel de l'entreprise. Ces situations ont été catégorisées selon quatre environnements :

- en voyage,
- dans son entreprise,
- à son bureau, devant son ordinateur,
- à son domicile.

Ces situations sont accompagnées de fiches pratiques qui regroupent les bonnes pratiques à suivre dans ces cas et les risques qu'elles couvrent.

Le CIGREF, réseau de Grandes Entreprises, a été créé en 1970. Il regroupe plus de cent très grandes entreprises et organismes français et européens de tous les secteurs d'activité (banque, assurance, énergie, distribution, industrie, services...). Le CIGREF a pour mission de promouvoir la culture numérique comme source d'innovation et de performance.

TITRE DU RAPPORT : SÛRETÉ ET RISQUES NUMÉRIQUE : SCENARIO D'UN *SERIOUS GAME*

EQUIPE DU CIGREF

Jean-François PÉPIN – Délégué général
Sophie BOUTEILLER – Directrice de mission
Anne-Sophie BOISARD – Directrice de mission
Josette WATRINEL – Secrétaire de direction
Frédéric LAU – Directeur de mission
Matthieu BOUTIN – Chargé de mission
Marie-Pierre LACROIX – Chef de projet
Josette LEMAN – Assistante de direction

REMERCIEMENTS :

Nos remerciements vont à Jean-Marc de FELICE, Directeur des Ressources Techniques de Radio France, qui a piloté cette réflexion.

Nous remercions les personnes qui ont participé au groupe de travail CIGREF :

Nicolas BURTIN – Caisse des Dépôts
Pierre CACCAVELLI – RSI
Brigitte DECLERCK – Agirc Arrco
Martine FREREBEAU – La Poste
David GARCIA – France Télévisions
Emmanuel GARNIER – Systalians
Philippe GEERAERT – Thalès
Mathias LARGILLIERE – Saur
Frédéric LENOIR – RTE
Marc MENCEL – Nexter Group
Fabrice NERACOULIS – SNCF
Guy NICOLAS – Nexans
Joël NOIROT – SNCF
Jean-Michel PERRIN – La Poste
Gérard PESCH – Thalès
Yann PIEDERRIERE – Air Liquide
Gilles SAINT JEVIN – SNCF
Charles SUTTER – Société Générale
Pierre TARIF – GDF Suez
Matthieu WILLM – Dassault Aviation
Isabelle ZAWADZKI BERTHET - Areva

et les auditeurs de la promotion 2012-2013 du cycle Sécurité Numérique CIGREF-INHESJ :

Emmanuel ADELINE – Société Générale
Xavier AGHINA – Orange
Rémi BAGUE – SCOR
Olivier DALOY - LVMH
Pierre DELORT – ANDSI
Thierry GAUCHET – Sanofi
Pierre HASTIR – Euro Disney
Philippe LESEIGNEUR – EDF
Philippe MARGAINE – CCI Vaucluse
Olivier PARENT – SPIE
Marc RAYMOND – Essilor
Stéphane ROYER – Axa
Betty SFEZ – Deleporte Wentz Avocats
Christophe VIATTEAU – Total

Ce document a été rédigé par Matthieu BOUTIN, CIGREF.

POUR TOUT RENSEIGNEMENT CONCERNANT CE RAPPORT, VOUS POUVEZ CONTACTER LE CIGREF AUX COORDONNÉES CI-DESSOUS :

CIGREF, Réseau de Grandes entreprises
21, avenue de Messine 75008 Paris
Tél. : + 33.1.56.59.70.00
Courriel : contact@cigref.fr

Sites internet :
http://www.cigref.fr/
http://www.fondation-cigref.org/
http://www.histoire-cigref.org/
http://www.questionner-le-numerique.org
http://www.entreprises-et-cultures-numeriques.org

cigref Réseau de Grandes Entreprises

SOMMAIRE

1. Sécurité et risques numériques pour l'entreprise 1
2. Apport des *Serious Games* 3
2.1. Qu'est-ce qu'un *Serious Game* ? 3
2.2. Le jeu au service de la formation 4
2.3. Enjeux des *Serious Games* pour l'entreprise 4
2.4. La sécurité numérique par le jeu 4
3. Présentation du scénario et remarques générales 5
3.1. Constats 5
3.2. Objectifs 5
3.3. Personnalisation – Paramétrage 6
3.4. Evolutivité 6
3.5. Mesurabilité - Suivi et *reporting* 6
3.6. Fidélisation du joueur 6
4. Univers de jeu et scénarios 7
4.1. En voyage 7
4.1.1. Raisons du choix de cet univers 7
4.1.2. Description des saynètes 7
4.2. Dans l'entreprise 9
4.2.1. Raisons du choix de cet univers 9
4.2.2. Description des saynètes 9
4.3. Devant son ordinateur, à son bureau 12
4.3.1. Raisons du choix de cet univers 12
4.3.2. Description des saynètes 13
4.4. Au domicile 15
4.4.1. Raisons du choix de cet univers 15
4.4.2. Description des saynètes 15
5. Fiches Conseil : bonnes pratiques et risques couverts 18
En mobilité 18
Dans un lieu public 18
Déplacement dans un pays « à risques» 18
Collaboration avec un partenaire 18
Connexion de visiteurs 19
En quittant son poste de travail 19
Installation de nouveaux logiciels 19
Mise à jour des postes de travail 19
Mots de passe 19

Détection d'anomalie sur les postes de travail 20
Courriels suspects 20
Bon usage des systèmes d'information professionnels 20
6. Prochaines étapes 21
Annexe : Préconisations techniques 22
Hébergement 22
Compatibilité et optimisation 22
Qualité et pérennité 22
Performance 22
Sécurité 22
Administration 23
Déclarations réglementaires 23

1. SÉCURITÉ ET RISQUES NUMÉRIQUES POUR L'ENTREPRISE

La sécurité de l'information a toujours été une composante importante de la stratégie des entreprises, ne serait-ce que pour la protection des données confidentielles qu'elles détiennent. Mais si la sécurité était facilitée auparavant par une certaine autarcie du système d'information et que sa gestion en était donc confiée aux experts du domaine, il n'en est plus de même aujourd'hui.

Puisque le numérique a un caractère transversal dans l'entreprise, les risques liés ne sont pas circonscrits au seul périmètre des systèmes d'information. Le CIGREF a publié une étude[1] sur ce sujet en 2011, qui avait pour objectif d'en établir une cartographie. 8 familles de risques ont donc été identifiées : ressources humaines, dématérialisation des rapports humains, stratégie, contrôle des systèmes d'information, éthique et juridique, patrimoine numérique, marketing, et risques périphériques.

Certains risques sont localisés, comme les risques marketing qui sont principalement concentrés sur les relations avec les clients, et tous n'apparaissent pas au même moment. Alors que certains seront d'actualité tout au long de la vie de l'entreprise, comme ceux relatifs à la cybercriminalité, d'autres n'apparaissent qu'au moment du passage vers le numérique, pour s'estomper ensuite. C'est le cas du risque lié au manque d'adhésion des employés, ou celui lié à la concurrence entre supports de vente. Ces distinctions sont importantes lorsqu'il s'agit de chercher à faire de la prévention car les politiques de gestion des risques à court, moyen et long terme dépendent du moment où les risques sont susceptibles d'apparaitre.

La sécurité n'est donc plus limitée à un débat d'expert mais bien portée au plus haut niveau stratégique dans l'entreprise, car elle a un impact fort sur leur pérennité. L'atteinte aux données stratégiques et confidentielles peut en effet avoir des conséquences sur la survie même de l'entreprise.

Dans un contexte où l'externalisation des systèmes est de plus en plus courante, il ne faut pas oublier que la constitution d'une politique de sécurité des systèmes d'information passe par une analyse fine des risques. Dans ce cadre, toutes les données, et les traitements qui les concernent, ne nécessitent pas le même niveau de préoccupation, et seront donc traitées avec une considération sécuritaire adaptée. L'entreprise doit donc mettre en place les moyens juridiques et techniques nécessaires pour garantir la sécurité de son patrimoine.

[1] Les risques numériques pour l'entreprise, CIGREF, mars 2011

Cette problématique est d'ailleurs traitée par un guide rédigé conjointement par le CIGREF, l'IFACI et l'AFAI sur la protection des données dans le Cloud[2]. Ce guide, à destination des dirigeants d'entreprises, a pour but d'aiguiller sur les réflexions à mener autour de la caractérisation des données selon leur degré de confidentialité et de leur externalisation possible on non dans les différents types de *Cloud* (interne/externe, public/privé).

Mais au-delà des moyens technologiques et organisationnels mis en œuvre dans les entreprises pour maitriser la sécurité liée à l'IT, le facteur humain, l'utilisateur du SI de l'entreprise, représente l'un des risques majeurs encourus. C'est également l'un des plus difficiles à appréhender et à maitriser.

Parce que chaque employé de l'entreprise a accès au système d'information de l'entreprise, et donc potentiellement à un certain nombre de données sensibles, la sécurité numérique en entreprise doit être portée par l'ensemble des collaborateurs. Tous ont un rôle important à jouer dans la protection de leur entreprise. C'est pourquoi il est nécessaire que la communication sur ce sujet soit portée par les plus hautes instances dirigeantes au sein de l'entreprise, pour que les bonnes pratiques de sécurité soient intégrées dans la culture et les valeurs de l'entreprise.

Les risques de cybercriminalité et de cyberterrorisme ont connu une augmentation de fréquence d'occurrence et de gravité au cours des deux dernières années. Sujet encore mal connu et ne remportant pas l'intérêt de la grande majorité des employés, il est primordial de trouver un moyen de l'aborder afin que tous soient sensibilisés.

[2] Cloud et protection des données : guide pratique à l'attention des directions opérationnelles et générales, CIGREF-AFAI-IFACI, mars 2013

2. APPORT DES *SERIOUS GAMES*

Le traitement des questions de sensibilisation, d'information et de formation des collaborateurs de l'entreprise à la question de la sécurité apparait donc comme primordial, et dans ce domaine, la quasi-totalité des moyens de formation a déjà été employée. Formations magistrales, mises en situation, *e-learning*, films de promotion..., tous ces moyens ont montré une efficacité limitée, que ce soit sur la taille de la population touchée par cette formation, et sur la retenue des messages par les auditeurs.

On considère que nous retenons différemment les choses selon le moyen utilisé :

- 10% de ce que nous lisons
- 20% de ce que nous entendons
- 30% des images que nous voyons
- 50% de ce que nous voyons ET entendons (films, démonstrations...)
- 70% de ce que nous disons (participation à une discussion, présentation...)
- 90% de ce que nous disons ET faisons (simulation d'une expérience réelle)

Le jeu semble alors être un moyen très pertinent pour faire évoluer les comportements des utilisateurs.

2.1. Qu'est-ce qu'un *Serious Game* ?

Les *Serious Games* sont des moyens ludiques pour aborder des aspects sérieux. Ils ont donc une finalité utilitaire, en utilisant les ressorts des jeux pour y parvenir. Nous en gardons la définition suivante :

> *« Application informatique, dont l'intention initiale est de combiner, avec cohérence, à la fois des aspects sérieux (Serious) tels, de manière non exhaustive et non exclusive, l'enseignement, l'apprentissage, la communication , ou encore l'information, avec des ressorts ludiques issus du jeu vidéo (Game) »* (Julian Alvarez, Thèse en Science de la communication et de l'Information, 2007)

Le *Serious Game* se trouve donc à mi-chemin entre le jeu vidéo et le simulateur, en prenant les dimensions ludiques du premier (facteurs de motivation) et la finalité sérieuse du second (métier, pédagogie, etc.).

Un *Serious Game*, pour être efficace, ne doit pas seulement « avoir un air ludique ». Il doit utiliser un certain nombre de ressorts issus du monde du jeu vidéo qui apporteront une forte motivation pour les utilisateurs : immersion, quêtes, missions, récompenses, suspense, dramaturgie. Les facteurs de motivation sont alors divers, qu'ils soient internes à la personne (intérêt personnel, curiosité, challenge, impact émotionnel) ou externes (obtention de compliments, amélioration des compétences...).

2.2. Le jeu au service de la formation

E-learning et *Serious Game* sont donc bien deux méthodologies de formation radicalement différentes. Le module de *e-learning* va se servir des ressorts d'une formation classique, à savoir une première partie didactique qui présente les connaissances à acquérir puis un contrôle à la fin. Le *Serious Game*, quant à lui, a une approche radicalement différente, basée sur le principe « essai-erreur ». L'apprenant intégrera d'autant mieux les messages clés qu'il se sera confronté aux différentes situations, se sera « trompé », et aura appris de ses erreurs (les conséquences des erreurs doivent alors être montrées). Le *Serious Game* de formation tire donc son intérêt non pas du résultat final mais du temps passé dessus et du nombre de situations rencontrées, en offrant une rejouabilité importante.

3. Enjeux des *Serious Games* pour l'entreprise

Pour une entreprise, les enjeux des *Serious Games* sont multiples : baisser le coût global de la formation (adaptation aux pays, moyens matériels), passer d'une pédagogie « passive » à une pédagogie « active », former sur des fondamentaux « métiers »... Plus que des jeux, ils constituent un nouveau mode d'apprentissage.

La perception des *Serious Game* est très bonne au sein de l'entreprise avec de très hauts niveaux de satisfaction. Il y a une forte attractivité pour ce moyen par rapport à la formation en distanciel : alors que 70% des apprenants ne terminent jamais les modules *e-learning*, 100% des apprenants vont jusqu'au bout du *Serious Game*[3]. La notion de « *scoring* » intégrée est importante car elle apporte un effet viral intense et incite les participants à se lancer dans une course au meilleur score. Cela peut d'ailleurs faire l'objet de challenges au sein de l'entreprise.

4. La sécurité numérique par le jeu

S'il est bien un sujet sur lequel la communication est difficile, c'est bien la sécurité numérique. Souvent considéré comme un empêcheur de tourner en rond, le responsable de la sécurité des SI obtient généralement des résultats mitigés sur les éléments de sensibilisation qu'il fait circuler au sein de l'entreprise. Face à un sujet aussi sérieux, le CIGREF considère que le jeu est un moyen efficace de véhiculer les messages clés autour des risques numériques. Il a donc cherché à développer un scénario de *Serious Game*, centré autour de situations reconnues comme étant à risques et adapté à l'ensemble des collaborateurs de l'entreprise. La question d'une formation plus « technique » n'est donc ici pas abordée, même si la possibilité de réaliser plusieurs épisodes de jeu est envisageable afin de faire le tour complet de la problématique.

[3] Chiffres issus d'une étude menée chez Renault en 2012

3. PRÉSENTATION DU SCÉNARIO ET REMARQUES GÉNÉRALES

Les grands principes du *Serious Game* sur la sécurité numérique reposent sur la mise en situation d'un joueur dans différents univers représentatifs de situations courantes de risques numériques (le Guide d'hygiène informatique élaboré par l'ANSSI a notamment été pris en référence afin de garder une cohésion globale avec les actions menées par l'Etat en ce sens).

Chaque situation comprend :

- Une mise en contexte
- L'arrivée d'un évènement
- Un choix multiple
- Le passage à la situation suivante, si le choix est bon
- Des explications claires, si le choix est mauvais

Le scénario proposé s'articule autour de quatre univers décrivant des situations spécifiques :

- En voyage
- Dans l'entreprise
- Devant son ordinateur
- Au domicile.

3.1. Constats

L'élaboration du scénario est partie de trois constats fondateurs :

- Les collaborateurs utilisent les systèmes d'information dans le cadre de leur vie professionnelle et personnelle
- Parmi les collaborateurs de nos sociétés, peu d'entre eux sont sensibilisés à la sécurité des systèmes d'information
- Pourtant les menaces courantes ciblent de plus en plus la crédulité des collaborateurs et les outils informatiques qu'ils utilisent.

3.2. Objectifs

Le scénario du *Serious Game* vise donc plusieurs objectifs pour l'entreprise :

- Faire prendre conscience aux collaborateurs de nos entreprises des risques encourus de par l'utilisation de nos systèmes d'information
- S'assurer qu'un maximum de nos collaborateurs adoptent de bonnes pratiques par le biais de formations professionnelles et ludiques (le collaborateur gagne en compétence tout en suivant une formation non rébarbative)
- S'assurer que les collaborateurs se reconnaissent dans les univers abordés en intégrant des contextes variés : en déplacement, dans la vie de tous les jours, à son domicile

- Permettre au collaborateur de mieux appréhender les risques numériques sans pour autant en faire prendre à son entreprise
- Pérenniser la sensibilisation aux risques numériques en incitant les collaborateurs à se confronter régulièrement à cet outil pédagogique.

3. Personnalisation – Paramétrage

La personnalisation des quatre univers aux identités graphiques des différentes entreprises auxquelles le *Serious Game* est destiné sera un élément clé d'appropriation de l'outil par les collaborateurs de l'entreprise. Par ailleurs, le jeu sera paramétrable pour s'adapter au contexte spécifique et à la politique de sécurité de chaque entreprise.

Parmi les éléments techniques importants, le jeu devant être utilisable par tous et à n'importe quel moment, il fonctionnera sur PC comme sur support mobile (tablette, *smartphone*), en mode *SaaS*. Il devra être multilingue (*a minima* français et anglais) et garantir l'accessibilité aux collaborateurs en situation de handicap.

4. Evolutivité

La sécurité des systèmes d'information est en constante évolution. Les menaces grandissent et de nouvelles font leur apparition constamment. Cela entraîne donc la nécessité de mettre à jour ce jeu régulièrement, par l'ajout de modules complémentaires dédiés.

5. Mesurabilité - Suivi et *reporting*

Le *Serious Game* devra permettre un suivi des performances et de la participation des collaborateurs (consultation de l'historique des participations, des scores, des temps passés dans le jeu, etc.) par un accès à des statistiques d'utilisation. Cela permettra d'assurer le suivi de la campagne de sensibilisation auprès des collaborateurs.

6. Fidélisation du joueur

Le jeu devra permettre aux collaborateurs de prendre conscience de leurs progrès en matière de compréhension des risques numériques en les matérialisant par différents niveaux de difficulté. Il faut garantir un certain niveau de rejouabilité qui offrira une meilleure captation des messages clés.

Les éléments clés de la session de jeu (situations rencontrées, bonnes pratiques, score...) seront restitués au joueur en fin de session, afin qu'il puisse garder une trace de son apprentissage. Le jeu doit comporter une fonction qui permettra au joueur de mesurer sa progression (points acquis, niveaux de jeu, ...) et inclura une fonction « d'assistance » présentant des fiches d'aide (qui sont annexées à ce document).

4. UNIVERS DE JEU ET SCÉNARIOS

Cette section du document présente de manière détaillée les situations qui ont été retenues dans chaque univers, avec les propositions d'actions liées. La description des saynètes comprend ici la situation initiale, l'élément perturbateur et l'ensemble des choix proposés, avec l'effet de chacun de ces choix, selon la légende suivante :

: Action éliminatoire
: Action très risquée
: Action risquée
: Action attendue du collaborateur

1. En voyage

1. Raisons du choix de cet univers

- La mobilité est un facteur de risque de plus en plus avéré et dont l'impact est d'autant plus important
- La sensibilisation des travailleurs nomades permet d'assurer une meilleure propagation des messages / bonnes pratiques et ces collaborateurs constituent des cibles privilégiées
- Les cadres de l'entreprise étant souvent amenés à réaliser des déplacements professionnels, ils se sentiront d'autant plus concernés par ce scénario
- Cet univers nous permet d'aborder des situations qui ne se produisent pas ou peu au bureau.

4.1.2. Description des saynètes

- Le collaborateur est chez un partenaire
  - Le partenaire lui donne une clé USB
    - Il la branche
    - Il ne la branche pas
    - Il propose à son partenaire de prendre sa propre clé USB
  - Au moment du déjeuner, que faire de l'ordinateur portable ?
    - aisse la session non verrouillée et le poste en évidence pendant l'heure de déjeuner

- ✓ range le PC dans sa sacoche et s'assure que la salle ferme à clé avant d'aller déjeuner. Dans le cas contraire, il prend sa sacoche avec lui

- Le collaborateur est à l'hôtel
  - Il doit quitter sa chambre
    - Il laisse son PC dans sa chambre en évidence sur le bureau
    - ⛔ Il laisse son PC dans sa chambre dans le coffre-fort
    - ✓ Il prend son PC avec lui

- Le collaborateur est à l'aéroport
  - Utilisation du point d'accès Wifi non sécurisé de l'aéroport
    - ✓ active son VPN[4] et envoie des documents confidentiels par sa messagerie professionnelle
    - ✓ Il ne se connecte pas à un point d'accès wifi public
    - ✓ Il n'a pas de VPN, mais a pris soin de chiffrer les documents auparavant en prenant soin de ne mentionner aucune information confidentielle dans le corps du mail
    - ⛔ Il envoie des mails sans avoir pris soin de les chiffrer auparavant
  - Pour passer le temps à l'aéroport, il souhaite installer des logiciels sur son smartphone / tablette/ PC
    - ⛔ Oui
    - ✓ Non
  - Il perd son terminal mobile ou une mémoire amovible pendant un déplacement
    - ✓ déclare immédiatement la perte du terminal ou de la mémoire amovible au service support de son entreprise
    - ⛔ attend d'être de retour au bureau pour déclarer la perte, à moins de l'avoir retrouvé(e) dans ses bagages
  - Alors qu'il travaille dans un lieu public, pour éviter le regard insistant et de travers de sa voisine
    - ✓ Il met son filtre écran
    - ✓ Il se déplace vers un autre siège
    - ✓ Il ferme son écran
    - ⛔ Il continue de travailler comme si de rien n'était

[4] Réseau Privé Virtuel (*Virtual Private Network* ou VPN)

- Dans un lieu public, un individu demande de charger son téléphone sur le port USB de son PC
  - ⛔ Il accepte de brancher son téléphone sur son port USB
  - ✓ Il n'accepte pas

- Le collaborateur est sur un site appartenant à son entreprise, mais qui n'est pas son site habituel
  - Il souhaite se connecter au réseau
    - ✓ Il branche son PC comme s'il était à son bureau
    - ✓ Il demande un accès WIFI invité et active son VPN
    - ✓ Il n'a pas confiance, et ne se branche pas sur ce réseau
  - Dans les réseaux WIFI accessibles, il détecte un réseau ouvert appartenant à un particulier, et un réseau appartenant à l'entreprise nécessitant un mot de passe
    - ⛔ Se connecte sur le réseau ouvert du particulier
    - ✓ Il demande le mot de passe permettant de se connecter au réseau de l'entreprise, puis s'y connecte

- Le collaborateur doit partir dans un pays "à risques"
  - ✓ Il demande à son service informatique un "PC blanchi"
  - ✓ Il consulte les recommandations de l'ANSSI pour les voyageurs
  - ⛔ Il y va sans prendre de précautions particulières
  - ⛔ Il ne prend pas son matériel informatique puisqu'il se connectera depuis un cybercafé / un business center

2. Dans l'entreprise

1. Raisons du choix de cet univers

- Le choix d'un univers mettant en scène un collaborateur « type » permet d'assurer une meilleure appropriation par tous les joueurs
- Cet univers illustre les risques les plus courants, au quotidien
- Cet univers complète celui du collaborateur en mobilité.

4.2.2. Description des saynètes

- En route ou en déplacement à proximité de son entreprise, le collaborateur attend un mail important
  - ✗ Il demande à quelqu'un de lui prêter son PC pour regarder ses mails

- ✅ N'attend d'être de retour au bureau pour consulter sa messagerie
- ✅ Ne regarde pas ses mails et appelle le bureau pour se tenir au courant

- Lors d'un court déplacement, le collaborateur utilise son smartphone ou sa tablette fournie par son entreprise pour consulter ses mails
  - Via le point d'accès wifi gratuit et ouvert
    - ✅ Il lance son client VPN
      - ✅ Il ouvre son mail
      - ✅ Il ouvre son webmail sécurisé en HTTPS
    - ⛔ Il ouvre son webmail non sécurisé en HTTP
  - Via le wifi protégé par un mot de passe de son opérateur téléphonique
    - ✅ Il lance son client VPN
      - ✅ Il ouvre son mail
      - ✅ Il ouvre son webmail sécurisé en HTTPS
    - ⛔ Il ouvre son webmail non sécurisé en HTTP
  - Via son abonnement 3G
    - ⛔ Il ouvre son webmail non sécurisé en HTTP
    - ✅ Il ouvre son webmail sécurisé en HTTPS

- Le collaborateur trouve une clé USB portant le logo de l'entreprise ou un autre périphérique USB dans le parking de l'entreprise
  - ✅ Il la ramasse et l'amène au service Sécurité
  - ❌ Il la ramasse et la branche sur son PC
  - ⛔ Il la laisse

- Le collaborateur assiste à la scène suivante :
  Une personne demande à rencontrer un collaborateur absent. Elle donne alors une clé USB à l'hôtesse d'accueil, et lui demande de la brancher sur son PC afin de transmettre un document à ce collaborateur
  - ✅ Il prévient le service de sécurité
  - ✅ Il dit à l'hôtesse de ne pas brancher la clé USB sur son PC
  - ❌ Il ne fait rien

- Le collaborateur reçoit un fournisseur dans une salle de réunion et ce dernier a besoin d'une connexion Internet pour réaliser une démonstration de son produit
  - ❌ Lui permet de se connecter sur la prise réseau présente dans la salle

- ✗ Il lui donne un accès temporaire au réseau wifi de l'entreprise
- ✓ Il lui donne le SSID du réseau wifi utilisable par les visiteurs
- ✓ Il lui indique que c'est interdit

- Le collaborateur reçoit la visite de son auditeur aux comptes qui a besoin de se connecter sur le réseau de l'entreprise, pour avoir accès à la GED de la comptabilité afin de travailler sur certaines pièces comptables
  - ⛔ Il permet à l'auditeur d'utiliser son PC portable et de le connecter au réseau, car c'est un partenaire qu'il connait de longue date et auquel il fait totalement confiance
  - ⛔ Il lui permet d'utiliser une station de travail de l'entreprise (il le connecte avec son compte et son mot de passe)
  - ✓ Il appelle le support informatique pour demander un compte pour l'auditeur et lui permet d'utiliser une station de travail de l'entreprise

- Le collaborateur reçoit son neveu pour son stage de 3ème. Le neveu demande de pouvoir aller sur Internet pour consulter son Facebook (il possède un smartphone wifi)
  - ⛔ Il lui permet d'utiliser une station de travail de l'entreprise (il le connecte avec son compte et son mot de passe)
  - ⛔ Il lui donne un accès temporaire au réseau wifi qui permet d'accéder à Internet et il utilise son smartphone
  - ✓ Il lui donne le SSID du réseau wifi utilisable par les visiteurs qui permet d'accéder à Internet et il utilise son smartphone
  - ✓ Il demande au support informatique un compte et un mot de passe pour son neveu et lui indique une station de travail à partir de laquelle il pourra se connecter à Internet

- Le collaborateur est en charge d'un projet qui va nécessiter la présence d'un prestataire pendant plusieurs semaines sur le site. Ce prestataire, pour être efficace, a besoin d'utiliser son propre PC et d'avoir un accès à Internet
  - ⛔ Il lui permet de connecter son PC sur la prise réseau présente là où il travaille
  - ⛔ Il lui donne un accès temporaire au réseau wifi d'entreprise qui permet d'accéder à Internet
  - ✓ Il lui donne le SSID du réseau wifi utilisable par les visiteurs pour qu'il puisse se connecter à Internet

- ✔ appelle le support informatique pour demander un compte pour ce prestataire et lui permet d'utiliser une station de travail de l'entreprise pour se connecter à Internet

- Le collaborateur est en charge d'un projet qui va augmenter la productivité de l'entreprise de 500% (du moins c'est ce que dit le commercial) et le fournisseur qui recommande cet outil propose de venir l'installer provisoirement dans un des bureaux de l'entreprise. Il a besoin pour monter cette maquette de connecter un appareil sur le réseau
  - ⛔ Il lui permet de faire cette connexion car ce projet est suivi et approuvé par la direction générale
  - ⛔ Il débranche le câble d'un poste qui n'est pas utilisé pour lui permettre de se connecter au réseau
  - ✔ Il demande aux personnes en charge du réseau informatique de réaliser cette connexion

- Le responsable marketing du collaborateur lui demande de tester son intervention pour un prochain colloque. Il utilisera pour sa présentation une tablette wifi, une imprimante 3D wifi et un routeur wifi à brancher sur le réseau du colloque pour connecter le tout à Internet. Il doit vérifier que les appareils fonctionnent harmonieusement.
  - ⛔ Il connecte le tout sur le réseau de l'entreprise pour voir comment ça marche
  - ⛔ Il demande aux personnes en charge du réseau informatique de réaliser cette connexion sur le réseau d'entreprise
  - ✔ Il teste la configuration sur une Box indépendante du réseau de l'entreprise
  - ✔ Il se rend en avance sur le lieu de la présentation pour tester la configuration avant la présentation

3. Devant son ordinateur, à son bureau

1. Raisons du choix de cet univers

- Cet univers permet de montrer de manière lisible les fenêtres qui apparaissent sur l'écran d'un PC (vu de loin, ce serait illisible)
- Il permet également une bonne appropriation du contexte par le joueur qui se sent d'autant plus impliqué qu'il voit directement le contenu de l'écran

- Ceci est renforcé par le fait de ne pas montrer l'utilisateur : tous sont concernés par ce scénario, indépendamment de la fonction du joueur dans l'entreprise ou du contexte dans lequel il opère.

4.3.2. Description des saynètes

- On demande au collaborateur de changer son mot de passe Windows. Il choisit de mettre
  - ⛔ Son numéro de carte de crédit
  - ⛔ Le même que l'identifiant
  - ⛔ password02
  - ⛔ azertyqsdf
  - ⛔ jean-marie12031973
  - ⛔ Son mot de passe de messagerie perso qui est p2ssw0rd!
  - ✔ p2ssw0rd!
  - ✔ Au moins un chiffre, une lettre, un symbole et 8 caractères minimum

- On demande au collaborateur de changer son mot passe de l'outil de compta / ERP / ou autre outil métier. Il choisit :
  - ⛔ Le nom du département : supplychain2013
  - ⛔ Un mot de passe partagé avec l'ensemble de l'équipe
  - ⛔ Un mot de passe qu'il partage avec son *backup*
  - ✔ Un mot de passe propre qui est le même que son mot de passe Windows, à savoir p2ssw0rd!

- Pour mémoriser les mots de passe de ses applications et ses sites Web
  - ⛔ Il utilise un fichier Excel contenant ses mots de passe
  - ✘ Il utilise un fichier Excel zippé protégé par mot de passe contenant ses mots de passe
  - ✔ Mot de passe propre dans un coffre-fort à mot de passe
  - ✔ Il retient tous les mots de passe de tête

- Le collaborateur a une fenêtre d'alerte signalant que son PC est infecté
  - ✔ Il alerte le support
  - ✔ Il débranche le câble réseau
  - ⛔ Il demande à son collègue qui s'y connait

- Le collaborateur reçoit un mail « louche » (de *phishing*)
  - ❌ Il répond, ça a l'air tentant
  - ⛔ Il fait suivre à l'assistante ou aux collègues
  - ✔ Il le fait suivre à une adresse "report-spam@..."
  - ✔ Il le supprime
  - ✔ Il le signale au *helpdesk*, correspondant sécurité

- Le collaborateur reçoit une blague par mail contenant une pièce jointe
  - ⛔ Il le lit et ouvre le fichier attaché
  - ✔ Il le lit mais n'ouvre pas le fichier attaché ni ne clique sur un lien
  - ✔ Il supprime le mail

- Le collaborateur va prendre une pause café
  - ✔ Il verrouille sa session en enlevant le badge de son lecteur de carte à puce
  - ✔ Il verrouille sa session en appuyant sur « Windows + L »
  - ⛔ Il ne verrouille pas son PC car il en a juste pour quelques minutes

- Le collaborateur a besoin d'installer Adobe Acrobat ou un autre outil bureautique
  - ⛔ Il l'achète et essaie de l'installer (son collègue connait le mot de passe administrateur)
  - ⛔ Il le télécharge et essaie de l'installer
  - ✔ Il en fait la demande au support

- Le collaborateur s'apprête à quitter le bureau en fin de journée
  - ✔ Il arrête son PC
  - ✔ Il le verrouille
  - ⛔ Il le laisse se mettre en veille prolongée

- Quelqu'un demande son mot de passe au collaborateur
  - C'est un collègue
    - ⛔ Il lui donne car il est sympa
    - ⛔ Il lui donne, car c'est son chef ou sa secrétaire / son assistant
    - ✔ Il ne lui donne pas son mot de passe
  - C'est le support qui intervient physiquement
    - ✔ change son mot de passe pour "password123", et le rechangera lorsqu'ils rendront son PC

- ⛔ Il leur donne son mot de passe actuel

- C'est quelqu'un du support qui l'appelle par téléphone et lui demande son mot de passe
  - ✔ leur demande d'envoyer un email pour prouver qu'il s'agit bien du support ou leur propose de les rappeler lui-même
  - ⛔ Il leur donne son mot de passe actuel

4. Au domicile

1. Raisons du choix de cet univers

- Cet univers permet notamment d'illustrer les risques liés à l'apport de technologies numériques au travail par chaque collaborateur (« IT *Consumerization* ou BYOD – *Bring Your Own Device* ») ainsi que ceux ayant trait au travail à domicile
- Il montre en particulier les risques liés :
  - Au mélange de la vie privée et de la vie professionnelle des collaborateurs
  - A la difficulté de la valorisation de l'expérience professionnelle d'un collaborateur tout en assurant la confidentialité de ses travaux pour l'entreprise
  - A l'utilisation courante des réseaux sociaux dans l'entreprise
- Cet univers permet également une bonne appropriation du sujet par les joueurs, qui sont fréquemment confrontés à ces problématiques (chaque soir et chaque week-end!)

4.4.2. Description des saynètes

- Sur l'ordinateur portable de la société, le collaborateur reçoit une invitation à une conférence téléphonique sur un outil en ligne pour traiter une question professionnelle
  - ⛔ Il clique sur le lien, installe et ouvre le logiciel. (Le firewall se déclenche, un message d'alerte apparaît et bloque l'ouverture)
  - ⛔ Le collaborateur tente de désactiver le firewall, y parvient, le programme malveillant prend le contrôle de l'ordinateur qui se bloque infecté
  - ✔ Le collaborateur arrête la procédure et propose de passer par le téléphone professionnel, moins pratique mais autorisé
  - ✔ L'employé propose de passer par une solution de messagerie instantanée autorisée par l'entreprise

- Un partenaire demande au collaborateur de lui transmettre un fichier de travail stratégique pour qu'ils travaillent ensemble sur ce fichier
  - ⛔ collaborateur propose de déposer le fichier sur un DropBox et demande au partenaire si ce dernier détient un compte sur lequel il pourrait déposer le fichier.
  - ✓ L'employé suit la procédure de l'entreprise et dépose le fichier chiffré sur une version entreprise de "Dropbox"
    - ✓ Il donne le mot de passe par téléphone.
    - ✓ Il donne le mot de passe par un mail séparé et crypté

- Le partenaire propose au collaborateur de continuer à travailler chacun de son côté sur la future version du fichier
  - ✗ Il place son fichier dans Google Drive et le partage avec son partenaire
  - ⛔ Il envoie le fichier par messagerie personnelle et propose des allers-retours pour les mises à jour
  - ✓ Il chiffre puis envoie le fichier par messagerie personnelle et propose des allers-retours du document chiffré pour les mises à jour
  - ✓ Il utilise sa messagerie d'entreprise qui dispose d'une fonction de chiffrement pour les tiers partenaires

- La fille du collaborateur souhaite utiliser son PC professionnel à son domicile
  - ✓ Il le lui interdit
  - ⛔ Il lui laisse faire ce qu'elle veut
  - ⛔ Il a oublié de verrouiller son PC, elle peut y accéder librement
  - ✓ L'employé déverrouille son PC et lui laisse l'utiliser à condition qu'elle respecte quelques règles :
    - ✓ Elle n'installe aucun logiciel
    - ✓ Elle ne télécharge rien
    - ✓ Elle n'utilise pas sa messagerie professionnelle
    - ✓ Elle n'utilise pas les réseaux sociaux
    - ✓ Elle n'utilise pas de messagerie instantanée
    - ✓ Elle ne regarde aucun film en *streaming*
    - ✗ Elle peut installer les logiciels qu'elle veut du moment qu'elle les supprime ensuite
    - ✗ Elle fait ce qu'elle veut du moment qu'elle coupe le son

- ❌ Elle peut utiliser sa messagerie professionnelle du moment qu'elle n'écrit qu'à ses amis en précisant qu'elle est l'auteur des messages
- ❌ Parmi les réseaux sociaux, elle ne va que sur Facebook

- Le collaborateur met son CV à jour et enrichit sa fiche LinkedIn/Viadeo
  - ❌ y précise des détails sensibles mais professionnellement valorisants sur des projets qu'il a menés
  - ✓ Il limite les détails sur les projets qu'il a menés

- Après avoir travaillé sur sa présentation du lendemain depuis sa tablette
  - ❌ Il l'ajoute à son Google Drive pour y accéder le lendemain depuis son PC professionnel
  - ✓ Il le chiffre et l'envoie à son adresse mail professionnelle depuis sa messagerie personnelle
  - ✓ Il dépose sa présentation sur une clé USB chiffrée qu'il prendra avec lui le lendemain

5. FICHES CONSEIL : BONNES PRATIQUES ET RISQUES COUVERTS

Destinées à apparaître sous forme de « *pop-up* » au cours du jeu, les fiches Conseil regroupent quelques bonnes pratiques essentielles.

En mobilité

Bonnes pratiques

- ✓ Gardez votre poste de travail (ou autres *devices*) avec vous quel que soit le lieu où vous vous trouvez (ne faites pas confiance aux coffres-forts des hôtels par exemple)

Risques couverts

- ➧ Vol d'information

Dans un lieu public

Bonnes pratiques

- ✓ Ne consultez pas de données à caractère confidentiel
- ✓ N'abordez pas de sujets sensibles
- ✓ Utilisez des filtres de confidentialité sur vos écrans
- ✓ Si vous trouvez des périphériques USB, remettez-les à votre service sécurité

Risques couverts

- ➧ Vol d'information

Déplacement dans un pays « à risques»

Bonnes pratiques

- ✓ Prenez connaissance des recommandations mises à disposition par l'ANSSI

Risques couverts

- ➧ Vol d'information

Collaboration avec un partenaire

Bonnes pratiques

- ✓ Ne connectez que des périphériques de confiance à votre système
- ✓ N'utilisez que des plateformes sécurisées d'échange de fichiers, validées par votre entreprise, pour collaborer avec des tiers
- ✓ Ne transférez pas de documents professionnels vers votre messagerie personnelle

Risques couverts

- ➧ Vol d'information et infection virale

Connexion de visiteurs

Bonnes pratiques

- ✓ Ne connectez jamais une machine n'appartenant pas à votre entreprise directement au réseau de votre entreprise
- ✓ Proposez à vos interlocuteurs un accès au Wi-Fi Invités (s'il existe)

Risques couverts

- Vol d'information et infection virale

En quittant son poste de travail

Bonnes pratiques

- ✓ Verrouillez votre session de travail, fermez votre bureau à clef ou attachez votre poste de travail

Risques couverts

- Fraude et vol d'information

Installation de nouveaux logiciels

Bonnes pratiques

- ✓ Pour installer un logiciel sur votre poste de travail, contactez votre support utilisateur

Risques couverts

- Infection virale, conformité (licences logicielles) et instabilité du matériel informatique et des logiciels

Mise à jour des postes de travail

Bonnes pratiques

- ✓ Lorsque vous y êtes invité par votre système, redémarrez votre poste de travail (*a minima* une fois tous les quinze jours)

Risques couverts

- Infection de l'ordinateur et pénétration des systèmes de l'entreprise.

Mots de passe

Bonnes pratiques

- ✓ Utilisez un mot de passe complexe
- ✓ Utilisez un mot de passe différent pour chaque outil nécessitant une authentification (site web, ordinateur, sessions utilisateurs…)

- ✓ Ne partagez pas votre mot de passe avec un tiers (famille, collègue, etc.)

Risques couverts

- Usurpation d'identité

Détection d'anomalie sur les postes de travail

Bonnes pratiques

- ✓ En cas de d'activité suspecte sur votre ordinateur, contactez votre support utilisateur

Risques couverts

- Infection virale et vol d'information

Courriels suspects

Bonnes pratiques

- ✓ Supprimez tout mail suspicieux
- ✓ En parallèle, remontez cet incident au support utilisateur (remarque : le support peut demander à disposer du mail)

Risques couverts

- Infection virale et vol d'information

Bon usage des systèmes d'information professionnels

Bonnes pratiques

- ✓ Le matériel professionnel (poste de travail, portable, tablette, etc.) est uniquement à l'usage des collaborateurs de l'entreprise

Risques couverts

- Usurpation d'identité

6. PROCHAINES ÉTAPES

Aujourd'hui, un grand nombre d'entreprises sont convaincues par le bien-fondé de l'utilisation d'un *Serious Game* pour la sensibilisation à la sécurité numérique, et sont prêtes à continuer l'aventure.

Il s'agit maintenant, en partenariat avec le Comité Richelieu, de déterminer les parties prenantes qui seront impliquées dans la réalisation du *Serious Game* : État, financeurs publics et privés, éditeur de logiciel... L'objectif final est de pouvoir diffuser cet outil auprès des entreprises membres du CIGREF, mais également d'avoir la possibilité d'en faire un vecteur de communication sur les risques numériques auprès de l'ensemble des entreprises françaises (petites et grosses), et du grand public.

ANNEXE : PRÉCONISATIONS TECHNIQUES

Hébergement

Pour faciliter son déploiement, le *Serious Game* devra être accessible en mode « *Software As A Service* » (SaaS). Il pourra être hébergé soit chez un tiers de confiance, soit directement sur les infrastructures de l'entreprise.

Compatibilité et optimisation

Le *Serious Game* pourra s'intégrer aux intranets des entreprises, afin d'en faciliter l'accès au personnel de l'entreprise.

Il sera accessible sur le plus grand nombre possible de navigateurs et avec un minimum de pré requis techniques (*plugins* additionnels / matériels audio ou vidéo spécifiques, etc.).

Il est nécessaire que le jeu soit accessible facilement à l'ensemble des collaborateurs quels que soient les terminaux utilisés (poste de travail, tablette, etc.), en mobilité ou au bureau.

Qualité et pérennité

Les langages de programmation et outils utilisés pour les développements seront sélectionnés parmi les standards du marché, utilisés conformément à l'état de l'art.

Performance

Une attention toute particulière sera apportée aux performances (temps de réponse, nombre de joueur simultanés, ...).

Sécurité

Le jeu devra être développé conformément aux meilleures pratiques en matière de sécurité des systèmes d'information (prévention des attaques par déni de service, des tentatives

d'intrusion ou de défiguration, etc.). En particulier les recommandations de l'ANSSI[5] et de l'OWASP[6] seront prises en compte.

Le jeu devra authentifier les joueurs conformément aux politiques de sécurité des entreprises, cette authentification devra être protégée (https).

Administration

Le jeu devra permettre un chargement par lot des comptes utilisateurs pour permettre aux entreprises de le déployer aisément.

Le jeu devra permettre aux participants de modifier leur code d'accès, leurs informations personnelles, etc.

Cette interface d'administration devra être disponible en plusieurs langues (*a minima* français / anglais).

Déclarations réglementaires

Les entreprises seront responsables de réaliser les déclarations réglementaires nécessaires (notamment auprès de la CNIL, G29 et des organismes étrangers similaires).

[5] http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-de-l-externalisation/externalisation-et-securite-des-systemes-d-information-un-guide-pour-maitriser.html

[6] http://www.owasp.org

BIBLIOGRAPHIE

- « *Nécessaire réforme de la gouvernance de l'Internet* », commission des affaires étrangères du Sénat, **M. Gaëtan Gorce**, rapporteur (Sénat, n° 102, 2014-2015,19 novembre 2014).

- « *Nécessaire réforme de la gouvernance de l'Internet* », commission des affaires européennes du Sénat, **Mme Colette Mélot**, rapporteur (Sénat, n° 81, 2014-2015, 4 novembre 2014).

- Proposition de résolution européenne sur la « *Nécessaire réforme de la gouvernance de l'Internet* » de **Mme Catherine Morin-Desailly et M. Gaëtan Gorce**, sénateurs (Sénat, n° 44, 2014-2015, 22 octobre 2014).

- « *Jules Ferry 3.0. Bâtir une économie créative et juste dans un monde numérique* ». **Conseil national du numérique**, octobre 2014.

- « *La nouvelle France industrielle. Présentation des feuilles de route des 34 plans de la nouvelle France industrielle* », septembre 2014.

- « *Étude annuelle 2014. Le numérique et les droits fondamentaux* ». **Conseil d'État**, septembre 2014.

- « *Supprimer le recours aux machines à voter pour les élections générales* », proposition de loi présentée par **M. Philippe Kaltenbach**, sénateur (Sénat, n° 763, 2013-2014, 22 juillet 2014).

- « *Politique de sécurité des systèmes d'information de l'État* », **Instruction du Premier ministre. ANSSI**, juillet 2014.

- "*Big Data in Business*" *POSTNOTE. Houses of Parliament.* ***Parliamentary Office of Science & Technology****. Number 469. July 2014.*

- « *Accélération du passage à la norme IPv6* » proposition de loi présentée par **Mme Laure de La Raudière et plusieurs de ses collègues**, députés (Assemblée nationale, quatorzième législature, n° 2140, 16 juillet 2014).

- « *L'Europe au secours de l'Internet : démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique industrielle européenne* », rapport d'information du Sénat, mission commune d'information « *Nouveau rôle et nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'Internet* » (tome I : rapport, tome II : comptes rendus des auditions), **M. Gaëtan Gorce**, président, **Mme Catherine Morin-Desailly**, rapporteur, (Sénat, n° 696, 2013-2014, 8 juillet 2014).

- « *Amélioration du matériel informatique dans les écoles élémentaires, sécurisation de l'accès à Internet et protection des élèves* », proposition de loi, présentée par **M. Denis Jacquat**, député (Assemblée nationale, quatorzième législature, n° 2087, 2 juillet 2014).

- « *La direction de l'information légale et administrative (DILA) face aux défis du numérique : les conditions de la réussite d'une mutation* », rapport d'information, commission des finances du Sénat, **M. Philippe Dominati**, rapporteur (Sénat, n° 670, 2013-2014, 1er juillet 2014).

- « *Le numérique, le renseignement et la vie privée : de nouveaux défis pour le droit* ». *Actes de la journée d'étude du 22 mai 2004* », rapport d'information, commission des lois du Sénat, **M. Jean-Pierre Sueur**, rapporteur (Sénat, n° 663, 2013-2014, 27 juin 2014).

- « *Rendre obligatoire l'enseignement du codage informatique à l'école* », proposition de loi présentée par **Mme Laure de La Raudière** et **M. Bruno Le Maire et plusieurs de leurs collègues**, députés (Assemblée nationale, quatorzième législature, n° 2022, 11 juin 2014).

- « *Proclamer Edward Snowden citoyen d'honneur de la République française et lui accorder l'asile politique* », proposition de résolution de **M. Yves Jégo**, député (Assemblée nationale, quatorzième législature, n° 2008, 10 juin 2014).

- « *Refonder le droit à l'information publique à l'heure du numérique : un enjeu citoyen, une opportunité stratégique* » (Tome I : Rapport et Tome II : Audition et contributions écrites), rapport d'information, mission commune d'information sur « *L'accès aux documents administratifs et aux données publiques* », **M. Jean-Jacques Hyest**, président et **Mme Corinne Bouchoux**, rapporteur (Sénat, n° 589, 2013-2014, 5 juin 2014).

- « *Pour une véritable politique publique du renseignement* », **Pr Sébastien-Yves Laurent,** Institut Montaigne, Étude (juin 2014).

- « *Science, innovation et numérique : les sociétés en question* », **IHEST**, travaux du cycle national 2013-2014.

- « *L'homologation de sécurité en neuf étapes simples* ». Version 2.0. **ANSSI**. Juin 2014.

- Proposition de résolution européenne sur le « *Projet d'accord de libre-échange entre les États-Unis d'Amérique et l'Union européenne* », commission des affaires étrangères de l'Assemblée nationale, **M. André Chassaigne**, rapporteur (quatorzième législature, n° 1938, 14 mai 2014) et, en annexe au rapport, texte de la commission (Assemblée nationale, quatorzième législature, n° 1938, 14 mai 2014).

- « *Agir pour une France numérique : De l'audace, encore de l'audace, toujours de l'audace…* », rapport d'information sur « *Le développement de l'économie numérique française* », commission des affaires économiques de l'Assemblé nationale, **Mmes Corinne Erhel** et **Laure de La Raudière**, rapporteurs (Assemblée nationale, quatorzième législature, n° 1936, 14 mai 2014).

- Proposition de résolution européenne sur le « *Projet d'accord de libre-échange entre l'Union européenne et les États-Unis d'Amérique* », commission des affaires européennes de l'Assemblée nationale, **M**. **André Chassaigne**, rapporteur (quatorzième législature, n° 1930, 13 mai 2014) et, en annexe au rapport, texte de la commission des affaires européennes (Assemblée nationale, quatorzième législature, n° 1930, 13 mai 2014).

- « *Partenariat transatlantique de commerce et d'investissement : faire du volet numérique un atout pour la négociation* ». **Conseil national du numérique**, mai 2014.

- « *Approbation de l'accord relatif à l'hébergement du centre de sécurité Galileo* », commission des affaires étrangères de l'Assemblée nationale, **Mme Pascale Boistard**, rapporteur (Assemblée nationale, quatorzième législature, n° 1915, 30 avril 2014).

- « *La protection des données personnelles dans l'*open data *: une exigence et une opportunité* » rapport d'information, commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale du Sénat, sur « *L'*open data *et la protection de la vie privée* », **MM. Gaëtan Gorce** et **François Pillet**, rapporteurs (Sénat, n° 469, 2013-2014, 16 avril 2014).

- Proposition de résolution européenne sur « *Le projet d'accord de libre-échange entre l'Union Européenne et les États-Unis d'Amérique* », commission des affaires européennes de l'Assemblée nationale, de **M. André Chassaigne et plusieurs de ses collègues**, députés (Assemblée nationale, quatorzième législature, n° 1876, 10 avril 2014).

- « *Vote électronique : préserver la confiance des électeurs* », rapport d'information, commission des lois du Sénat, **MM. Alain Anziani** et **Antoine Lefèvre**, rapporteurs (Sénat, n° 445, 2013-2014, 9 avril 2014).

- "*ISTR. Internet Security Threat Report*". **SYMANTEC**. 2013 *Trends, Volume 19, published April 2014.*

- "*Social Media and Big Data*" *POSTNOTE. Houses of Parliament.* ***Parliamentary Office of Science & Technology****. Number 460. March 2014.*

- « *Panorama de la cybercriminalité, année 2013* ». Les synthèses du **CLUSIF**. Janvier 2014.

- « *DSI, préparez-vous à devenir* Cloud broker *!* » Observatoire de la transformation des entreprises. Les synthèses Solucom n° 48. **Solucom management et IT consulting**. Janvier 2014.

- « *Science et société : les normes en question* ». **IHEST**, Éditions Actes Sud, 2014.

- « *Menaces informatiques et pratiques de sécurité en France* ». Edition 2014. Club de la sécurité de l'information français. **CLUSIF**.

- « *La souveraineté des États à l'épreuve de l'Internet* », **Mme Pauline Türk**, maître de conférences, Université de Lille 2 ; Revue du Droit Public. N° 6-2013.

- « *Histoires et cultures du Libre. Des logiciels partagés aux licences échangées.* ». Collectif sous la direction de Camille Paloque- Berges et Christophe Massuti. Framabook, Cube Inno, **INRIA** Inventeurs du monde numérique. 2013.

- « *Autoriser l'usage de la géolocalisation dans le cadre des enquêtes préliminaires et de flagrance* » proposition de loi présentée par **M. François Pillet et plusieurs de ses collègues**, sénateurs (Sénat, n° 236, 2013-2014, 17 décembre 2013).

- « *Les défis du cyberespace* ». Revue de la **gendarmerie nationale**. N° 248. Décembre 2013.

- « *Sûreté et risques numériques. Scenario d'un* serious game **». CIGREF**, octobre 2013.

- « *Un principe et sept ambitions pour l'innovation* ». **Commission Innovation 2013,** rapport au Président de la République, octobre 2013.

- Proposition de résolution de l'Union européenne sur « *La stratégie numérique de l'Union européenne* », commission des affaires économiques de l'Assemblée nationale, **Mme Corinne Erhel**, rapporteur (Assemblée nationale, quatorzième législature, n° 1458, 15 octobre 2013).

- Proposition de résolution de l'Union européenne sur « *La stratégie numérique de l'Union européenne* », commission des affaires européennes de l'Assemblée nationale, **M. Hervé Gaymard** et **Mme Axelle Lemaire** rapporteurs (Assemblée nationale, quatorzième législature, n° 1409, 8 octobre 2013).

- « *L'humanité augmentée. L'administration numérique du monde* » **M. Éric Sadin.** Éditions l'échappée ; collection « Pour en finir avec ». 2013.

- « *Le risque numérique : en prendre conscience pour mieux le maîtriser ? Compte rendu de l'audition publique du 21 février 2013 et de la présentation des conclusions le 26 juin 2013.* » Les rapports de l'OPECST. **M. Bruno Sido**, sénateur et **M. Jean-Yves Le Déaut**, député, rapporteurs (Assemblée nationale, quatorzième législature, n° 1221, 3 juillet 2013 et Sénat, n° 721, 2012-2013, 3 juillet 2013).

- « *Guide d'hygiène informatique* ». Agence nationale de la sécurité des systèmes d'information (**ANSSI**). Version de juin 2013.

- « *L'enseignement de l'informatique en France. Il est urgent de ne plus attendre.* » **Académie des sciences**. Mai 2013.

- « *L'Union européenne, colonie du monde numérique ?* », rapport d'information, commission des affaires européennes du Sénat, **Mme Catherine Morin-Desailly**, rapporteur (Sénat, n° 443, 2012-2013, 20 mars 2013).

- « *L'éthique des* hackers », **M. Steven Levy**. Éditions Globe, mars 2013 (1984, en anglais).

- « *Cybersociété – Entre espoirs et risques* » **Mme Myriam Quéméner.** Éditions L'Harmattan, collection « Justice & Démocratie ». 2013.

- Livre blanc sur la défense et la sécurité nationale, 2013.

- « *Cybersecurity policy making at a turning point. Analysing a new generation of national cybersecurity strategies for the Internet economy* », **OECD**. 2012.

- « *L'emprise numérique. Comment Internet et les nouvelles technologies ont colonisé nos vies*. » **M. Cédric Biagini**. Éditions l'échappée. Collection « Pour en finir avec ». 2012.

- « *L'observatoire de la filière de la confiance numérique en France* ». **Alliance pour la confiance numérique (ACN)**, novembre 2012.

- Directive européenne sur la politique de cybersécurité, juillet 2012.

- Directive européenne sur la politique industrielle de sécurité, juillet 2012.

- « *La cyberdéfense : un enjeu mondial, une priorité nationale* » rapport d'information, commission des affaires étrangères, de la défense et des forces armées du Sénat, **M**. **Jean-Marie Bockel**, rapporteur (Sénat, n° 681, 2011-2012, 18 juillet 2012).

- « *Gouvernance de l'Internet. Stratégie du Conseil de l'Europe 2012-2015 telle qu'adoptée par le Comité des Ministres le 14 mars 2012* ». **Conseil de l'Europe**. 14 mars 2012.

- « *Dénis de service – Prévention et réaction* », note d'information du CERTA, janvier 2012.

- « *Steve Jobs. La biographie du génie qui a changé le monde* », **M. Walter Isaacson**. Éditions JC Lattès. Décembre 2011.

- Accord de coopération et de coordination technique sur la cyberdéfense entre la France et l'Alliance atlantique, 30 septembre 2011.

- **G8** : Déclaration de Deauville des 26 et 27 mai 2011.

- « *La neutralité de l'internet* », rapport d'information, commission des affaires économiques de l'Assemblée nationale, **Mme Corinne Erhel**, présidente, et **Mme Laure de La Raudière**, rapporteur (Assemblée nationale, treizième législature, n° 3336, 13 avril 2011).

- « *Les progrès de l'informatique et de la télématique et la question de la sécurité internationale* », résolution 65/41 de l'**Assemblée générale des Nations-Unies** du 8 décembre 2010.

- Rapport du groupe d'experts intergouvernementaux de l'**ONU**, 2010.

- « *La protection des données, recueil des textes du Conseil de l'Europe* », Direction générale des droits de l'Homme et des affaires juridiques, novembre 2010.

- « *A Digital Agenda 2010-2020 for Europe : Every European Digital* », *communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, **Mme Neelie Kroes**, COM (2010) 245 final, 19.5.2010).

- « *CYBERDROIT : le droit à l'épreuve de l'Internet* » *par* **Me Christiane Féral-Schuhl,** avocat au Barreau de Paris (2011-2012 Praxis Dalloz, sixième édition 2010).

- « *Cyberdéfense : un nouvel enjeu de sécurité nationale* » rapport d'information, commission des affaires étrangères, de la défense et des forces armées du Sénat, **M. Roger Romani**, rapporteur (n° 449 -2007-2008, 8 juillet 2008).

- Livre blanc sur la défense et la sécurité nationale, 2008.

- « *Recommandations sur la protection des infrastructures d'information critiques* ». **OCDE**, 30 juin 2008.

- « *Sécurité et défense des infrastructures stratégiques de l'économie* ». **Centre des Hautes Études de l'Armement (CHEAr)**, rapport de comité, session 2006-2007.

- « *La sécurité des systèmes d'information : un enjeu majeur pour la France* », rapport au Premier ministre, **M. Pierre Lasbordes**, député, 2006.

- « *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information* ». **OCDE**. 2002.

- Convention de Budapest sur la cybercriminalité, **Conseil de l'Europe** (STE n° 185 du 23 novembre 2001).

GLOSSAIRE

Certaines des définitions extraites du glossaire figurant sur le site de l'ANSSI ont été résumées.

***3GPP* :** *Third Generation Partnership Project*. Organisme de standardisation en télécommunications qui produit et publie les spécifications techniques pour les réseaux mobiles de 3e (3G) et 4e générations (4G).

Accaparement de nom de domaine (*Cybersquatting, Domain Name Grabbing*) : action malveillante qui consiste à faire enregistrer un nom de domaine dans le but de **bloquer toute attribution ultérieure de ce nom, éventuellement au détriment de titulaires plus naturels ou plus légitimes**.

Remarques : l'objectif peut être d'obtenir un avantage financier en échange de la rétrocession du nom ainsi détourné. Cette pratique est fréquente pour certains noms de domaine comme .net, .com, ou .org.

Voir : Chantage, Faute de frappe opportuniste. (ANSSI)

Accès sans fil (*Wi-Fi*) : technologie de réseau informatique sans fil pouvant fonctionner pour construire un réseau interne et accéder à Internet à haut débit. Cette technologie est basée sur la norme IEEE 802.11 (*ISO*/CEI 8802-11).

Remarque : **l'accès sans fil rend nécessaire l'élaboration d'une politique de sécurité** dans les entreprises et chez les particuliers, par le biais de la norme 802.11i (*WPA2* ou *Wi-Fi Protected Access*) notamment. (ANSSI)

Address munging *: voir* Moisson de courriels.

Adresse *IP* *: voir* Protocole *IP*.

Adwords *:* lorsqu'un internaute utilise *Google*, deux listes de résultats sont affichées : les résultats du moteur de recherche au centre de la page et, sur le côté droit, les résultats provenant de la régie publicitaire de *Google* nommée *AdWords* qui commercialise l'espace publicitaire du moteur de recherche auprès des annonceurs souhaitant apparaître suite à une recherche effectuée par un internaute.

Algorithme : un algorithme constitue une **suite itérative d'opérations menées en vue de résoudre un problème donné**. L'algorithmique est l'ensemble des activités logiques qui relèvent des algorithmes. Cette discipline est au cœur de la conception des programmes informatiques puisque un programme est composé de plusieurs

algorithmes. La conception d'un algorithme prend en compte l'ensemble des règles et des techniques nécessaires à l'automatisation des fonctions qu'assurera le logiciel.

Antivirus : programme informatique capable de déceler et de détruire des programmes malveillants (virus ou autres).

Applications : programme ou ensemble de programmes destiné à aider l'utilisateur d'un ordinateur pour le traitement d'une tâche précise (traitement de texte, tableur, comptabilité, système d'information, etc.).

***APT* (*Adverse Persistent Threat*)** : le terme *APT* est un terme générique qui regroupe l'ensemble des **attaques informatiques complexes et ciblées**.

Authentification/identification : l'authentification a pour but de vérifier l'identité informatique dont une entité se réclame. Généralement, l'authentification est précédée d'une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté. En résumé, **s'identifier c'est communiquer son identité, s'authentifier c'est apporter la preuve de son identité**.

Voir : Mot de passe. (ANSSI)

Autocomplétion : l'autocomplétion suggère à l'utilisateur des compléments de sa saisie ; c'est un **système d'« aide à la saisie »** utilisé régulièrement dans les applications de tous les jours : client de messagerie, navigateur *Web*, moteur de recherche, etc.

AVEC (« *Apportez vos équipements personnels de communication* ») *: voir BYOD.*

Balayage de ports (*Port scanning*) : technique qui consiste à **envoyer des paquets de données sur les différents ports d'une machine, puis à en déduire la disponibilité de ces ports en fonction de la réponse retournée**, si elle existe.

Remarque : Cette technique peut être utilisée pour découvrir les services fonctionnant sur la machine, en faisant une extrapolation entre les ports vus en l'état ouvert et les services fonctionnant traditionnellement avec ce port.

Les paquets de données peuvent être envoyés sur les ports linéairement (l'un à la suite de l'autre) ou bien de manière plus discrète, en modifiant les temps d'envoi des paquets, en les envoyant dans un ordre aléatoire ou encore à partir de plusieurs adresses *IPs*.

Voir : Code malveillant, Porte dérobée, Test d'intrusion. (ANSSI)

***Big data** : voir* Données massives**.**

***Bit* (*Binary digit*)** : **information binaire composée de 0 et de 1 ; seule information comprise par un ordinateur**.

Bitcoin : (de l'anglais « *bit* » : unité d'information binaire et « *coin* » : pièce de monnaie) ce terme désigne à la fois le système de paiement « pair à pair » sur l'Internet (*Bitcoin*) et la monnaie qu'il utilise (*bitcoin*). Le principe du *bitcoin* repose sur un système en réseau détenant une liste publique de toutes les transactions. Cette liste réputée infalsifiable grâce à l'utilisation de signatures cryptographiques est tenue à jour au fur et à mesure des échanges (ventes/achats) exprimés en *bitcoins*. De cette façon, un *bitcoin* constitue une monnaie d'échange cryptographique.

Bluetooth *:* sous le nom *Bluetooth* se cache la **norme 802.15.1** qui permet des **communications radio à courte portée** donc sans fil. *Bluetooth* ou « La dent bleue » provient du nom d'un ancien roi viking. Il existe plusieurs versions, dont les plus répandues sont actuellement v1.2 (débit théorique de 1 Mbit/s) et v2.0 (débit théorique de 3 Mbit/s).

Voir : Accès sans fil et *Wi-Fi*. (ANSSI)

Bombardement de courriels (*Mail bombing*) : envoi d'une grande quantité de courriels à un destinataire unique dans une **intention malveillante**.

Remarque : forme particulière de déni de service contre les systèmes de courriers électroniques.

Voir : Courriel, Déni de service, Pourriel. (ANSSI)

Bombe programmée, bombe logique (*Logic bomb*) : **logiciel malveillant** conçu pour causer des dommages à un système informatique et qui est déclenché lorsque certaines conditions sont réunies. (ANSSI)

Remarque : certains virus contiennent une fonction de bombe logique : déclenchement à date fixe ou quand une certaine adresse est affichée, etc.

Botnet *: voir* Réseau de machines zombies.

Broadcast *: voir* Diffusion générale.

Bring Your Own Device : cf. *BYOD.*

***BYOD* (« *Bring Your Own device* » ou « Apportez vos appareils personnels ») :** désigne **l'utilisation d'équipements personnels** (téléphone, ordinateur portable, tablette électronique…) **dans un contexte professionnel** soit pour accéder aux

informations et applications de l'entreprise personnelles lors des activités professionnelles soit pour accéder aux informations et applications de l'entreprise depuis ses équipements personnels.

Voir : AVEC.

Canal caché (*Covert Channel*) : canal de communication qui permet à un processus malveillant de **transférer des informations d'une manière dissimulée**. Le canal caché assure une communication par l'exploitation d'un mécanisme qui n'est pas censé servir à la communication.

Remarque : les canaux cachés sont l'objet de nombreux travaux de recherche, tant pour les créer que pour les détecter.

Voir aussi : Pare-feu, Réseau de machines zombies. (ANSSI)

Canular (*Hoax*) : **information**, vraie ou fausse, souvent transmise par messagerie électronique ou dans un forum, et **incitant les destinataires à effectuer des opérations ou à prendre des initiatives, souvent dommageables**.

Remarque : il peut s'agir d'une fausse alerte aux virus, de chaîne de solidarité, pétitions, promesse de cadeaux, etc. Quelques canulars fréquents sont répertoriés sur des sites spécialisés comme « *Hoaxbuster* » ou « *Hoaxkiller* ».

Voir : Courriel, Pourriel. (ANSSI)

Capteur clavier, enregistreur de frappes (*Keylogger, keystroke logger*) : logiciel ou matériel employé par un utilisateur malveillant pour **capturer à son insu ce qu'une personne frappe au clavier**.

Remarque : cette technique permet de voler efficacement les mots de passe, les données bancaires, les messages électroniques, etc.

Voir : Cheval de Troie, Code malveillant, Espiogiciel, Logiciel espion. (ANSSI)

Centre de sécurité opérationnelle : voir *SOC*.

Certificat numérique ou électronique ou de **clé publique** : **signature numérique** mettant en œuvre un processus pour certifier qu'une information n'a pu être émise que par la personne habilitée à l'émettre et qu'elle ne pourra être lue que par la personne habilitée à sa lecture. Pour ce faire, le système élabore un lien cryptographique réputé infalsifiable à l'aide d'un **système de clé publique et de clé privée**. Au sein de ce système, chaque acteur, l'émetteur et le récepteur, possède une paire de clé privée/clé publique. **La clé privée ne doit jamais être révélée** ; **la clé publique est diffusée**.

Chantage (*Ransomware*) : **forme d'extorsion imposée par un code malveillant à un utilisateur du système**. Si ce dernier refuse de payer ou d'effectuer une tâche imposée, le service auquel il veut accéder lui est refusé par le code malveillant.

Remarque : un code malveillant peut chiffrer des fichiers et empêcher alors l'utilisateur d'y accéder. Ce dernier reçoit des indications de paiement (ou autre forme de chantage) afin de pouvoir récupérer les fichiers inutilisables en l'état. Céder au chantage ne garantit pas la récupération des fichiers.

Voir : Code malveillant, Ingénierie sociale. (ANSSI)

Cheval de Troie (*Trojan Horse*) : programme informatique dont **l'apparente fonction utile** dissimule une **fonction cachée et potentiellement malveillante**.

Remarque : la fonction cachée exploite parfois les autorisations légitimes d'une entité du système qui invoque ce programme. Elle peut, par exemple, permettre la collecte frauduleuse, la falsification ou la destruction de données.

Voir : Porte dérobée. (ANSSI)

Chiffrement : transformation cryptographique de données produisant un **cryptogramme**. (ANSSI)

Clonage de serveur *DNS* (*DNS pharming*) : **activité malveillante** visant à modifier un serveur *DNS* (serveur de noms de domaine), dans le but de **rediriger un nom de domaine vers une adresse *IP* différente de l'adresse légitime**. En croyant aller sur un site connu, **l'internaute navigue en réalité sur un site factice**.

Remarque : le trafic envoyé au domaine souhaité (organisme bancaire, messagerie électronique, etc.) peut être capturé par un utilisateur malveillant, qui, par exemple, a déjà copié des pages du domaine visé à l'adresse nouvellement indiquée par le *DNS*. La personne qui se connecte au domaine risque alors d'entrer des informations confidentielles sur le site factice, même si elle a pris la précaution de mentionner l'adresse correcte.

Voir : Hameçonnage. (ANSSI)

Code confidentiel d'une carte bancaire : le code à quatre chiffres associé à une carte bancaire permet de valider un acte de paiement ou de retrait d'argent sur un distributeur de billets. **Il équivaut à la signature du porteur** et donc à l'engagement du porteur lors de l'acte d'achat. Le code est rigoureusement personnel et ne doit pas être communiqué à des tiers même au sein de la famille. Il est fortement déconseillé de réutiliser le code de la carte pour d'autres codes d'accès comme celui d'un digicode d'une porte d'entrée ou du code de déverrouillage d'un téléphone portable. (ANSSI)

Code d'exploitation (*Exploit*) : tout ou partie d'un programme permettant d'**utiliser une vulnérabilité ou un ensemble de vulnérabilités d'un logiciel** (du système ou d'une application) **à des fins malveillantes**.

Remarque : les objectifs malveillants consistent souvent en une intrusion, une élévation de privilèges ou un déni de service. L'exploitation peut se faire directement à partir du système ciblé si l'utilisateur malveillant possède un accès physique (*local exploit*), ou à distance s'il s'y connecte (*remote exploit*).

Voir : Code malveillant, Déni de service, Élévation de privilège, Vulnérabilité. (ANSSI)

Code malveillant, logiciel malveillant (*Malicious software*, *malware*) : **tout programme développé dans le but de nuire** à ou au moyen d'un système informatique ou d'un réseau.

Remarque : les virus ou les vers sont deux types de codes malveillants connus.

Voir : Chantage, Cheval de Troie, Élévation de privilège, Outil de dissimulation d'activité, Ver, Virus, Vulnérabilité. (ANSSI)

Coffre-fort : désigne le **stockage sécurisé de données dans un nuage numérique spécialisé** qui reprend l'image du coffre-fort réel.

Confidentialité : propriété d'une information qui n'est ni disponible ni divulguée aux personnes, entités ou processus non autorisés. (ANSSI)

Contournement de la politique de sécurité : toute action ayant pour conséquence la mise en échec des règles ou des mécanismes de sécurité mis en place. (ANSSI)

Cookie *:* fichier texte stocké sur l'ordinateur de l'internaute. Accessible par le biais du navigateur, il peut être modifié par les sites *web* que visite l'internaute. Il s'agit d'un **fichier de suivi des différentes activités de connexion du navigateur**, indiquant l'heure, le nom de *login* utilisé pour se connecter sur un site *web* sécurisé. **Parfois, l'identifiant de la session en cours est inscrit dans ce fichier**, pourtant, ces informations sont des informations de sécurité qui, si elles sont révélées, permettraient à celui qui les détient de se connecter sur le site *web* sécurisé. Le vol de ce genre d'information est à l'origine des attaques en vol d'identité.

Voir : Historique de navigation.

Courriel (*e-mail*, *mail*) : document informatisé qu'un utilisateur saisit, envoie ou consulte en différé par l'intermédiaire d'un réseau. L'adresse électronique de l'internaute (adresse courriel ou *e-mail*) est le plus souvent composée d'un nom d'utilisateur et d'un nom de domaine séparés par un @.

Remarque : un courriel contient le plus souvent un texte auquel peuvent être joints d'autres textes, des images ou des sons. Par extension, le terme « courriel » et son synonyme « courrier électronique » sont employés au sens de « messagerie électronique ».

Voir : Canular, Moisson de courriels, Pourriel. (ANSSI)

Coquille : *voir* Faute de frappe opportuniste.

Cryptographie : discipline incluant les principes, moyens et méthodes de transformation de données dans le but de cacher leur contenu, d'empêcher que leur modification passe inaperçue et/ou d'empêcher leur utilisation non autorisée (ISO 7498-2).

Voir : Chiffrement, Cryptologie, Déchiffrement. (ANSSI)

Cryptologie : (en grec, **science du secret**) : souvent associée à de mystérieux enjeux d'espionnage militaire et diplomatique bien éloignés des préoccupations scientifiques habituelles, la cryptologie s'est longtemps résumée à un jeu sans fondements théoriques profonds entre ingénieux concepteurs de codes secrets et cryptanalystes acharnés ; à l'aube du XXIe siècle, elle s'est transformée en une science dynamique à l'intersection de nombreuses autres, plus orthodoxes, telles que les mathématiques, l'informatique et la micro-électronique.

Voir : Infrastructure de gestion de clés. (ANSSI)

Cyberrésilience : **capacité d'un système informatique à regagner un état de fonctionnement viable ou initial** à la suite d'une attaque. Les notions de configuration ou de paramétrage sont les éléments de base de la résilience. La restauration des sauvegardes est également un élément indispensable de la résilience.

Cybercrime as a Service *:* le cybercrime se traduit par de nouvelles formes de criminalité, en rapport notamment avec l'utilisation de l'Internet. Le « *Cybercrime as a Service* » (*CaaS*) peut consister en la **mise à disposition d'attaques préétablies en facilitant l'achat en ligne de logiciels malveillants, de données personnelles ainsi que la vente de numéros de cartes de crédit volées**. Le modèle d'affaire de cette forme de criminalité se développe dans le *Darkweb* avec des modes de paiement de type *bitcoins* capables de préserver l'anonymat des criminels.

Darkweb : *web* profond ou caché **partiellement ou pas du tout accessible en ligne**.

Voir : *Deepweb*, *Web* profond.

Dashboard : **tableau de bord de gestion informatique** permettant de surveiller et d'évaluer plusieurs indicateurs de performance à des moments donnés ou sur des périodes données.

Data : *voir* Donnée.

DDoS* (*Distributed Denial of Service attack) : ce genre d'attaque a pour objectif, comme une attaque en déni de service (*DoS* ou *Denial of Service attack)*, de **mettre un service en état d'indisponibilité**. Pour ce faire, **l'attaquant s'organise depuis plusieurs serveurs** dont il a le contrôle pour émettre en même temps des requêtes vers la cible. Criblé de requêtes, le service ne pouvant y répondre est alors considéré comme indisponible par ses clients légitimes.

Voir : Déni de service.

Déchiffrement : opération inverse d'un chiffrement réversible se traduisant par la **transformation d'un cryptogramme en donnée**.

Deepweb : voir *darkweb*.

Défiguration, barbouillage (*defacement*) : résultat d'une **activité malveillante qui a modifié l'apparence ou le contenu d'un serveur Internet** et a donc violé l'intégrité des pages en les altérant.

Remarque : Cette action malveillante est souvent accompagnée de revendications.

Voir : Déni de service. (ANSSI)

Démonstration de faisabilité (*Proof of Concept, PoC*) : code écrit pour **démontrer la faisabilité d'une attaque utilisant une vulnérabilité donnée**.

Remarque : ce code de démonstration n'est généralement pas malveillant ; il est **souvent écrit pour inciter l'éditeur à produire un correctif de la vulnérabilité**. Toutefois, un code malveillant peut être développé par la suite, à partir de ce code rendu public.

Voir : Code d'exploitation. (ANSSI)

Déni de service (*Denial of Service attack, DoS*) : **action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu**.

Remarque : **cette action n'est pas nécessairement malveillante**. Elle peut aussi traduire un mauvais dimensionnement du service, incapable de fournir la réponse à une forte demande. Si l'action est lancée depuis plusieurs sources, il est fréquent de parler de Déni de service distribué (*DDoS*).

Voir : Bombardement de courriels, Réseau de machines zombies. (ANSSI)

Dépassement ou débordement de mémoire (*buffer overflow*) : technique d'exploitation d'une vulnérabilité dans le code d'un programme qui ne vérifie pas correctement la taille de certaines données qu'il manipule.

Remarque : le principe peut être utilisé pour profiter de l'accès à certaines variables du programme par le biais de fonctions particulières. Il faut considérer celles qui ne

contrôlent pas la taille de la variable à enregistrer dans le tampon afin de pouvoir **écraser la mémoire jusqu'à l'adresse de retour de la fonction en cours d'exécution. L'utilisateur malveillant peut alors choisir les prochaines instructions qui seront exécutées par le système**. Le code introduit est généralement lancé avec les droits du programme détourné. Les exemples de fonctions les plus communément employées de façon vulnérable sont *scanf*() ou *strcpy*() dans la bibliothèque du langage C.

Voir : Vulnérabilité. (ANSSI)

Diffusion générale (*Broadcast*) : méthode de transmission de données à l'ensemble d'un réseau. (ANSSI)

***DNS* (*Domain Name System*)** : *voir* Système d'adressage par domaines.

***DNSSEC* (*Domain Name System Security Extensions*)** : extension pour la sécurité du protocole *DNS* (*Domain Name System*). (ANSSI)

Donnée : description élémentaire, souvent codée, d'une réalité (chose, transaction, événement, etc.).

Voir : *Data*.

Données massives (« *big data* ») : **ensembles volumineux de données impossibles à traiter avec les outils classiques** de gestion de bases de données car les fonctions classiques d'un système d'information qui consistent à capturer, stocker, rechercher, partager, analyser et visualiser les données et ne sont plus adaptées. En revanche, le traitement de ces données massives offre des perspectives (**corrélations inédites entre différentes données)**.

Voir : *Big data*.

DoS (Denial of Service attack) : *Voir* Déni de service.

Élévation de privilège (*Privilege escalation*) : **obtention de privilège supérieur par exploitation d'une vulnérabilité**. Par exemple, si un utilisateur local accède à des droits normalement réservés à l'administrateur, il y a élévation de privilège. Une élévation de privilège est souvent recherchée par une personne malveillante lorsqu'elle a réussi à s'introduire sur un système d'information en usurpant l'identité d'un utilisateur légitime.

Voir : Code malveillant, Vulnérabilité. (ANSSI)

E-mail *: voir* Courriel.

Espiogiciel (*Spyware*) : logiciel dont l'objectif est de collecter et de transmettre à des tiers des informations sur l'environnement dans lequel il est installé, sur les usages habituels des utilisateurs du système, à l'insu du propriétaire et de l'utilisateur. (ANSSI)

Exécution de code arbitraire à distance : mise en œuvre de commandes à distance sur un ordinateur, à l'insu de son utilisateur légitime.

Voir : Code malveillant, Mouchard Internet. (ANSSI)

Faille : vulnérabilité dans un système informatique permettant à un attaquant de porter atteinte à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient. (ANSSI)

Faute de frappe opportuniste, coquille (*Typosquatting*) : action malveillante qui consiste à **déposer un nom de domaine très proche d'un autre nom de domaine**, dont seuls un ou deux caractères diffèrent.

Remarque : les objectifs de cette action sont de **capter une partie du trafic adressé à un site officiel**. Par exemple, des noms de domaine comme certa.ssi.gouve.fr, ou encore certa.ssi.gouv_.fr au lieu de certa.ssi.gouv.fr.

Voir : Accaparement de noms de domaine. (ANSSI)

Fibre (optique) : désigne un type de câble pour relier deux nœuds d'un réseau local ou étendu. Il s'agit d'un fil en verre ou en plastique très fin conducteur de la lumière qui permet la transmission de données transformées en code binaire. Ce type de déploiement spécifique du réseau Internet constitue une alternative avantageuse en bande passante au réseau *RTC* initial grâce à un **débit binaire nettement supérieur à celui des câbles coaxiaux** (*RTC*) et peut servir de **support à un réseau « large bande »** (transit de la télévision, du téléphone, de la visioconférence ou de données informatiques).

La fibre désigne également le **mode de câblage** pour des réseaux physique locaux ou métropolitains.

Filoutage : *voir* Hameçonnage.

Firewall *: voir* Pare-feu.

Fonction de hachage (*Hash function*) : **fonction cryptographique** qui transforme une chaîne de caractères de taille quelconque en une chaîne de caractères de taille fixe et généralement inférieure. Cette fonction satisfait entre autres deux propriétés : la fonction est dite « à sens unique » quand il est difficile pour une image de la fonction donnée de calculer l'antécédent associé ; la fonction est dite

« sans collision » quand il est difficile de trouver deux antécédents différents de la fonction ayant la même image. (ANSSI)

Forensic science : l'informatique légale ou l'investigation numérique légale est l'application de techniques et de protocoles d'investigation numériques respectant les procédures légales ; elle est destinée à **collecter, analyser et conserver des preuves numériques à la demande d'une institution de type judiciaire** par réquisition, ordonnance ou jugement.

Fournisseur d'accès à l'Internet (FAI) : entreprise ou personne dont l'activité est d'offrir un accès à des services de communication au public en ligne, autrement dit à l'Internet.

Voir : la liste des membres de l'association des fournisseurs d'accès en France (AFA) sur le site de cette association : www.afa-france.com. (ANSSI)

Garde-barrière : *voir* Pare-feu.

GOST : *GOsudarstvennyi Standard* (standard gouvernemental) est un algorithme de chiffrement qui était devenu un standard en Union soviétique.

GRX : *GPRS Roaming Exchange* est un protocole pour faciliter la mobilité des usagers du *GPRS*. Le GRX permet d'établir le lien entre les réseaux *GPRS/IP* des différents opérateurs mobiles ; il s'agit d'une **épine dorsale de réseau centralisée à laquelle se connecte l'ensemble des réseaux *GPRS*** afin de leur fournir une connectivité continue.

GNU : « *GNU's Not UNIX* », soit en français « *GNU* n'est pas *UNIX* », est un **projet de système d'exploitation libre,** lancé en 1983 par Richard Stallman, qui se détachait du système d'exploitation *UNIX* dont les distributions étaient, pour la plupart, propriétaires et non libres d'usage.

Hachage *(Hash function)* : *voir* Fonction de hachage.

Hameçonnage, filoutage (*Phishing*) : **vol d'identités ou d'informations confidentielles (codes d'accès, coordonnées bancaires) par subterfuge : un système d'authentification est simulé par un utilisateur malveillant**, qui essaie alors de convaincre des usagers de l'utiliser et de communiquer des informations confidentielles, comme s'il s'agissait d'un système légitime.

Remarque : **les sites fréquentés par les usagers attaqués sont reproduits**, après avoir été aspirés. L'utilisateur est souvent invité à visiter le site frauduleux par un courrier électronique. (ANSSI)

Historique de navigation : *voir Cookie*.

Hoax : *voir* Canular.

Homme-au-milieu, entre-deux (*Man-in-the-Middle, MITM*) : **attaque par laquelle une personne malveillante s'interpose dans un échange de manière invisible** pour les utilisateurs ou les systèmes.

Remarque : la connexion est maintenue, soit en substituant d'autres éléments aux éléments transférés, soit en les réinjectant. Une attaque connue dans cette catégorie repose sur une compromission des tables *ARP* (*ARP Poisoning*). Contrer ce type d'attaque par le milieu est aussi l'un des objectifs des infrastructures de gestion de clés. (ANSSI)

Information : en informatique, une information représente un **renseignement**, une **documentation** au sujet de quelque chose ou de quelqu'un à partir desquels un programme ou une application pourront décider de la suite de leur exécution. Contrairement à la donnée, **l'information constitue une unité qui portée à la connaissance de quelqu'un le rend capable de prendre une décision**. On peut obtenir une information en combinant des données.

Infrastructure de clés publiques (ICP) : **outil cryptographique permettant de garantir l'authenticité des clés publiques** par la signature électronique d'autorités de certification organisées de façon hiérarchique. Une ICP est l'un des outils fondamentaux d'une infrastructure de gestion de clés (IGC). (ANSSI)

Infrastructure de gestion de clés (IGC) (*Public Key Infrastructure - PKI*) : ensemble organisé de composantes fournissant des services de gestion des clés cryptographiques et des certificats de clés publiques au profit d'une communauté d'utilisateurs. (ANSSI)

Ingénierie sociale (*Social Engineering*) : **manipulation consistant à obtenir un bien ou une information en exploitant la confiance, l'ignorance ou la crédulité de tierces personnes**.

Remarque : les personnes malveillantes partent du principe que **le facteur humain est le maillon faible de la sécurité d'un système d'information**. (ANSSI)

Injection de code indirecte (*Cross Site Scripting, CSS, XSS*) : **activité malveillante qui consiste à injecter des données arbitraires dans le code de pages *HTML* pour en détourner le sens ou en capter les utilisateurs**. Un utilisateur malveillant peut parvenir à afficher sur un site *web* vulnérable un contenu agressif ; ce contenu peut

rediriger l'utilisateur vers d'autres sites, ou transmettre des informations (jetons de sessions, aussi appelés *cookies*, etc.) ou des droits.

Remarque : les données arbitraires sont souvent écrites en *JavaScript*, en *HTML* ou en *VBScript*. La personne malveillante introduit ainsi du code dans le serveur vulnérable qui héberge le site. **Ce serveur est rarement affecté par ce code** (porteur sain). Les visiteurs du site, potentiellement victimes, consultent la page contenant le code injecté. L'exécution du code ne se fait pas au niveau du serveur, mais par le client de navigation de l'utilisateur. La notation *XSS* a été introduite pour remplacer *CSS*, acronyme déjà utilisé pour signifier *Cascading Style Sheet*.

Voir : Code malveillant. (ANSSI)

IPsec - IPv4 - IPv6 : *voir* Protocole *IP*, Intégrité.

Java : **langage de programmation informatique dont l'objectif central est de rendre les programmes exprimés dans ce langage indépendants des plates-formes** (*PC, Apple*, etc.), **de leurs processeurs** (*ARM, INTEL, RISC*, etc.), **de leurs systèmes d'exploitation** (*Linux, Windows, Mac OS,* etc.). Pour ce faire, chaque plate-forme recevra un cadre logiciel, appelé **machine virtuelle *Java***, développé spécifiquement pour recevoir les programmes développés en *Java* pour que la « portabilité » des applications développées en *Java* soit garantie sur chaque plate-forme. Le second avantage du langage *Java* est sa **structure de conception des applications orientée objet** qui permet au concepteur de l'application de traduire la problématique réelle en langage machine de manière plus intuitive.

Journaux d'événements : la journalisation des événements (de l'anglais « *logging* ») fait appel au concept de « *log* » qui désigne l'**enregistrement séquentiel dans un fichier ou dans une base de données de tous les événements affectant un processus comme une application, l'activité d'un réseau informatique**… Les « *logs* » permettent d'analyser pas à pas l'activité interne d'un processus informatique et ses interactions avec son environnement. Ces journaux sont datés et classés par ordre chronologique pour mener des opérations d'investigation et de reconstituer le mode opératoire d'attaquants lors d'une analyse forensique.

Logs *: voir* Journaux d'événements.

Logiciel de contrôle parental ou de filtrage : ces systèmes de protection s'installent sur un ordinateur et permettent notamment de **bloquer l'accès à des sites inappropriés aux plus jeunes**. Certains permettent de paramétrer l'accès à l'Internet (plages horaires, durée, applications…). Tout ordinateur personnel utilisé par un mineur devrait en être équipé (voir les résultats du comparatif des principaux logiciels existants sur le marché).

Voir : Pare-feu. (ANSSI)

Logiciel espion : *voir* Espiogiciel.

Logiciel libre : alternative au logiciel propriétaire. L'usage d'un logiciel libre, son étude, sa modification et sa duplication en vue de sa diffusion sont techniquement et légalement autorisés afin de **garantir le contrôle du programme par l'utilisateur et la possibilité de son partage entre usagers**.

Logiciel publicitaire (*Adware*) : code ayant pour finalité d'**afficher des bandeaux publicitaires par le biais du navigateur Internet de l'utilisateur**.

Remarque : ce code, très souvent perçu comme une méthode envahissante, engendre fréquemment d'autres effets sur le système, comme l'apparition de fenêtres surgissantes (*popups*), la dégradation de la bande passante ou de la performance de la machine de l'utilisateur.

Voir : Code malveillant. (ANSSI)

Main frame : **ordinateur de grande puissance** de traitement dont l'infrastructure repose sur un **modèle centralisé**, par opposition au modèle distribué que constituent les réseaux de machines. Puissant et fiable, ce type d'ordinateur est utilisé dans les très grandes entreprises (banques, compagnies d'assurances, compagnies aériennes, sociétés de services, mairies…). Jusqu'à la fin des années 1990, ce type d'ordinateurs a été le seul capable de répondre au traitement de très grandes bases de données auxquelles accèdent des milliers d'utilisateurs. Ce terme désigne aujourd'hui plutôt les ordinateurs issus de la gamme *IBM* 360 et 370, tandis que **les grands systèmes non *IBM* sont plutôt appelés « serveurs » ou « superordinateurs »**.

Mail *: voir* Courriel.

Malicious software : *voir* Code malveillant.

Malware *: voir* Code malveillant.

Messagerie instantanée (MI ou *IM*) : logiciel permettant de dialoguer en direct avec une liste connue d'amis (le plus courant MSN). (ANSSI)

Moisson de courriels (*Mail harvesting*) : action qui consiste à parcourir un grand nombre de ressources publiques (pages Internet, groupes de discussion, etc.), afin d'y **collecter des adresses électroniques avec des intentions malveillantes** comme, par exemple, envoyer des courriels contenant des virus, des canulars ou des pourriels.

Remarque : pour s'en prémunir, il est possible de **présenter sur ces ressources publiques une adresse électronique qui trompe les outils de recherche** (comme prenom.nom_AT_domain.fr pour les outils cherchant '@', caractéristique d'une adresse) ; cela est appelé *address munging*.

Voir : Canular, Courriel, Pourriel. (ANSSI)

MOOC (en anglais : *Massive Open Online Course ou* « cours en ligne ouvert et massif » (*CLOM*)) : **cours en ligne ouvert à tous** où enseignants et élèves sont dispersés géographiquement et communiquent uniquement par l'Internet. Les *MOOCs* constituent une forme de formation ouverte et à distance en télé-enseignement. Le terme « massif » exprime l'ouverture de ces cursus scolaires à plusieurs centaines ou plusieurs milliers de personnes.

Mot de passe (*Password*) : un mot de passe est un **élément de déverrouillage** permettant de vérifier l'identité annoncée d'une personne par un système d'information.

Voir : Authentification, Identification. (ANSSI)

Mouchard Internet (*Web Bug*) : support graphique implanté dans une page Internet ou un courriel qui a pour objectif de **surveiller la consultation de cette page ou de ce courriel, à l'insu des lecteurs**.

Remarque : **ces supports sont souvent invisibles**, car beaucoup sont paramétrés avec une taille très petite (1x1 pixel). Ils sont aussi fréquemment représentés par des balises *HTML IMG*.

Voir : Espiogiciel. (ANSSI)

No SQL : désigne communément la **façon plus intuitive de rechercher une information dans de grands volumes de données. Elle s'oppose au mode *SQL*** qui fait appel à un langage rigoureux, dépendant de la structure de la base de données dite « en tableau », désignant ainsi la façon dont les données sont stockées et reliées entre elles. De façon technique, *no SQL* désigne la catégorie de systèmes de gestion de base de données (SGBD) qui n'est plus fondée sur l'architecture classique des bases relationnelles et où l'unité logique n'est plus la table, et, où les données ne sont en général pas manipulées avec *SQL*.

Numéroteur (*Dialer*) : logiciel qui **compose automatiquement des numéros de téléphone**.

Remarque : les numéroteurs sont souvent proposés pour accéder à des sites à caractère pornographique (appels surtaxés). Par extension, un *war dialer* est une application composant une liste de numéros, et qui enregistre ceux retournant une tonalité spéciale, comme un modem ou un fax. (ANSSI)

Open data **(**données ouvertes**)** *:* des données numériques mises à disposition par les institutions publiques ou d'origine privée (une collectivité) selon une méthodologie et une licence ouverte garantissant leur **libre accès** et leur **réutilisation par tous, sans restriction technique, juridique ou financière**. L'information publique est considérée comme un bien commun dont la diffusion est d'intérêt général.

Opérateur d'importance vitale (OIV) : l'article R. 1332-1 du code de la défense précise que les opérateurs d'importance vitale sont désignés parmi les **opérateurs publics ou privés** mentionnés à l'article L. 1332-1 du même code, ou parmi les **gestionnaires d'établissements** mentionnés à l'article L. 1332-2. Un opérateur d'importance vitale : exerce des activités mentionnées à l'article R. 1332-2 et comprises dans un secteur d'activités d'importance vitale ; gère ou utilise au titre de cette activité un ou des **établissements ou ouvrages**, une ou des **installations** dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement d'obérer gravement le **potentiel de guerre ou économique**, la **sécurité** ou la **capacité de survie de la Nation** ou de mettre gravement en cause **la santé ou la vie de la population**. (ANSSI)

OS (en anglais *Operating System*) ou système d'exploitation : **premier programme exécuté lors de la mise en marche de l'ordinateur**, l'OS permet de gérer les activités et fonctions du processeur et des autres ressources matérielles d'un ordinateur. Ses services généraux facilitent la création de logiciels applicatifs ; il sert **d'intermédiaire entre ces logiciels et le matériel informatique**.

OTT (en anglais *Over The Top*) ou **Communications *OTT***: **ces réseaux de services interviennent « par-dessus » les réseaux des opérateurs**, diffusés à très grande échelle ; leur succès mondial crée une valeur colossale pour le fédérateur du service sans contrepartie pour les opérateurs. Par exemple, en France, le réseau « voix » de « *skype* » rémunère sa compagnie et soustrait des revenus à l'opérateur *Orange*.

Outils de dissimulation d'activité (*Rootkit*) : tout programme ou ensemble de programmes permettant de **dissimuler une activité, malveillante ou non, sur une machine**, permettant à une personne malveillante de maintenir un contrôle illégitime du système d'information en y dissimulant ses activités. L'activité dissimulée peut être une activité sur le système de fichiers (création, lecture, écriture), une activité réseau, une activité en mémoire. Pour cela, un *rootkit* peut travailler dans l'environnement de l'utilisateur, sans droits particuliers, ou en profondeur dans le système d'exploitation, nécessitant par conséquent des droits d'exécution élevés.

Remarque : l'installation de ces programmes nécessite que le système soit préalablement compromis (cheval de Troie, intrusion). Ces programmes modifient souvent les commandes usuelles de l'administrateur, afin de dissimuler toute trace de leur présence. Ils effectuent aussi fréquemment plusieurs opérations au niveau du noyau du système d'exploitation, comme l'**installation de portes dérobées**, la **capture des frappes du clavier**, etc. Un outil de dissimulation d'activité n'a pas

pour but d'offrir un accès quelconque à la machine hôte. En revanche, la plupart de ces outils malveillants embarquent des fonctionnalités de porte dérobée permettant à l'auteur un accès à distance et un maintien sur le système compromis.

Voir : Capteur clavier, Cheval de Troie, Code malveillant, Porte dérobée. (ANSSI)

Pare-feu (*Firewall*) : un pare-feu (ou garde-barrière), est un outil permettant de **protéger un ordinateur connecté à un réseau ou à l'Internet**. Il protège d'attaques externes (**filtrage entrant**) et souvent de connexions illégitimes à destination de l'extérieur (**filtrage sortant**) initialisées par des programmes ou des personnes malveillants. (ANSSI)

Paquets : le transport sous forme d'un signal par les câbles ou plus généralement les médias de communication des informations ou messages entre humains exige des adaptations (voir Protocole), dont le **découpage, en paquets, de chaînes de données trop longues afin de les rendre compatibles avec les contraintes d'un signal électrique**. Chaque paquet est transmis séparément puis ils sont **réassemblés, lors de la réception, pour reconstituer le même message**. Le protocole émet les règles de découpage (conditionnement), d'apposition d'un en-tête (en anglais, *header*) comprenant les informations nécessaires pour acheminer et réassembler le message afin que ces paquets transmis soient réassemblables. La notion de paquet évoque un paquet réseau et plus particulièrement un paquet *IP*.

***Password** : voir* Mot de passe.

***Phishing** : voir* Filoutage, Hameçonnage.

***PKI* (*Public Key Infrastructure*)** : voir IGC.

Plate-forme informatique : **base de travail** permettant d'écrire, de lire, d'utiliser et de développer des logiciels, des applications, des sites Internet, etc.

Polymorphe (*Polymorphic*) : ver ou **virus dont le code est chiffré**, changeant le code de déchiffrement d'une infection à l'autre, et donc l'apparence et/ou la signature.

Voir : Code malveillant, Ver, Virus. (ANSSI)

Port : **porte donnant accès à un système d'exploitation**. Le code numérique est utilisé dans les protocoles comme *TCP* ou *UDP* pour identifier le service auquel appartient un paquet d'information du protocole *IP*. Par exemple, le service *HTTP* est associé au port 80. (ANSSI)

Porte dérobée (*Backdoor*) : **accès dissimulé, soit logiciel soit matériel, qui permet à un utilisateur malveillant de se connecter à une machine de manière furtive**. *Remarque* : une porte dérobée peut également être la cause d'une mise en œuvre incorrecte d'un protocole. (ANSSI)

Voir : Canal caché, Cheval de Troie, Code malveillant, Poste à poste (*Peer-to-Peer*, P2P), réseau d'échange et de partage de fichiers de particulier à particulier (exemples *e-mule*, *kasaa*, *limewire*, *eDonkey*).

Poste à poste (Peer to peer ou, en français, pair à pair) : abrégé en « P2P », **modèle de réseau informatique où chaque client est également un serveur**, à la différence d'un modèle centralisé (*main frame*) ou du modèle client-serveur. Dans la pratique, le poste à poste permet le **partage de fichiers**, le **calcul distribué** (*grid computing*) ou la **communication d'égal à égal**. Lorsque ces partages ne sont pas reliés par des serveurs de communications d'hébergeurs, les échanges échappent à leur contrôle, c'est de cette façon que les échanges poste à poste contournent, par exemple, les règles de téléchargement fixées par les opérateurs.

Pourriel, polluriel (*spam*) : **courrier électronique non sollicité par le destinataire**. *Remarque* : le courrier est souvent envoyé simultanément à un très grand nombre d'adresses électroniques. Les produits les plus vantés par ces pourriels sont les services pornographiques, la spéculation boursière, les médicaments, le crédit financier, etc.

Voir : Courriel, Hameçonnage. (ANSSI)

Protocole (informatique ou de communication) **: spécification et automatisation des règles précises employées par un logiciel ou un programme pour effectuer un type de communication** donné entre deux ordinateurs ou entre deux programmes d'un même ordinateur. Les protocoles représentent ces processus de traduction successifs.

Les informations reçues sont traduites sous forme d'un signal en une information compréhensible par l'homme ou par les applications. De même sont traduites en signal les informations produites par l'homme ou les applications. Les règles de traduction du langage humain vers le signal doivent correspondre à celles utilisées pour traduire le signal en langage humain.

Pour assurer l'interopérabilité entre des ordinateurs conçus par des constructeurs différents, et donc l'application universelle de ces règles, des normes de ces protocoles ont été définies, c'est le rôle d'organismes comme *l'ISO, l'IETF, l'IEEE*, etc. Chaque concepteur conçoit son équipement en programmant sept couches abstraites correspondant à **sept règles de traduction** : physique, liaison de donnée, réseau, transport, session, présentation, application. Ainsi, la couche physique représente l'interface physique qui connecte l'ordinateur au réseau physique (au réseau téléphonique commuté, *RTC*, par exemple).

Un protocole régit tout aussi bien la communication entre deux machines distantes que la communication entre plusieurs couches d'une même machine.

Protocole *IP* : la communication sur l'Internet est fondée sur un protocole appelé *IP* pour *Internet Protocol* qui **permet aux ordinateurs de communiquer entre eux. Ce protocole utilise des adresses numériques pour distinguer ces machines et tronçonne la communication en paquets** comportant chacun une adresse de source et une adresse de destination. La version la plus couramment employée du protocole est la version *IPv4* dans laquelle les adresses sont composées de quatre nombres comme par exemple 213.56.176.2. Une nouvelle version du protocole est en cours de déploiement : *IPv6*. Elle utilise des adresses plus longues composées de huit nombres notés en hexadécimal comme par exemple 1 fff:00a88:85a3:0000:000:ac1f:8001. Enfin *IPsec* désigne un protocole de chiffrement et de signature des paquets *IP*. (ANSSI)

Référentiel général de sécurité (RGS) : ensemble des règles établies par l'ANSSI et prévues par l'ordonnance n° 2005-1516 du 8 décembre 2005 « *relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives* » que doivent respecter certaines fonctions contribuant à la sécurité des informations, parmi lesquelles la **signature électronique**, l'**authentification**, la **confidentialité** ou encore l'h**orodatage**. (ANSSI)

Renifleur (*Sniffer*) : **outil matériel ou logiciel dont l'objet est de capturer les trames transitant sur le réseau**.

Remarque : **si les trames contiennent des données non chiffrées, un utilisateur malveillant peut aisément récupérer des données confidentielles**, comme des mots de passe, des courriers électroniques, des contenus de pages Internet, etc. L'utilisateur malveillant peut aussi, à partir des trames, récupérer **des informations** sur les systèmes échangeant les trames, comme le système d'exploitation ou les services employés. (ANSSI)

Réseau de machines zombies (*Botnet*) : un *botnet*, autrement dit un réseau de *bots* (contraction de réseau de robots) est un **réseau de machines compromises, également appelées « zombies », à la disposition d'un individu malveillant (le maître)**. Ce réseau est structuré de façon à permettre à son propriétaire de transmettre des ordres à tout ou partie des machines du réseau et de les actionner à sa guise.

Remarque : Certains réseaux peuvent atteindre des nombres considérables de machines (plusieurs milliers). Celles-ci peuvent faire l'objet de commerce illicite ou d'actions malveillantes contre d'autres machines.

Voir : Déni de service. (ANSSI)

Ressource : composants, matériels ou logiciels, connectés à un ordinateur.

RFID (*Radio Frequency IDentification*) : **récupération et mémorisation de données à distance** grâce à des radios étiquette comprenant une antenne associée à une puce électronique.

Rootkit *: voir* Outil de dissimulation d'activité.

SCADA (en anglais *Supervisory Control and Data Acquisition*) : **système de contrôle et d'acquisition de données qui permet la gestion à grande échelle et en temps réel d'un grand nombre de capteurs**. Les capteurs sont chargés de collecter les données de mesures ; le *SCADA* gère et fédère ces télémesures. Un *SCADA* incorpore également un système de contrôle qui lui permet de **réguler à distance les installations techniques**. Un *SCADA* désigne également la suite logicielle industrielle qui gère les installations techniques. La nouvelle génération de *SCADA* est de plus en plus intégrée aux outils de gestions de l'entreprise : les *ERP* par le biais d'une interface appelée *MES* conformément au standard *ISA-95*.

Serveur racine ou serveur de noms de la racine (*Root name server)* *:* en informatique, la racine est le point de départ d'une arborescence. Il existe actuellement **treize serveurs de noms de la racine** répartis dans le monde.

Ces serveurs hébergent les données permettant le bon fonctionnement du Système d'adressage par domaines (*DNS*) et des services qui utilisent ce système (Internet, courrier électronique, etc.). (ANSSI)

SIEM (*Security Information and Event Management)* : **ensemble d'outils d'analyse permettant la supervision de la sécurité d'un système d'information**.

Signal : *voir* Protocole.

SOC (Security Operations Center) : **centre de sécurité opérationnelle** qui agit sur un site donné mais peut intervenir à distance à l'aide d'outils spécifiques et particulièrement sécurisés : cette supervision est dite centralisée et distribuée. Un *SOC* est une partie du système d'information de l'entreprise destiné à la **mise en place de solutions pour la détection, la localisation et la qualification des événements de sécurité et la mise à disposition de plans de réaction**.

Spam *: voir* Pourriel.

Spyware *: voir* Espiogiciel.

SSL (Secure Sockets layer) : *voir Transport Layer Security* (*TLS*).

Système d'adressage par domaines (*domain name system*, *DNS*) : système de bases de données et de serveurs assurant la **correspondance entre les noms de domaine ou de site utilisés par les internautes et les adresses numériques utilisables par les ordinateurs**. Par exemple, le *DNS* établit la correspondance entre le domaine « cert.ssi.gouv.fr » et l'adresse 213.56.176.2. Ce système permet aux internautes d'utiliser, dans la rédaction des adresses, des **noms faciles à retenir au lieu de la suite de chiffres du protocole *IP***.

Voir : Protocole *IP*. (ANSSI)

Système de traitement automatisé de données ou STAD (expression utilisée en droit pénal français depuis la loi Godfrain du 5 janvier 1988) : ensemble composé d'une ou plusieurs unités de traitement, de mémoire, de logiciel, de données, d'organes d'entrées-sorties et de liaisons, qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs de sécurité.

Test d'intrusion (*Penetration test*) : action qui consiste à essayer plusieurs codes d'exploitation sur un système d'information afin de déterminer ceux qui donnent des résultats positifs permettant d'y pénétrer.

Remarque : il s'agit à la fois d'une intention défensive (mieux se protéger) et d'une action offensive (agresser son propre système d'information). (ANSSI)

Transport Layer Security ou *SSL* (*Secure Sockets Layer*) : **protocole de sécurité des échanges** développé à l'origine par *Netscape* et normalisé par l'*IETF*. Il fonctionne suivant un mode client-serveur afin de répondre aux exigences de sécurité : **authentification du serveur** (le client s'assure que le serveur est légitime), **authentification du client** (le serveur s'assure que le client est légitime), confidentialité des données échangées grâce à l'**utilisation d'une clé de session** qui permet de chiffrer les données et d'assurer leur intégrité, Le protocole est très largement utilisé dans le déploiement de *VPN* (*Virtual private Network*) de niveau 5 (couche session).

***Typosquatting** : voir* Faute de frappe opportuniste.

***Trojan horse** : voir* Cheval de Troie.

Usurpation d'adresse (*Address Spoofing*) : action malveillante qui consiste à **utiliser délibérément l'adresse d'un autre système en lieu et place de la sienne**.

Remarque : il faut rapprocher cette action de l'usurpation d'identité, considérée comme un délit par le droit pénal français. L'idée est de faire passer son système d'information pour un autre. L'adresse usurpée peut être une adresse *MAC* (pour *Medium Access Control*), une adresse *IP*, une adresse de messagerie, etc.

Voir : Canular, Pourriel, Protocole *IP*. (ANSSI)

Ver (*Worm*) : **logiciel malveillant indépendant cherchant à propager son code au plus grand nombre de cibles, puis à l'exécuter sur ces mêmes cibles**. Il perturbe le fonctionnement des systèmes concernés en s'exécutant **à l'insu des utilisateurs**.

Remarque : les deux termes ver et virus sont relativement proches. Un ver est un virus qui se propage de manière quasi autonome (sans intervention humaine directe) *via* le réseau. Les vers sont une sous-catégorie de virus dont le vecteur primaire de propagation reste le réseau.

Voir : Code malveillant, Virus. (ANSSI)

Virus : **programme ou morceau de programme malveillant** dont le but est de survivre sur un système informatique (ordinateur, serveur, appareil mobile, etc.) et, bien souvent, d'en atteindre ou d'en **parasiter les ressources** (données, mémoire, réseau). Le mode de survie peut prendre plusieurs formes : réplication, implantation au sein de programmes légitimes, persistance en mémoire, etc. Pour sa propagation, un virus utilise tous les moyens disponibles : messagerie, partage de fichiers, portes dérobées, pages Internet frauduleuses, clés USB, etc.

Voir : Code malveillant, Ver. (ANSSI)

Voix sur réseau IP (*VoIP Voice over Internet Protocol*) : technologie qui permet de véhiculer la voix sur l'Internet ou tout autre réseau acceptant le protocole *TCP/IP*. Cette technologie est notamment utilisée par le service de téléphonie *IP* (*ToIP - telephony over Internet protocol*) à travers des logiciels tels que *SIP*, *Windows Live Messenger*, *Skype*, *Asterisk*, *Ekiga*, *Google talk*, etc. (ANSSI)

Vulnérabilité (*Vulnerability*) : faute, par malveillance ou maladresse, dans les spécifications, la conception, la réalisation, l'installation ou la configuration d'un système, ou dans la façon de l'utiliser.

Remarque : une vulnérabilité peut être utilisée par un code d'exploitation et conduire à une intrusion dans le système.

Voir : Code d'exploitation. (ANSSI)

Web *ou World Wide Web (www)* : terme anglais signifiant **la toile d'araignée mondiale** ; il désigne un **système d'hypertexte fonctionnant sur le réseau Internet**. Le système d'*HyperText* permet de modéliser la connaissance sous forme de lien jusqu'à former des pans complet de connaissances déposées sur des serveurs distants.

Le *web* repose sur une **architecture client/serveur** utilisant pour communiquer le **protocole *HTTP***. Le *web* s'adapte particulièrement bien à l'Internet du fait de la taille des éléments qui sont transportés. Le *web* est une application distincte d'autres applications comme le courrier électronique, la messagerie instantanée et le partage de fichiers de pair à pair.

***Wireless Fidelity* (*Wi-Fi*)** : *voir* Accès sans fil, *Bluetooth*.

Zéro jour (*Zero-day*) : catégorie particulière de codes d'exploitation qui ciblent des **vulnérabilités qui ne sont pas encore publiquement annoncées** par l'éditeur, le constructeur ou un chercheur en sécurité.

Remarque : Ces codes d'exploitation sont **particulièrement dangereux** sur le plan de la sécurité des systèmes informatiques car ils ne sont **pas connus** et il n'y a **pas de correctif** pour s'en protéger. Seule une défense en profondeur permet de limiter les risques. Ils doivent être mis hors d'état de nuire immédiatement.

Voir : Code d'exploitation, Code malveillant.

***Web* profond** : partie du *web* accessible ou non en ligne mais non pas par les moteurs de recherche indexés comme *Google,* etc. mais par des moteurs de recherche tels que *BASE* ou *Tor*, indexant de façon spécifique cette partie du réseau.

Zombies, réseau de zombies : *voir* Réseau de machines zombies (*Botnet*).

LEXIQUE DES SIGLES

Les sigles assortis d'une explication ne figurent que dans le glossaire.

ACN : Alliance pour la confiance numérique

ACPR : Autorité de contrôle prudentiel et de résolution

ADPF : Association pour la diffusion de la pensée française

***ADSL* :** *Asymmetric Digital Subscriber Line*

AES : *Advanced Encryption Standard*

AFA : Association des fournisseurs d'accès et de services Internet

AFNOR *:* Association française de normalisation

ANSES : Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail

ANSI : *American National Standards Institute*

ANSSI : Agence nationale de la sécurité des systèmes d'information

ANTS : Agence nationale des titres sécurisés

ASCII : *American Standard Code for Information Interchange*

ASIP Santé : Agence des systèmes d'information partagés de santé

B2i : Brevet informatique et Internet

BCR : *Binding Corporate Rules* (règles de sécurité compatibles avec les métiers de l'entreprise)

BICS : *Belgacom International Carrier Services* (opérateur)

BND : *Bundesnachrichtendienst* - Service fédéral de renseignement allemand

BSC : *Base Station Controller*

BTS : *Base Transceiver Station*

C2i2mi : Certificat informatique et Internet, niveau 2 des « métiers de l'ingénieur »

CADA : Commission d'accès aux documents administratifs

CALID : Centre d'analyse de lutte informatique défensive

CDEFI : Conférence des directeurs des écoles françaises d'ingénieurs

CDSE : Club des directeurs de sécurité des entreprises

CEA-DAM : Commissariat à l'énergie atomique - Direction des applications militaires

CECyF : Centre expert contre la cybercriminalité français

CEN : Comité européen de normalisation

CENELEC : *European Committee for Electrotechnical Standardization*

CERN : Organisation européenne pour la recherche nucléaire

CERT/CC : *Computer Emergency Response Team Coordination Center*

CESIN : Club des experts de la sécurité de l'information et du numérique

CICS *:* Conseil des industries de confiance et de sécurité

CIGREF : Club informatique des grandes entreprises françaises

CIM : *Computer Integrated Manufacturing*

CLUSIF : Club de la sécurité de l'information français

CNIL *:* Commission nationale de l'informatique et des libertés

CNNum : Conseil national du numérique

CoFIS *:* Comité de la filière industrielle de sécurité

CPU : Conférence des présidents d'université

CSCG: *Cybersecurity Coordination Group créée conjointement par les autorités européennes CEN, CENELEC et ETSI*

CVE : *Common Vulnerabilities and Exposures*

DARPA : *Defense Advanced Research Projects Agency*

DCRI : Direction centrale du renseignement intérieur devenue DGSI

DGA : Direction générale de l'armement

DGCIS : Direction générale de la compétitivité, de l'industrie et des services

DGE : Direction générale des entreprises

DGSE : Direction générale de la sécurité extérieure

DGSI : Direction générale de la sécurité intérieure

DES : *Data Encryption Standard*

DHCP : *Dynamic Host Configuration Protocol*

DIN : *Deutsches Institut für Normung* (Institut allemand de normalisation)

DoD : *United States Department of Defense*

DMP : Dossier médical personnel

DMZ : *Demilitarized Zone*

DNS : Directives nationales de sécurité

DPSD : Direction de la protection et de la sécurité de la défense

DSI : Direction ou directeur des systèmes d'information

DTE : *Data Terminal Equipment*

DCE : *Data Circuit-terminating Equipment*

EC3 : *European Cybercrime Centre (Europol)*

eIDAS : *Electronic identification and trust services* (règlement européen sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur)

ENISA : *European Union Agency for Network and Information Security*

EPN : Espace public numérique

ERP : *Enterprise Resource Planning*

ESIEA : École supérieure d'informatique électronique automatique

ETI : Entreprises de taille intermédiaire

ETSI : *European Telecommunications Standards Institute*

FIEEC : Fédération des industries électriques, électroniques et de communication

FISA : *Foreign Intelligence Surveillance Act*

FNTC : Fédération nationale des tiers de confiance

GAC : *Govermental Advisory Committee*

GAFA : *Google, Amazon, Facebook, Apple*

GGSN : *Gateway GPRS Support Node*

GICAN : Groupement des industries de construction et activités navales

GICAT : Groupement des industries de défense et de sécurité terrestres et aéroterrestres

GIFAS : Groupement des industries françaises aéronautiques et spatiales

GITSIS : Groupement interprofessionnel pour les techniques de sécurité des informations sensibles

GPS : *Global Positioning System*

GPRS : *General Packet Radio Service*

GSM : *Global System for Mobile Communications*

GSMA : *GSM Association* (qui représente 850 opérateurs de téléphonie mobile dans le monde)

HLR : *Home Location Register*

HSS : *Home Subscriber Server*

HTML : *HyperText Markup Language*

HTTP : *HyperText Transfer Protocol*

HTTPS : *HyperText Transfer Protocol Secure*

IaaS : *Infrastructure as a Service*

IANA : *Internet Assigned Numbers Authority*

ICANN : *Internet Corporation for Assigned Names and Numbers*

ICASI : *Industry Consortium for Advancement of Security on the Internet*

IEC : *International Electrotechnical Commission*

IETF : *Internet Engineering Task Force*

IHEST : Institut des hautes études pour la science et la technologie

INHESJ : Institut national des hautes études de la sécurité et de la justice

INRIA : Institut national de recherche en informatique et en automatique

INSA : Institut national des sciences appliquées

IP : *Internet Protocol*

ISMS : *Information Security Management System* (système de gestion de la sécurité de l'information)

ISN : Enseignement « Informatique et sciences du numérique »

ISO : *International Organization for Standardization* (en français : Organisation internationale de normalisation)

***ITIF* :** *Information Technology and Innovation Foundation*

JTC : *Joint Technical* Committee (groupe de travail dépendant du mécanisme de normalisation de l'*ISO*)

LORIA : Laboratoire lorrain de recherche en informatique et ses applications

LPM : Loi de programmation militaire

MES : *Manufacturing Execution System*

MIT : *Massachusetts Institute of Technology*

MSC : *Mobile Switching Center*

MSS : *Maximum Segment Size*

NIST : *National Institute of Standards and Technology*

NSA : *National Security Agency*

OCLCTIC : Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication

OIV : Opérateurs d'importance vitale

OMNSH : Observatoire des mondes numériques en sciences humaines

OPECST : Office parlementaire d'évaluation des choix scientifiques et technologiques

OTP : *One Time Password*

PaaS *Platform as a Service*

PC : *Personal Computer*

PCA : Plan de continuité de l'activité

PHAROS : Plate-forme d'harmonisation, d'analyse, de recoupement et

d'orientation des signalements

PIA : Programme d'investissements d'avenir

PIAs : *Privacy Impact Assessments*

PME : Petites et moyennes entreprises

PMI Petites et moyennes industries

PNIJ : Plate-forme nationale d'interceptions judiciaires

Prism : Programme nord-américain de surveillance électronique par la collecte de renseignements à partir d'Internet et d'autres fournisseurs de services électroniques, également appelé US-984XN.

PSSIE : Politique de sécurité des systèmes d'information de l'État

RLE : Réseau local d'entreprise

RSSI : Responsable de sécurité des systèmes d'information

RTC : Réseau téléphonique commuté

SaaS *Software as a Service*

SAP : *Systems, applications, and products for data processing*

SCAP : *Security Content Automation Protocol*

SGDSN : Secrétariat général de la défense et de la sécurité nationale

SGG : Secrétariat général du Gouvernement

SGSN **:** *Serving GPRS Support Node*

SIF : Société informatique de France

Signal Spam : Plate-forme de signalement des *spams*

SIM : *Subscriber Identity Module*

SMS : *Short Message Service*

SMTP : *Simple Mail Transfer Protocol*

SNMP : *Simple Network Management Protocol*

SSID : *Service Set Identifier*

TAFTA : *Trans-Atlantic Free Trade Agreement* (voir *TTIP*)

TCP/IP : *Transmission Control Protocol / Internet Protocol*

TIs : Technologies de l'information

TLD *:* *Top Level Domain*

TPE : Très petites entreprises

TTIP *:* *Transatlantic Trade and Investment Partnership,* traité de partenariat transatlantique de commerce et d'investissement avec les États-Unis d'Amérique (voir *TAFTA*)

UEFI : *Unified Extensible Firmware Interface*

UPMC : Université Pierre et Marie Curie

URL : *Uniform Ressource Locator*

USB : *Universal Serial Bus*

VLAN : *Virtual Local Area Network*

VLR : *Visitor location register*

VPN : *Virtual Private Network*

W3C : *World Wide web Consortium*

WAN : *Wide Area Network*

WIPO : *World Intellectual Property Organization*

ZRR : Zones à régime restrictif