LA SECURITE DE L'INFORMATION ET DES RESEAUX EST-ELLE UNE AFFAIRE D'ETAT(S) ?

PAR

Alain ESTERLE*

SOCIETE DE L'INFORMATION ET ENJEUX DE SECURITE

Jusqu'au milieu des années 1990, la sécurité de l'information concernait essentiellement la protection de l'information classifiée, celle qui relève de la défense et de la sécurité collective dont l'Etat à la charge[1]. Elle s'appuyait sur les mécanismes définis et mis en place par la puissance publique : cadre juridique fort (code pénal), technologies spécifiques (cryptologie) et procédures rigoureuses (habilitation des personnes, enregistrement-stockage-transport-destruction de l'information et de ses supports). Les dix dernières années ont vu se déployer les technologies de l'information et de la communication (TIC) sous forme de réseaux toujours plus complexes, interconnectés et supportant des débits croissants. Les travaux de l'OCDE, par exemple, rendent compte de cette évolution technico-opérationnelles et de son impact sur la vie quotidienne et l'économie : dès 2007, les deux tiers des liaisons Internet dans les pays de l'OCDE sont à large bande et concernent 20 % de la population totale ; 95 % en moyenne des entreprises de plus de 10 personnes utilisent internet, dont 17 % pour vendre leurs produits ou services ; d'ores et déjà, 25 % des consommateurs en moyenne utilisent internet pour acheter ou commander des biens ou services et 30 % d'entre eux pour accéder aux services bancaires[2]. Cela est tout sauf une surprise : c'est plutôt une révolution annoncée, sœur de la globalisation économique voulue ou subie du Nord au Sud.

Permettant de s'affranchir des frontières spatiales et temporaires pour l'échange de données et de savoirs, les technologies de l'information et de la communication (TIC) sont devenues un facteur majeur dans les mécanismes de prises de décision politique, économique et personnelle. Elles font figure de nouveau paradigme de la modernité et du développement. Si les Etats-Unis se sont engagés massivement dans cette voie dès les années 1990, l'Europe n'a pas tardé à leur emboîter le pas avec la Stratégie de Lisbonne adoptée en 2000. Objectif affiché : faire de l'Union européenne « *la zone économique la plus compétitive et dynamique au monde, fondée sur l'information et la connaissance et capable d'une croissance économique durable, d'emplois plus nombreux et de meilleure qualité et d'une plus grande cohésion sociale* ».

Il ne s'agira pas ici de discuter la validité de visions initiales sur l'entrée dans une nouvelle ère de l'humanité[3] ou d'apprécier si la crise financière et la récession économique qui s'engagent en 2008 vont remettre en cause ou conforter le paradigme des technologies de l'information comme moteur de croissance. Notre propos sera plutôt d'identifier, à travers

---

* Consultant indépendant spécialisé en sécurité des systèmes d'information.

1 *Cf.* décret n° 98-608, relatif à la protection des secrets de la défense nationale, 17 juil. 1998.

2 Pour plus d'informations, *cf.* par exemple OECD, « The future of economy », disponible sur le site Internet www.oecd.org/dataoecd/44/56/40827598.pdf.

3 *Cf.* Alvin TOFFLE, « The third wave ».

les évolutions en cours, d'éventuels éléments de blocage ou de changements profonds, notamment en ce qui concerne le rôle de l'Etat.

Confiance et sécurité

Un facteur essentiel dans l'usage des technologies de l'information est celui de la confiance. C'est un passage obligé pour la plupart des activités de la vie quotidienne, c'est en quelque sorte la réponse individuelle à la complexité du monde : faute de maitriser les savoirs techniques et opérationnels nécessaires, chacun est bien obligé de s'appuyer sur les capacités de ceux qui ont la charge d'assurer le bon fonctionnement et la sécurité des systèmes techniques mis en place.

Cependant, pour s'établir et perdurer, cette confiance a besoin d'éléments concrets, vérifiables et stables dans la durée. Quatre éléments sont couramment mis en avant pour assurer la sécurité des réseaux et de l'information qu'ils véhiculent : la disponibilité des réseaux, c'est-à-dire leur capacité à résister à toutes sortes d'agressions, volontaires ou non, et, en cas d'interruption, à revenir rapidement à des conditions normales de fonctionnement ; la confidentialité des informations, qui garantit que personne d'autre que le ou les récipiendaire(s) légitime(s) ne peu(ven)t avoir accès au contenu des messages ; l'intégrité des messages, autrement dit le fait que le contenu des messages reçus est identique à ce qu'il était lorsqu'ils furent envoyés ; l'authentification des interlocuteurs, c'est-à-dire la fourniture d'éléments suffisants de preuve quant à leur identité. La confidentialité était traditionnellement l'élément central de la protection de l'information classifiée. Les nouveaux réseaux, en particulier l'Internet et les mobiles, changent-ils la donne ? Peuvent-ils être utilisés pour traiter de l'information classifiée et jusqu'à quel stade ?

Les entreprises sont amenées, dans leur recherche constante de gains de productivité, à employer toujours plus les TIC. Elles doivent aussi protéger des informations très sensibles (savoir-faire internes, choix stratégiques), dont l'importance pour leur devenir, voire leur survie, n'a pas grand-chose à envier à celle de l'information classifiée pour le devenir de la nation. Vont-elles utiliser des outils de protection différents de ceux employés pour l'information classifiée ? Vont-elles développer des outils plus adaptés à un usage généralisé des TIC ? L'information classifiée pourra-t-elle en profiter ?

La gestion des réseaux publics de communication électronique relève aujourd'hui d'opérateurs privés. Pour autant, l'accès à ces réseaux et leur fiabilité, y compris pour Internet, est devenu d'une importance majeure, voire vitale, pour le bon fonctionnement de larges secteurs d'activité socio-économique dont l'Etat doit se porter garant. Dès lors, quel mode de gouvernance entre secteur public et secteur privé pour garantir au mieux la robustesse des réseaux publics et la continuité d'activité ?

Forces et faiblesses des outils de sécurité

Modifier un document papier sans laisser de trace apparente est une opération délicate alors que modifier ou dupliquer un document électronique est une opération aisée et il faut mettre en jeu des outils mathématiques complexes pour s'assurer que le contenu d'un message électronique n'a pas subi d'altération. La transmission électronique de messages est certes plus souple et rapide que la transmission de documents papier. En revanche, il est relativement facile de submerger un serveur avec des messages électroniques si nombreux qu'ils bloquent son fonctionnement et l'empêchent de recevoir tout message nouveau (attaque dite par « dénis de service »). La confidentialité des informations transmises a

toujours été un souci et le principe de confidentialité des correspondances est depuis longtemps au cœur des échanges postaux ; dans le cas des échanges électroniques, les nombreuses possibilités d'attaques dites par « l'homme au milieu » (*man in the middle*)[4] obligent à crypter les messages dont on veut assurer la confidentialité.

Authentifier les auteurs des messages électroniques est aussi une question délicate. Dans le cyberespace, on s'authentifie en fournissant des éléments de preuve de son identité sur la base de ce qu'on connaît (un mot de passe), ce qu'on est (une trace biométrique) ou ce qu'on a (une clef électronique).

Toutefois, aucun de ces outils n'est à la fois simple à créer, facile à utiliser et sûr dans la durée. Il est facile de se souvenir d'un mot de passe court (par exemple, les quatre chiffres du code PIN d'une carte à puce), mais il est dangereux d'utiliser partout le même mot de passe – s'il est découvert, on perd tous ses secrets d'un coup – et les mots de passe courts sont faciles à « casser » avec des outils informatiques[5]. Le problème est alors de se souvenir ou de gérer de manière sécurisée des mots de passe longs et diversifiés.

Les données biométriques (empreintes digitales, iris de l'œil, forme de la paume…) sont en principe caractéristiques d'un individu. En pratique, les senseurs qui relèvent rapidement ces traces pour les comparer à celles déposées dans une base de données donnent lieu à une proportion non négligeable d'erreurs, sous forme de « faux positifs » – déclarer identiques des traces de personnes différentes – ou de « faux négatifs » – déclarer différentes des traces d'une même personne). De plus, ces traces sont d'accès public, assez faciles à prélever (empreintes digitales sur des objets quotidiens) et à utiliser ensuite pour une reconnaissance à distance ; plus grave encore, lorsque une trace biométrique a été compromise, il est impossible à son vrai propriétaire de la remplacer comme cela peut se faire couramment pour un mot de passe et une clef numérique.

Ces dernières sont des outils cryptographiques qui permettent de vérifier l'identité de l'auteur d'un message. A une personne donnée sont attribuées deux clefs jumelles, l'une publique (tout le monde y a accès), l'autre privée (seule la personne la connait) ; ces deux clefs ont la propriété de se correspondre de façon exclusive dans une action de chiffrement/déchiffrement : un message chiffré par l'une ne peut être déchiffré que par l'autre[6], de sorte que déchiffrer avec succès un message avec la clef publique de quelqu'un garantit qu'il en est bien l'auteur. Le problème est alors d'être sûr qu'une clef publique donnée correspond bien à la personne à qui elle est censée appartenir. Pour cela est mis en place une « infrastructure de gestion de clefs » (IGC), où une autorité habilitée (Autorité de certification) génère un certificat électronique garantissant la correspondance entre une clef publique et une personne physique[7]. Cette méthode de certificats est couramment utilisée pour des actions très sensibles (déclaration d'impôts) et est à la base de la signature électronique[8]. Restent des points faibles, tels que la perte de la clef privée, qui nécessite de révoquer les deux clefs jumelles et d'en générer de nouvelles, le niveau de confiance à

4 Ce terme désigne toute une série de techniques permettant d'intercepter et de lire un message électronique au cours de son transfert entre l'émetteur et le récipiendaire

5 Ses mots de 8 à 10 caractères sont généralement préconisés pour assurer une bonne sécurité

6 *Cf.* par exemple le « *chiffrement asymétrique* » évoqué par Ivan MAXIMOFF, « Cryptologie et relations internationales », *Annuaire français de relations internationales*, vol. VI, 2005, p. 1 030-1 046.

7 L'Autorité de certification peut générer la bi-clef publique-privée, mais peut aussi se fonder sur une bi-clef existante après s'être assurée que la personne concernée est bien en possession de la clef privée.

8 *Cf.* directive EC/1999/93, transposée en France par la loi 2000-220 portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique, 13 amrs 2000, et complétée par le décret 2001-272, 30 mars 2001.

accorder aux autorités de certification et la compatibilité entre différentes infrastructures de gestion de clefs. En principe, une autorité de certification peut elle-même posséder un certificat garantissant sa signature et émis par une autorité de certification d'un niveau supérieur. En pratique, une telle pyramide de confiance est difficile à mettre en place et des IGC à usage spécifique se développent, notamment en Europe, sans liaison entre elles. L'usager doit alors avoir une signature par application électronique, ce qui devient vite très compliqué à gérer.

Dans ce contexte, le vol d'identité dans le cyberespace est une pratique courante. Sa forme la plus simple est le *social engineering*, où l'attaquant demande sous un prétexte quelconque de fournir volontairement son identifiant et son mot de passe[9]. Les dommages, financiers ou autres, peuvent être très élevés.

Evolution des menaces, des attaques et des incidents

Depuis les premiers virus informatiques il y a une vingtaine d'années, la typologie des outils et méthodes d'attaque a relativement peu évolué : il s'agit principalement de paralyser un réseau, de bloquer un point d'accès ou de se substituer à un utilisateur légitime afin de prendre le contrôle d'un ordinateur ou de pénétrer une base de données pour y récupérer les informations qu'elle contient ou y implanter des informations erronées.

En pratique, les virus (programme informatique auto-reproducteur), les vers (virus capable de se propage tout seul) et les chevaux de Troie (programme informatique à action masquée), toujours plus sophistiqués, continuent à proliférer tout en se sophistiquant. Lorsqu'ils ont pu être implantés dans un ordinateur au cours d'un échange de courrier ou d'un téléchargement, des logiciels pirates ou espions permettent d'en prendre un contrôle partiel ou total, d'y exécuter des ordres reçus à distance ou de récupérer des données à l'insu de l'utilisateur. Ils peuvent aussi altérer ou défigurer des sites web.

Autre fait pénalisant, la difficulté à disposer d'une évaluation quantitative fiable des incidents, des attaques (réussies ou non) et des dommages subis. Non pas qu'on manque de données : les fournisseurs de produits et services de sécurités[10] collectent les signaux d'alerte enregistrés par leurs senseurs disséminés dans de multiples réseaux à travers le monde et les associations d'utilisateurs[11] mènent régulièrement des enquêtes auprès de leurs membres sur la nature et les fréquences d'attaques subies. Pourtant, la disparité des méthodes de collecte, la réticence à diffuser des données brutes, l'ignorance fréquente des victimes quant aux attaques subies ou leur crainte de discrédit en cas d'ébruitement concourent à priver les experts de données synthétiques fiables[12]. Les données disponibles s'accordent néanmoins pour dessiner une évolution qualitative claire des menaces sur les quelques années écoulées, évolution qui peut se résumer en trois phases.

---

9 C'est aussi le principe du *phishing*, où un faux site Internet se fait passer pour celui d'un de vos prestataires habituels, votre banque par exemple, et vous invite alors à utiliser vos identifiant et mot de passe pour les utiliser ultérieurement à son profit.

10 Symantec, McAfee, Sophos pour n'en citer que quelques-uns

11 Notamment le CLUSIF en France et ses homologues en Italie et au Luxembourg.

12 *Cf.* par exemple le rapport de l'Agence européenne sur la sécurité de l'information et des réseaux, ENISA, « Examining the feasiblity of a data collection framework », nov. 2007, disponible sur le site Internet www.enisa.europa.eu/doc/pdf/studies/data_collection_report_20080214.pdf. Il est à noté que la mise en place d'un partenariat pour établir des données fiables d'incidents de sécurité avait rencontré moins de réticences du côté du secteur privé que du secteur public.

Jusque vers les années 2003-04, les menaces viennent surtout de personnes individuelles désireuses de démonter leur niveau de performance en pénétrant des réseaux ou des sites réputés protégés ou en créant et diffusant des virus pour affecter le plus grand nombre possible de machines ; un autre critère de performance est la capacité à construire le plus rapidement possible une attaque contre une vulnérabilité connue : de fait, la publication simultanée d'une vulnérabilité et de sa correction (*patch*) expose toutes les machines non corrigées dès qu'une attaque efficace (« exploit ») est construite[13] ; c'est la course au « *zero day* », qui désigne le cas où un « exploit » est connu dès que la vulnérabilité est révélée, mettant immédiatement en danger tous les systèmes où cette vulnérabilité existe et n'est pas corrigée.

A partir de 2004-05, des intérêts financiers sont apparus plus systématiquement être à l'origine des attaques contre les systèmes d'information. Le vol d'identité sert alors soit à détourner directement des fonds, soit à exercer des pressions ou même des chantages contre les personnes spoliées. Les attaques deviennent plus ciblées et un marché de l'insécurité se développe rapidement. Le principe est simple : les outils d'attaque sont proposés sous forme de kit accessible aux non-spécialistes, soit qu'il s'agisse d'une identité informatique volée (identifiant et mot de passe ou code PIN), d'un « exploit » contre une vulnérabilité ou d'un réseau de machines compromises (Botnet) permettant d'engager une attaque massive par déni de service. Ce marché montre des signes de maturité croissante avec une spécialisation des produits et services, des mécanismes de sous-traitance, de mise en concurrence et de modèles économiques adaptatifs[14].

Les années 2006-2007, enfin, ont été marquées par l'émergence d'attaques ciblant les services gouvernementaux avec une motivation explicitement politique. Ce fut le cas en Allemagne, aux Etats-Unis, au Royaume-Uni, en France[15] et surtout en Estonie. Du 27 avril au 14 mai 2007, les attaques informatiques contre les sites Internet et les nœuds du réseau Internet d'Estonie ont provoqué la paralysie dans la durée de larges secteurs de son réseau Internet[16], hissant du coup la menace informatique au rang de menace étatique. Ces événements ont conduit l'OTAN à décider la création d'un Centre d'excellence et de coopération en cyber-défense » et de choisir Tallin comme lieu d'implantation[17].

Ainsi, l'élargissement des menaces a accompagné la diversification et la complexification des réseaux et des applications, présageant que les menaces informatiques sont appelées à s'étendre à tout le spectre des menaces auxquelles les personnes, les entreprises et les Etats sont confrontés dans la vie réelle. Raison de plus pour évaluer les

---

13 Pour des informations régulières sur les vulnérabilités et les corrections disponibles, *cf.* les publications du CERTA, disponibles sur le site Internet www.certa.ssi.gouv.fr/.

14 *Cf.* par exemple « Symantec Internet security threat report », juil.-déc. 2007, disponible sur le site Internet eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiii_04-2008.en-us.pdf.

15 *Cf.* le site Internet www.lexpress.fr/actualite/politique/cyber-attaques-la-france-touchee-a-son-tour_466485.html.

16 En fait, les attaques se sont développées en deux phases. La première, apparemment peu coordonnée, visait les serveurs de sites Internet à forte connotation politique (Présidence, Parlement, police, autorités centrales, partis politiques), en rendant un certain nombre inaccessibles. Malgré l'aide des CERTs des pays voisins et un filtrage accru des messages pour réduire les perturbations, une deuxième vague a utilisé de larges réseaux de machines compromises (Botnets) pour bloquer des nœuds du réseau Internet et annihiler des sites plus diversifiés (autorités locales). Les perturbations ont duré trois semaines. *Cf.* le site Internet www.krisberedskapsmyndigheten.se/upload/17021/Large%20scale%20Internet%20attacks_utb-ser_2008-2.pdf.

17 Réunion du 15 mai 2008 à Bruxelles. *Cf.* par exemple le site Internet www.jamestown.org/single/?no_cache=1&tx_ttnews%5Btt_news%5D=33636.

nouvelles évolutions technologiques qui se dessinent, les nouveaux risques qui peuvent émerger et la manière dont les pouvoirs publics s'y préparent.

AMBITIONS EUROPEENNES ET EVOLUTIONS TECHNOLOGIQUES

Dès l'adoption de la Stratégie de Lisbonne, l'Europe a reconnu dans la question de la sécurité des réseaux et de l'information un facteur essentiel dans l'instauration d'une société de l'information et de la communication.

De 2000 à 2005, la Commission pilote les programmes préparatoires e-Europe 2000-02 et e-Europe 2002-05 et surtout deux actions majeures : la mise en place, en 2002, d'un cadre juridique encadrant le marché des systèmes de communication électronique (directives dites « Parquet Télécom ») et précisant la responsabilité des différents acteurs en matière de sécurité[18] ; la création, en mars 2004, de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)[19] pour stimuler la prise en compte de la sécurité pour les différents acteurs.

En 2005, l'adoption de l'initiative i2010 réaffirme les objectifs de la Stratégie de Lisbonne en précisant trois priorités : la mise en place d'un espace européen unique de l'information, le renforcement de l'innovation et de l'investissement, l'instauration d'une société de l'information incluant toutes les catégories sociales. L'espace européen unique de l'information doit « *relever le défi de la sécurité* », afin de « *rendre l'Internet plus sûr face aux menaces de fraudeurs, aux contenus préjudiciables et aux défaillances technologiques, pour augmenter la confiance des investisseurs et des consommateurs* »[20].

Un pas supplémentaire est franchi en mai 2006, avec la communication définissant « Une stratégie pour une société de l'information sûre »[21] et dont les orientations sont confirmées dans une résolution du Conseil en mars 2007. La stratégie proposée est simple : une société de l'information réellement sure doit se bâtir sur le dialogue, le partenariat et la responsabilisation des différents acteurs (administrations publiques, entreprises et utilisateurs individuels).

Cependant, une connaissance fiable des menaces, des incidents de sécurité, ainsi que des outils et procédures pour y faire face est nécessaire à la justification des investissements. Une série de travaux est alors engagée par la Commission européenne, sous l'égide de la Direction générale de la société de l'information et des médias : analyse des menaces (projet WOMBAT[22]), faisabilité d'un partenariat pour collecter des données sur les incidents de

---

18 Notamment : « *les Etats membres prennent toutes les mesures nécessaires pour assure l'intégrité des réseaux téléphoniques publics* » (directive 2002/22 dite « service universel », art. 23) ; « *les Etats membres garantissent l'indépendance des autorités réglementaires nationales* […] *les autorités réglementaires nationales* […] *garantissent l'intégrité et la sécurité des réseaux de communication publics* » (directive 2002/21 dite « cadre », art. 3 et 8) ; « *les autorités réglementaires nationales peuvent fixer les conditions que le fournisseur et les bénéficiaires devront satisfaire* […] *pour assurer le fonctionnement normal du réseau* » (directive 2002/19 dite « Accès », art. 5).

19 ENISA a été créée « aux fins d'assurer un niveau élevé et efficace de sécurité des réseaux et de l'information au sein de la Communauté et en vue de favoriser l'émergence d'une culture de la sécurité des réseaux et de l'information dans l'intérêt des citoyens, des consommateurs, des entreprises et des organismes du secteur public de l'Union européenne ». Cf. le site Internet www.droit-technologie.org/upload/legislation/doc/167-1.pdf.

20 *Cf.* le site Internet eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:FR:PDF.

21 *Cf.* le site Internet eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:FR:PDF.

22 *Cf.* le site Internet wombat-project.eu/.

sécurité et la confiance des utilisateurs (PISCE)[23], faisabilité d'un système d'alerte et d'échange d'information sur les incidents de sécurité (EISAS)[24], analyse du marché des outils et services de sécurité des réseaux et de l'information (étude SMART, travaux en cours).

Sur la base d'une proposition présentée par la Commission en novembre 2007, la révision des directives du Paquet Télécom a été entreprise comme convenu[25]. En matière de sécurité des réseaux et de l'information, la question principale porte sur l'obligation faite aux opérateurs de déclarer les brèches de sécurité. A ce jour, les avis convergent pour que les usagers soient informés en cas de compromission de leurs données personnelles (droit du consommateur). En revanche, les avis divergent quant à l'obligation d'informer une instance centrale (autorité nationale de régulation ?) en cas d'incident de sécurité. Il est prévu que les discussions soient achevées en 2010.

Par ailleurs, l'Union européenne a engagé une action vigoureuse en matière de protection des données classifiées. Des règlements de sécurité ont été adoptés par le Conseil européen en mars 2001[26] et la Commission en novembre 2001[27], pour définir notamment des règles techniques et procédures compatibles avec celles pratiquées dans les pays de l'Union pour la protection de l'information classifiée – y compris une table d'équivalence des différents niveaux de classification). Cependant, la reconnaissance de décisions de ce type par l'ensemble des Etats membres passe par un instrument juridique de la nature d'un traité, avec les procédures d'adoption formelle que cela suppose dans chaque pays. Il a donc fallu d'abord se contenter d'échanges de lettres entre les institutions européennes et chaque Etat membre. La procédure formelle d'adoption d'un traité a néanmoins été engagée par la France au cours de sa présidence de l'Union au second semestre 2008.

La mise en place d'un règlement de protection des informations classifiées a eu des répercutions politiques majeures : c'était une condition indispensable à la reconnaissance de l'Europe comme partenaire à part entière au niveau international en matière militaire et diplomatique, en particulier à la mise en œuvre de la Politique européenne de sécurité et de défense (PESD). Ainsi pouvait être signé le 17 mars 2003 l'accord dit « Berlin + » établissant non seulement les conditions d'échange d'informations classifiées entre l'OTAN et l'Union européenne, mais aussi un accès réciproque à certains de leurs outils opérationnels et les modalités d'une concertation sur le développement de leurs capacités respectives[28].

Evolutions technologiques

Parallèlement à ces efforts pour bien maitriser les conditions de sécurisation des réseaux et de l'information, l'Union européenne cherche à accroître sa compétitivité en développant de nouvelles technologiques et de nouveaux systèmes d'information de plus en plus centrés sur l'emploi du protocole Internet. Quelques exemples suffissent à esquisser les nouveaux enjeux de sécurité associés à ce « futur Internet ».

L'avenir est à la mobilité. Les téléphones mobiles accueillent données, images, vidéo, les liaisons Wifi et Wimax se généralisent : le paradigme des réseaux accessibles n'importe où, n'importe quand et par n'importe qui devient réaliste. En revanche, la sécurité est

23 *Cf.* le site Internet www.enisa.europa.eu/doc/pdf/studies/data_collection_report_20080214.pdf

24 *Cf.* le site Internet www.enisa.europa.eu/doc/pdf/studies/EISAS_finalreport.pdf.

25 Dans la plupart des directives communautaires, une clause prévoit leur révision au bout de quelques années.

26 Décision du Conseil européen 2001/264, 19 mars 2001

27 Décision de la Commission 2001/844/CE, 29 nov. 2001, modifiée par la décision du 31 janvier 2006.

28 *Cf.* le site Internet www.nato.int/shape/news/2003/shape_eu/se030822a.htm.

souvent négligée : contrôler l'accès d'un réseau avec une même clef pour tous (clef WEP d'un réseau Wifi), c'est prendre le risque d'intrusions faciles. Protéger un téléphone mobile avec un code PIN à quatre chiffres est raisonnable tant qu'un clavier manuel est l'unique mode d'accès, mais dès que les essais peuvent être générés électroniquement (voix sur IP), ce code peut être cassé en un clin d'œil et des contrôles d'accès plus complexes et donc plus difficiles à mémoriser deviennent indispensables.

Le concept de Grille informatique (ou Grid) se répand. Il ne s'agit plus de relier un ordinateur à un réseau, mais de relier entre elles des capacités de calcul et de stockage de données et de les rendre accessibles à beaucoup d'utilisateurs au grès de leurs besoins. Les utilisateurs sont alors délivrés de la charge de stocker et de mettre à jour eux-mêmes de larges volumes de données et logiciels ou même de savoir où les trouver. Encore faut-il qu'ils aient la certitude que ces données et logiciels resteront disponibles et facilement accessibles. A l'inverse, l'authentification des utilisateurs et le contrôle de leurs droits d'accès deviennent cruciaux.

Jusqu'à aujourd'hui, Internet relie surtout des individus[29]. Demain va se développer l'Internet des choses. Deux étapes principales. Dès à présent, l'identification par radiofréquence (ou RFID) interroge un petit émetteur-récepteur attaché à un objet pour recueillir des informations accumulées au cours de son histoire ; il peut ainsi être identifié de façon unique[30] et rapporter les informations enregistrées par ses capteurs (déplacements, environnement physico-chimique…). Cependant, les informations collectées sont centralisées pour traitement ultérieur : le RFID n'ayant pas de capacité de calcul et d'analyse, il ne peut proposer ni engager aucune action par lui-même. La situation devrait changer radicalement avec les calculateurs enfuis. Combinant les progrès attendus en nano-électronique et en programmation logicielle, ils pourront analyser les informations transmises par leurs capteurs et surtout entretenir des liaisons avec les calculateurs voisins pour fournir en permanence une analyse de la situation, diagnostiquer des évolutions et proposer des actions préventives ou correctives. Un marché considérable est en gestation, par exemple dans les secteurs de l'automobile (autodiagnostic des pannes, autocontrôle de la circulation), de l'environnement domestique (sûreté, environnement intelligent), des procédés industriels (flexibilité, contrôle, optimisation), des transports aériens (sureté, sécurité), des infrastructures publiques de distribution d'électricité, gaz, eau (optimisation des consommations, continuité de service), des équipements médicaux (chirurgie, diagnostic, imagerie, capteurs implantés), etc.

Ces évolutions, déjà largement engagées, présagent l'instauration d'« environnements intelligents » et de l'information omniprésente, sur la base de réseaux ouverts, reconfigurés en permanence par l'entrée et la sortie de nouveaux éléments. Dans ce « futur Internet », la gestion centralisée des règles de sécurité devra céder la place à une gestion distribuée, chaque nouvel entrant devant dialoguer avec les éléments environnant pour s'adapter aux conditions de l'ensemble.

---

29 Les personnes sont authentifiées par des adresses IP, mots de passe et autres éléments identité. Les serveurs s'authentifient aussi, mais ils gardent un rôle passif : ils ne font que répondre aux questions sans prendre d'initiative.

30 Le code-barres utilisé depuis une trentaine d'années ne permet que de lire par rayon laser quelques informations se rattachant à un objet donné (nature, catégorie, prix…). Il ne permet pas de l'identifier de façon unique

PROTECTION DES INFORMATIONS CLASSIFIEES ET DES INFORMATIONS NON CLASSIFIEES : QUELLES FRONTIERES ?

Beaucoup d'outils et de standards existent pour sécuriser un système d'informations[31], mais les bonnes politiques de sécurité reposent toujours peu ou prou sur la même architecture de base :

- évaluation des risques[32] : identification des systèmes et informations à protéger, évaluation des besoins de sécurité, analyse des contraintes juridiques, techniques et programmatiques, identification des risques
- gestion des risques : choix des risques à prévenir et des risques résiduels, choix d'outils et procédures de sécurité les plus adaptés aux besoins compte tenu des contraintes ;
- implantation des outils et procédures de sécurité et validation du système ainsi protégé ;
- gestion des incidents de sécurité, y compris la réaction aux attaques de grande ampleur, la gestion de crises et les plans de continuité d'activité ;
- planification de tests et audits réguliers des outils de sécurité, ainsi que sur les éléments sensibles du système ; sensibilisation du personnel, formation et exercices ;
- mises à jour : correction des vulnérabilités identifiées, mise en œuvre des conclusions des audits, adaptation des capacités de sécurité aux évolutions du système.

Plus les informations en cause sont sensibles, plus la politique de sécurité se fondera sur une architecture complète, détaillée et conforme aux standards en vigueur. Plus une entreprise est dotée de moyens et d'expérience, plus elle sera disposée à déployer des politiques de sécurité élaborées pour protéger ses systèmes d'information[33].

Systèmes d'information et informations classifiées

Chaque pays – et aussi, depuis 2001, les institutions européennes – dispose de règles de protection des informations classifiées. Les informations sont classifiées en niveaux de nuisance en cas de divulgation, auxquels correspondent les niveaux d'habilitation des personnes pour y accéder[34]. S'y ajoute une deuxième catégorisation par thème, portant sur le contenu des informations et qui, pour les personnes, doit correspondre au « besoin d'en connaître ». Ce croisement multicritères est complété par des règles de contrôle technique sur chaque mouvement ou traitement d'information : enregistrement, stockage, consultation, transmission, déclassement ou déclassification, destruction. Ces règles ont été mises en œuvre depuis longtemps dans le monde physique réel utilisant le support papier. Leur transposition à des systèmes électroniques a généralement conduit aux conditions suivantes – nous suivons ici le schéma décrit dans le règlement de sécurité du Conseil européen 2001/264).

---

31 *Cf.* par exemple « Network and information security report – ICTSB/NISSG », 2007, disponible sur le site Internet www.cen.eu/cenorm/businessdomains/businessdomains/isss/activity/nisfinalreport.pdf.

32 Un risque est la combinaison d'une vulnérabilité (faiblesse d'un système) et d'une menace (possibilité d'utiliser une vulnérabilité pour infliger des dommages au système). Les menaces peuvent être intentionnelles ou non. Le risque peut se mesurer comme le produit da la probabilité d'occurrence d'une menace par l'ampleur des dommages subis.

33 Il existe des méthodes et outils de sécurité adaptés aux moyens et contraintes des petites et moyennes entreprises.

34 *Cf.* en France le décret n° 68-608, 17 juil. 1998, et l'instruction interministérielle 1300/SGDN/PSE/SSD.

Deux autorités sont désignées, d'une part une autorité responsable de l'exploitation du système, d'autre part une autorité d'homologation de sécurité. L'homologation est une opération fondamentale, qui consiste à valider un système avant sa mise en exploitation et après vérification que l'ensemble des exigences de sécurité décrites dans un document de référence dénommé SSRS (System-specific Security Requirement Statement) ont bien été prises en compte.

Dès le début du développement du système, le SSRS est établi par l'autorité d'exploitation et doit être validé par l'autorité d'homologation. Il traite les différentes composantes de l'architecture générale de sécurité décrite ci-dessus : évaluation et gestion des risques, mise en œuvre et validation des conditions de sécurité, gestion des incidents, contrôles et mises à jour. Une attention particulière est prêtée aux procédures d'exploitation de sécurité (SecOP), qui s'appuient sur une description détaillée des opérations et des dispositifs de sécurité. Une fois le système développé, l'autorité d'homologation vérifie que le niveau de protection souhaité a bien été atteint conformément au SSRS et, si c'est bien le cas, délivre l'homologation. Les mêmes thèmes se retrouvent donc dans les démarches mises en œuvre pour sécuriser des systèmes, qu'ils traitent d'information classifiées ou non classifiée, mais avec quelques différences notoires.

Dans le cas des informations classifiées, la sécurisation des systèmes suit une démarche rigoureuse et systématique. Elle intervient très tôt, alors que les développements commerciaux font souvent l'impasse sur la sécurité pour gagner le plus rapidement possible des parts de marché (téléphones portables, réseaux Wifi…). Elle prévoit aussi la validation de chaque étape, de chaque sous-système et de chaque produit de sécurité[35]. La protection des informations classifiées prévoit aussi une analyse des rayonnements parasites compromettants, rarement prise en compte pour les informations non classifiées. Tous les équipements électroniques en fonctionnement rayonnent plus ou moins et ce rayonnement peut dans certains cas être récupéré et analysé pour restituer l'information d'origine (par exemple l'image d'un écran d'ordinateur), entraînant une perte de confidentialité. Les règlements prévoient alors des zones interdites d'accès à proximité des équipements informatiques, dimensionnées en fonction de leur niveau de rayonnement. Enfin, la protection des informations classifiées passe par une responsabilisation particulière des acteurs. En France le Code pénal punit les « *atteintes aux systèmes de traitement automatiques de données* », qu'elles soient classifiées ou non (article 323) : accès frauduleux, suppression ou modification de données, entrave au bon fonctionnement d'un système, introduction frauduleuse de données. Dans le cas des informations classifiées, l'article 413-10 du Code pénal prévoit en plus de punir toute personne dont les activités professionnelles auraient conduit, même « *par imprudence ou négligence* », à la divulgation d'un « *renseignement, procédé, objet, document, données informatisées ou fichier qui a un caractère de secret de la défense nationale* ».

La contrepartie de cette démarche rigoureuse réside dans un certain nombre de difficulté de mise en œuvre. Quel que soit le support utilisé, le marquage du niveau de classification des informations est une règle générale, aisée à mettre en œuvre de façon visible et stable sur tout support papier, plus difficile à respecter dans le cas de fichiers électroniques. La solution est alors de confiner les informations dans un réseau dédié exclusivement au niveau de classification en cause, voire au thème en question (besoin d'en connaître), mais cela peut entraîner d'autres difficultés pour la gestion de l'accès simultané à de multiples réseaux. Nous y reviendrons.

---

35 En France, cette validation des produits et sous-systèmes s'appelle « agrément ». Elle inclut notamment une évaluation selon des référentiels non publics (distincts des critères communs, même s'ils s'en inspirent en partie), une analyse des outils cryptographiques et un contrôle des rayonnements parasites compromettants

L'évaluation de produits et systèmes de sécurité selon les critères communs est une opération qui peut être longue et coûteuse, à la mesure de la complexité du système et du niveau d'assurance de sécurité souhaité[36]. L'évaluation de systèmes relativement simples (carte à puce par exemple) peut être menée dans de bonnes conditions, mais il ne suffit pas de combiner des évaluations de sous-systèmes simples pour obtenir l'évaluation d'un système complexe. Longtemps réticent à l'emploi des critères communs, probablement en raison de la brièveté du cycle de vie moyen d'une génération de produit et de la difficulté à amortir le coût d'une évaluation selon ces critères, le marché des TIC semble aujourd'hui évoluer favorablement à leur égard.

Le marché des technologies de l'information a aussi fait évoluer la question des signaux compromettants. Les équipements informatiques se sont réduits en taille, poids et puissance consommée, entraînant une diminution d'intensité des rayonnements parasites. Cependant, les réseaux Wifi et les équipements mobiles ont introduit de nouveaux risques dans l'emploi délibéré des rayonnements comme vecteurs de transmission d'informations (contrôle d'accès, interceptions…). La qualité des outils cryptologiques pour protéger la confidentialité des informations devient primordiale[37].

Enfin, les systèmes traitant des informations classifiées sont confrontés à une difficulté particulière pour la gestion d'informations de différents niveaux de classification sur un même équipement informatique[38]. Cela revient à établir un cloisonnement logique étanche dans une même machine physique, problème connu sous le nom de virtualisation – créer des machines virtuelles sur la base des composantes d'une machine réelle. Il y a là un intérêt économique et opérationnel majeur : se connecter en toute sécurité à des réseaux différents sans accroître le nombre d'équipements sur le lieu de travail. Des travaux sont en cours, d'une part pour connecter de façon étanche une machine à plusieurs réseaux d'un même niveau de classification, d'autre part pour connecter des réseaux de différents niveaux de classification en interdisant qu'une information du niveau supérieur puisse accéder à un réseau de niveau inférieur (principe de la diode).

Le développement des technologies de l'information réseaux pose des problèmes particuliers aux Etats pour la mise en œuvre des règles de protection des informations classifiées. Il en pose aussi en ce qui concerne la stabilité et la robustesse des réseaux publics de communication électronique.

---

36 Les critères communs pour l'évaluation de produits et systèmes d'information résultent de la fusion, au début des années 1990, de critères distincts utilisés aux Etats-Unis, en Europe et au Japon. Ces critères communs décrivent d'une part les fonctionnalités du produit (cible d'évaluation), d'autre part les niveaux d'assurance de sécurité (cible de sécurité). Ces niveaux d'assurance sont regroupés dans une échelle à 7 niveaux, la première correspondant à une analyse essentiellement documentaire, la dernière à une analyse détaillée des codes informatiques.

37 *Cf.* par exemple Ivan MAXIMOFF, *op. cit.*

38 On distingue couramment trois modes d'exploitation des équipements informatiques. Le mode exclusif, où les informations sont du même niveau de classification et traitent du même sujet ; l'accès au réseau peut être accordé sur la base de l'habilitation et du besoin d'en connaître. Le mode dominant correspond au cas des informations d'un même niveau de classification, mais les utilisateurs du réseau n'ont pas tous le même besoin d'en connaître ; il faut introduire des règles de sélection particulière dans l'exploitation du réseau. Le mode multi-niveaux désigne les réseaux dont l'accès est autorisé à des utilisateurs d'habilitation différente et de besoins d'en connaître distincts ; l'exploitation du réseau doit alors prévoir des règles particulières pour traiter des informations classifiées de différents niveaux et sur différents sujets.

RESILIENCE DES RESEAUX PUBLICS DE COMMUNICATION ELECTRONIQUE

Ces dernières années ont montré en Europe une capacité limitée à résister à des attaques électroniques d'une grande ampleur (*cf. supra*) ou à des incidents graves [39] et à rétablir rapidement un fonctionnement normal des systèmes (résilience). Cette problématique s'inscrit dans la perspective plus générale de la protection des infrastructures critiques[40] suscitée, entre autres, par les attentats terroristes contres les systèmes de transports aux Etats Unis, en Espagne et au Royaume-Uni depuis 2001. La capacité à assurer la résilience des réseaux publics de communication fait débat en termes de responsabilité, de partenariat, de règles de sécurité à appliquer et d'échange de données.

Dimension nationale et dimension européenne

Les conditions de protection des infrastructures critiques d'un pays relèvent de sa souveraineté et la responsabilité en incombe en premier lieu aux Etats membres et aux propriétaires/exploitants de ces infrastructures[41].

Néanmoins il existe certaines infrastructures dont l'implantation dépasse le cadre national d'origine et dont l'arrêt ou la destruction affecterait plusieurs Etats. D'où l'émergence du concept d'infrastructures critiques européennes, le besoin de les recenser et d'établir des politiques de sécurité dépassant le cadre strictement national, même si la responsabilité de leur protection « *incombe essentiellement et en dernier ressort aux Etats membres et leurs propriétaires/opérateurs* »[42]. Cette question est particulièrement importante pour les opérateurs qui travaillent sur plusieurs pays et pour lesquelles les disparités juridiques, techniques ou opérationnelles peuvent entrainer des surcoûts importants et générer des distorsions de compétitivité.

Depuis 2006, on assiste donc à un double mouvement : au niveau national, l'établissement de partenariats entre les secteurs public et privé pour définir des règles de sécurisation des infrastructures critiques, chacune dans son domaine ; au niveau européen, des échanges de données et d'expérience pour harmoniser au mieux les méthodes et règles de sécurisation des infrastructures européennes. Les réseaux publics de communication électronique (télécommunications fixes et mobiles ainsi qu'Internet) font bien sûr partie de cette double démarche.

Points communs et disparités entre stratégies nationales

Dès 2006, la Commission européenne a entrepris une étude des conditions de disponibilité et robustesse des réseaux de communication électronique à l'échelle européenne. Les résultats ont mis en évidence un souci partagé entre Etats membres de renforcer la robustesse de ces réseaux, mais aussi des faiblesses certaines, notamment un

---

39 *Cf.* par exemple les sites Internet www.journaldunet.com/solutions/0603/060322-panne-reseau-neuf-telecom.shtml ; www.mobinaute.com/167368-sfr-panne-reseau-touche-15-abonnes-mobiles.html ; forum.telecharger.01net.com/telecharger/telecom_et_reseaux/fournisseurs_dacces_internet/comment-neuf-telecom-maltraite-ses-clients-panne-6semaines-405903/messages-1.html.

40 *Cf.*la définition des Infrastructures critiques dans la directive 2008/114/EC, art. 2-a : un point, système ou partie de celui-ci, situé dans les Etats membres, qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien -être économique ou social des citoyens et dont l'arrêt ou la destruction aurait un impact significatif dans un Etat membre du fait de la défaillance de ces fonctions.

41 COM 2006/787 final, proposition de directive, 4e considérant.

42 Directive 2008/114/CE 6e considérant.

manque de coordination[43] transnationale pour la préparation aux situations de crise, ainsi que l'absence d'accord de soutien mutuel et de structure d'échange d'information. Les recommandations qui en découlent sur une analyse plus approfondie des mécanismes d'interdépendance entre les différents types d'infrastructures, une meilleure formalisation des partenariats entre parties prenantes, les échanges de bonnes pratiques. Des études complémentaires ont été entreprises pour approfondir ces différents points[44].

La résilience des réseaux publics de communication électronique a aussi été choisie comme un axe majeur du programme de travail d'ENISA pour la période 2008-2010. Les travaux de 2008 ont porté notamment sur l'analyse des rôles et responsabilités respectifs des instances de régulation et des opérateurs à l'échelle nationale (22 Etats membres analysés plus 3 pays voisins). Des différences notables apparaissent, par exemple en matière de régulation : co-régulation (Allemagne, Suède), autorégulation (Pays-Bas) ou règlementation nationale. Si règlement national il y a, il peut être centré sur les capacités de réponse aux attaques plutôt que sur les mesures préventives (Chypre, Hongrie). Il peut exister une entité spécifique chargée de piloter la stratégie nationale (CPNI[45] au Royaume-Uni, NICC[46] aux Pays-Bas, CNPIC[47] en Espagne), mais cette responsabilité peut aussi être confiée à des instances existantes à responsabilités plus larges (SGDN en France).

Echange d'informations à l'échelle européenne

Proposé dès 2005, un réseau européen d'alerte concernant les infrastructures critiques et dénommé CIWIN est en cours de mise en place[48]. Il est constitué d'un réseau informatique sécurité (niveau Restreint UE), géré par les services de la Commission européenne et disposant dans chaque Etat membre d'un point de contact ou « responsable CIWIN ». Le réseau CIWIN est appelé à remplir les fonctions de (a) forum informatique pour les échanges d'information concernant les infrastructures critiques, (b) système d'alerte rapide entre Etats membres en cas de menaces ou risques immédiat sur ces d'infrastructure, sans toutefois interférer avec les Systèmes d'alerte rapide existants, par exemple à Europol. Il appartient à chaque responsable CIWIN national de gérer les droits d'accès dans son pays.

Une démarche complémentaire a été engagée à partir de 2007-2008. Il s'agit de définir des modalités communes d'échange de données sur les infrastructures critiques[49] et de construire une plate-forme informatique pour concrétiser ces échanges entre les différentes parties prenantes sur une base volontaire. L'idée est que cette plate-forme soit compatible avec les différents modes de partenariat nationaux (par exemple centralisé ou distribué) afin de répondre à un enjeu de partage d'information sécurité le plus large possible. La première version, prévue en 2009, sera limitée aux informations non classifiées, tout en réservant la possibilité de l'étendre ultérieurement à des informations classifiées.

---

43 *Cf.* le rapport final de l'étude ARECI (Availability and Robustness of Electronic Communication Infrastructure), disponible sur le site Internet ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=3334.

44 *Cf.* par exemple le site Internet ec.europa.eu/justice_home/funding/cips/funding_cips_2en.htm.

45 Centre for the Protection of National Infrastructures.

46 The Netherlands National Infrastructure Crime Centre.

47 Centro nacional de protección de infraestructuras críticas.

48 *Cf.* le site Internet www.senat.fr/europe/textes_europeens/e4071.pdf.

49 Projet MS3I, Messaging Standard for Sharing Security Information.

QUEL ROLE POUR L'ETAT ? SELON QUEL MODELE ?

Les évolutions esquissées ci-dessus en matière de technologies de l'information, de réseaux et de services ainsi que leur impact sur les modalités de protection de l'information apportent des éléments de réponse à la question posée en titre. La sécurité des réseaux et de l'information reste clairement une affaire d'Etat, dans la mesure où l'Etat y est impliqué en premier chef et y exercent une responsabilité directe. Néanmoins, les modalités de cette implication et l'exercice de cette responsabilité ont sensiblement évolué avec l'émergence d'autres acteurs, qu'ils soient non étatiques (opérateurs de systèmes de communication électronique, autorité de régulation) ou qu'ils relèvent de nouvelles coopérations interétatiques (échange de bonnes pratiques, reconnaissance mutuelle de compétences, partage de capacités…). Sur cette base, chaque Etat adapte ses structures institutionnelles, sa politique et ses moyens aux nouveaux enjeux de sécurité, qu'il s'agisse de la protection des informations classifiées, des informations sensibles dans le secteur marchant ou des réseaux public de communications électroniques.

Une étude menée en 2004-2005[50] avait déjà montré les grandes disparités entre Etats membres de l'Union en matière de moyens, d'organisation, de priorités et, surtout, une insuffisance de coordination et de cohérence. Depuis lors, la généralisation des réseaux mobiles et Wifi et l'approfondissement de la problématique des infrastructures critiques dans le cadre de la lutte antiterroriste ont entraîné de nouvelles adaptations, tenant compte des spécificités de l'appareil socio-économique de chaque pays. Cela n'a pas réduit les disparités intra-européennes, bien au contraire, mais a renforcé le besoin de concertation et de coopération, ce qui est une bonne chose.

Dans ce contexte général, les orientations suivies par la France méritent une attention particulière. Annoncées dans le Livre blanc sur la défense et sécurité nationale, elle prévoient notamment un développement accru des moyens de détection précoce des attaques informatiques, le recours à des produits de sécurité et à des réseaux de confiance, « *des dispositions réglementaires pour que les opérateurs de communications électroniques mettent en œuvre les mesures nécessaires à la protection de leurs réseaux contre les pannes et les attaques les plus graves* », ainsi que la « *reconnaissance d'Internet comme infrastructure vitale* »[51]. Pour conforter ces choix et les capacités propres des moyens de l'Etat, une Agence nationale chargée de la sécurité des systèmes d'information est en cours de création pour assurer les trois missions fondamentales que sont la détection et la défense face aux attaques informatiques, le développement et l'acquisition des produits et services de sécurité essentiels à la protection des réseaux les plus sensibles de l'Etat et, enfin, les conseils au secteur privé en matière de sécurisation des réseaux, notamment pour les secteurs d'importance vitale, et la participation à la diffusion de la sécurité dans la société de l'information

Cette agence doit constituer un réservoir d'expertise en SSI apte à soutenir l'action des administrations et des opérateurs d'infrastructures vitales, notamment les systèmes de communication électronique, ainsi qu'à informer le grand public. Elle s'appuiera sur : a) des capacités industrielles nationales aptes à développer « *des produits de très haute sécurité totalement maîtrisés pour la protection des secrets de l'Etat, ainsi qu'une offre de produits et services de confiance labellisés à laquelle recourront les administrations et qui seront largement accessibles au secteur économique* » ; b) un réseau territorial d'experts au sein d'observatoires de la sécurité des systèmes d'information, chargés d'animer la remontée de signaux précurseurs d'incident et du soutien

50 « Sécurité de l'information : un nouveau défi pour l'Union européenne », *Cahier de Chaillot*, n° 76, mars 2005.

51 *Cf. Le Livre blanc Défense et sécurité* nationale, Odile Jacob/La Documentation française, », p. 182.

aux administrations locales en matière de formation et de conseil ; des liaisons étroites avec les partenaires étrangers, notamment européens, afin d'encourager le développement d'une politique de sécurité des réseaux de communication à l'échelle européenne.

La création de cette agence nationale représente une évolution rapide sur une dizaine d'années, en partant du Service central de la sécurité des systèmes d'information (SCSSI) directement rattaché au cabinet du Premier ministre et focalisé sur le contrôle des outils cryptologiques et la protection des informations classifiées et passant en 2000 par la Direction centrale de la sécurité des systèmes d'information (DCSSI) intégrée au Secrétariat général de la défense nationale (SGDN) et dotée de fonctions de régulation, d'évaluation des menaces et de capacité d'alerte, de formation et de conseil au bénéfice des services publics ainsi que de développement de l'expertise scientifique et technique. Cette évolution est remarquable à plus d'un titre. Elle concentre dans une même entité les fonctions essentielles de l'Etat en matière de sécurité des réseaux et de l'information, tout en préservant les liens entre les problématiques anciennes et nouvelles. Elle permet à la France de parler d'une seule voix dans les instances européennes ou internationales traitant des diverses facettes du sujet – d'autres Etats membres y sont souvent représentés par des services administratifs différents. Elle représente aussi une économie d'échelle car, si la nouvelle agence nécessite une forte croissance par rapport aux moyens humains de la DCSSI (de 110 à 300 personnes sur 3 ou 4 ans[52], elle restera très en-deçà des moyens déjà alloués aux organisations analogues au Royaume-Uni et en Allemagne (450 à 500 personnes). Cette réponse française à l'évolution des technologies de l'information et aux enjeux de sécurité qui en découlent est un modèle original, solides, adapté aux besoins et qui devrait engendrer des émules.

52 *Cf.* le rapport d'information sur la cyber-défense, Commission des Affaires étrangères, de la Défense et des Forces armées, p. 46, disponible sur le site Internet www.senat.fr/rap/r07-449/r07-4491.pdf.